Connected Communities
Infrastructure Solution
Design Guide
September 2020
Contents

Scope of CCI Release 2.0 .......................................................... 1
  New capabilities in CCI Release 2.0 ............................................. 2
References .............................................................................. 2
Document Organization ............................................................. 3
Solution Overview ................................................................. 4
  Cisco Connected Communities Infrastructure .......................... 4
  CCI Network Architecture ..................................................... 4
  CCI Validated Use Case Solutions ........................................... 5
  CCI Unique Selling Points ...................................................... 5
Solution Architecture ............................................................ 7
  CCI Overall Network Architecture .......................................... 7
  CCI Modularity ..................................................................... 7
  CCI Major Building Blocks ................................................... 8
    Centralized Infrastructure ................................................. 8
    Point of Presence (PoP) .................................................... 11
    Backhaul for Points of Presence ....................................... 13
    Remote Point of Presence (RPoP) ...................................... 14
CCI’s Cisco Software-Defined Access Fabric ......................... 14
  The SD-Access Fabric Network Layers of CCI ....................... 14
  Underlay Network ................................................................ 16
  Overlay Network .................................................................. 17
  Fabric Data Plane and Control Plane .................................... 17
  Fabric Border ...................................................................... 18
  Fabric Edge ........................................................................ 19
  Fabric-in-a-Box (FiaB) ......................................................... 19
  Extended Nodes and Policy Extended Nodes ......................... 19
  Endpoints ............................................................................ 22
  Transit Network .................................................................... 22
  Fusion Router ...................................................................... 24
Access Networks and Edge Compute ..................................... 24
Next-Generation Firewall (NGFW) and DMZ Network .......... 25
Common Infrastructure and Shared Services ......................... 27
  Cisco DNA Center ............................................................. 27
  Cisco DNA Center Appliance ............................................... 28
  Identity Services Engine (ISE) ............................................. 28
<table>
<thead>
<tr>
<th>Application Servers Network</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field Network Director (FND)</td>
<td>31</td>
</tr>
<tr>
<td>Network Time Protocol (NTP) Server</td>
<td>32</td>
</tr>
<tr>
<td>Cisco Prime Network Registrar (CPNR)</td>
<td>32</td>
</tr>
<tr>
<td>Headend Routers (HER)</td>
<td>32</td>
</tr>
<tr>
<td>Authentication, Authorization, and Accounting (AAA)</td>
<td>33</td>
</tr>
<tr>
<td>Remote Authentication Dial-In User Service (RADIUS)</td>
<td>33</td>
</tr>
<tr>
<td>Public Key Infrastructure (PKI)</td>
<td>33</td>
</tr>
<tr>
<td>Certificate Authority</td>
<td>33</td>
</tr>
<tr>
<td>Cisco Kinetic for Cities (CKC)</td>
<td>33</td>
</tr>
<tr>
<td>Cisco Wireless LAN Controller (WLC)</td>
<td>34</td>
</tr>
<tr>
<td>Cisco Prime Infrastructure</td>
<td>34</td>
</tr>
<tr>
<td>Cisco DNA Spaces</td>
<td>34</td>
</tr>
</tbody>
</table>

**Solution Components**

| CCI Security Architecture and Design Considerations | 34 |
| Security Segmentation Design | 38 |
| Advantages of Network Segmentation | 38 |
| Micro Segmentation Design in Ethernet Access Ring | 39 |
| Micro Segmentation Design in Policy Extended Nodes Ring | 40 |
| Network Visibility and Threat Defense using Cisco Stealthwatch | 42 |
| Flexible NetFlow Data Collection | 42 |
| Cisco Stealthwatch for CCI Security | 44 |
| Cisco Stealthwatch Deployment Considerations | 45 |
| Security using Cisco Stealthwatch for abnormal traffic detection | 45 |

**Secure Connectivity**

| CCI Network QoS Design | 46 |
| CCI Wired Network QoS design | 48 |
| QoS Design for Fabric Devices | 49 |
| CCI QoS Considerations | 56 |

**Ethernet Access Ring QoS Design**

| IE4000 and IE5000 Series Switches QoS Design | 57 |
| IE3300, ESS 3300, and IE3400 Series Switches QoS Design | 60 |
| Classification and Marking | 60 |

**CCI Wireless Network QoS Design**

| Cisco Unified Wireless Mesh Access Network QoS Considerations | 62 |
| SD-Access Wireless Network QoS Considerations | 64 |
| CCI QoS Treatment for CR-Mesh and LoRaWAN Use Cases Traffic | 65 |
| CCI QoS Design Considerations for CR-Mesh Traffic | 65 |
| CCI QoS Design Considerations for LoRaWAN Traffic | 66 |

**QoS Considerations on RPoP**

| CCI Network Data Flow Diagrams | 67 |
LoRaWAN device addition via Actility management portal ........................................... 136
LoRaWAN deployment guidance .................................................................................. 136
CCI Rail Trackside Access Network Solution .............................................................. 136
Rail Solution System Level Overview ......................................................................... 137
Connected Trains ........................................................................................................ 138
Trackside Network ....................................................................................................... 138
Station Network ............................................................................................................ 138
Backhaul ....................................................................................................................... 139
Centralized Infrastructure ............................................................................................. 139
Overview of Fluidmesh Technology ........................................................................... 139
Solution Components ................................................................................................. 141
Fluidmesh Mesh Point and Mesh End ......................................................................... 142
Fluidmesh Global Gateway .......................................................................................... 142
High Availability (Fluidmesh TITAN) ........................................................................ 143
Quality of Service Support .......................................................................................... 143
Network Provisioning and Monitoring ....................................................................... 144
Configuration Tools (Configurator and RACER) ......................................................... 144
Fluidmesh MONITOR .................................................................................................. 145
Fluidmesh and CCI Network Integration and Considerations ....................................... 146
Cisco DNAC .................................................................................................................. 146
Virtual Network and Segmentation ............................................................................. 146
IP Pool ............................................................................................................................ 146
Host Onboarding .......................................................................................................... 147
Datacenter PoP .............................................................................................................. 147
Edge PoP ....................................................................................................................... 147
End-to-End QoS Integration ....................................................................................... 152
Trackside Network Design and Considerations ......................................................... 152
Fluidmesh Product Compliance and Physical Deployment ........................................ 153
CCI Remote Point-of-Presence Design ...................................................................... 154
Remote Point-of-Presence Gateways .......................................................................... 154
Cisco IR1101 as RPoP Gateway ................................................................................... 154
Cisco CGR1240 as RPoP Gateway .............................................................................. 155
Remote Point-of-Presence Design Considerations .................................................... 155
RPoP Multiservice design in IR1101 .......................................................................... 155
RPoP Macro–Segmentation Design in IR1101 ............................................................. 156
RPoP High Availability Design ................................................................................... 158
CCI HER Redundancy .................................................................................................. 159
WAN Backhaul Redundancy ....................................................................................... 160
Combined Redundancy ............................................................................................... 161
RPoP Gateways Management ..................................................................................... 162
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validated Use Case Solutions</td>
<td>163</td>
</tr>
<tr>
<td>Smart Street Lighting CR-Mesh Solution with CCI Network</td>
<td>163</td>
</tr>
<tr>
<td>Public Cloud</td>
<td>163</td>
</tr>
<tr>
<td>CIMCON LightingGale</td>
<td>163</td>
</tr>
<tr>
<td>Software Upgrade</td>
<td>164</td>
</tr>
<tr>
<td>Template Management</td>
<td>164</td>
</tr>
<tr>
<td>Smart Street Light Controller (SLC)</td>
<td>164</td>
</tr>
<tr>
<td>CR-Mesh Access Network for CIMCON</td>
<td>164</td>
</tr>
<tr>
<td>CIMCON Smart Street Light over CCI CR-Mesh Access Network PoP</td>
<td>165</td>
</tr>
<tr>
<td>CIMCON Smart Street Light over CCI CR-Mesh Access Network RPoP</td>
<td>166</td>
</tr>
<tr>
<td>CIMCON System Scale</td>
<td>166</td>
</tr>
<tr>
<td>Cisco Kinetic for Cities (CKC)</td>
<td>166</td>
</tr>
<tr>
<td>Public Wi-Fi services with CCI Wi-Fi</td>
<td>167</td>
</tr>
<tr>
<td>Municipality-wide SSID</td>
<td>167</td>
</tr>
<tr>
<td>Captive Portal</td>
<td>167</td>
</tr>
<tr>
<td>Traffic separated from rest of network</td>
<td>167</td>
</tr>
<tr>
<td>Client Roaming</td>
<td>168</td>
</tr>
<tr>
<td>Analytics and Insights</td>
<td>168</td>
</tr>
<tr>
<td>Outdoor Wi-Fi as a sensor, with CCI Wi-Fi</td>
<td>168</td>
</tr>
<tr>
<td>Outdoor IP Camera with CCI Wi-Fi</td>
<td>168</td>
</tr>
<tr>
<td>Power</td>
<td>169</td>
</tr>
<tr>
<td>Connectivity</td>
<td>169</td>
</tr>
<tr>
<td>Segmentation</td>
<td>169</td>
</tr>
<tr>
<td>Safety and Security Solution with CCI</td>
<td>169</td>
</tr>
<tr>
<td>Supervisory Control and Data Acquisition (SCADA) Networking over CCI</td>
<td>169</td>
</tr>
<tr>
<td>CR-Mesh Backhaul Design Considerations</td>
<td>173</td>
</tr>
<tr>
<td>Cellular Backhaul Design Considerations</td>
<td>174</td>
</tr>
<tr>
<td>FlashNet Lighting LoRaWAN solution over CCI</td>
<td>175</td>
</tr>
<tr>
<td>Water Monitoring Sensor Technologies</td>
<td>175</td>
</tr>
<tr>
<td>Axis Camera Onboarding and Integration over CCI</td>
<td>176</td>
</tr>
<tr>
<td>Axis Components in CCI</td>
<td>176</td>
</tr>
<tr>
<td>Axis Camera Onboarding in CCI</td>
<td>177</td>
</tr>
<tr>
<td>Conclusions</td>
<td>182</td>
</tr>
<tr>
<td>Acronyms and Initialisms</td>
<td>183</td>
</tr>
</tbody>
</table>
Modernizing the technology landscape of our cities, communities, and roadways is critical. Efforts toward digital transformation will form the basis for future sustainability, economic strength, operational efficiency, improved livability, public safety, and general appeal for new investment and talent. Yet these efforts can be complex and challenging. What we need is a different approach to address the growing number of connected services, systems, devices, and their volumes of data. Overwhelming options for connecting new technologies make decision-making more difficult and present risks that often seem greater than the reward. This approach will require a strategic and unified consideration of the broad needs across organizational goals and the evolving nature of the underlying technology solutions.

Typically, multiple connectivity solutions are traditionally created as separate and isolated networks. This leads to duplication of infrastructure and effort and cost, inefficient management practices, and less assurance for security and resiliency. Traditional networking also commonly manages on a per-device basis, which takes time, creates unnecessary complexities, and heightens exposure to costly human errors.

With Cisco Connected Communities Infrastructure (CCI), you can create a single, secure communications network to support all your needs that is simpler to deploy, manage and secure. Based on the market-defining Cisco Digital Network Architecture (Cisco DNA) and Intent-based Networking capabilities, this solution provides:

- A single, modular network with wired (fiber, Ethernet), wireless (Wi-Fi, cellular, and V2X) and Internet of Things (IoT) communications (LoRaWAN and Wi-SUN mesh) connectivity options for unmatched deployment flexibility
- Cisco Software-Defined Access (SD-Access) to virtually segment and secure your network across departments and services, each with its own policies, control, and management as needed
- Cisco DNA Center for network automation with unified management of communications policy and security that significantly lowers operational costs; Cisco DNA Center also provides assistance in security compliance, which is becoming a significant challenge for our customers to prove
- Highly reliable outdoor and ruggedized networking equipment with simplified zero-touch in-street and roadway deployment options

For additional overview materials, presentations, blogs and links to other higher-level information on Cisco’s Connected Communities Infrastructure solution please see: [http://cisco.com/go/cci](http://cisco.com/go/cci)

**Scope of CCI Release 2.0**

This Design Guide provides network architecture and design guidance for the planning and subsequent implementation of a Cisco Connected Communities Infrastructure solution. In addition to this Design Guide, there is also a Connected Communities Infrastructure Implementation Guide that provides more specific implementation and configuration guidance and examples also exists.

For Release 2.0 of the CCI CVD, the horizontal scope covers all the access technologies listed in [Cisco Connected Communities Infrastructure, page 4](#). For V2X, this CVD release specifically covers Dedicated Short-Range Communications (DSRC).

This Release 2.0 supersedes and replaces the CCI Release 1.1 Design Guide.
New capabilities in CCI Release 2.0

- Supervisory control and data acquisition (SCADA) design
- New use cases:
  - SCADA Water
  - LoRaWAN Water Level and Flood Monitoring
  - LoRaWAN Lighting
  - Camera Auto Provisioning
  - Rail Trackside Roaming
- CR-Mesh / WiSUN Mesh updates
  - Orthogonal frequency-division multiplexing (OFDM) design
  - OFDM and FSK interoperability
  - Connected grid endpoint (CGE) compatibility guidance
- Cisco Flexible NetFlow and Stealthwatch in CCI Security
  - Flow Data Collection using Flexible NetFlow
  - Abnormal, malicious traffic and malware detection & malicious host quarantine
- Enhanced End-to-End QoS design
- Enhanced Remote Point-of-Presence (RPoP) design
  - IR1101 as RPoP gateway with multi-service and macro-segmentation at RPoP
  - IR1101 as RPoP gateway with Dual LTEs for WAN High Availability
- Solution enhancements: LoRaWAN updates, major software releases including FND 4.6 with OTA CGE updates and IDA gateway management

References

For associated deployment and implementation guides, related Design Guides, and white papers, see the following pages:

- Cisco Connected Communities Infrastructure: https://cisco.com/go/connected-communities-infrastructure
- Cisco Cities and Communities: https://cisco.com/go/smartconnectedcommunities
- Cisco Connected Roadways: https://cisco.com/go/connectedroadways
- Cisco Connected Community Infrastructure Design Guides: https://www.cisco.com/go/designzone
- Cisco IoT Solutions Design Guides: https://www.cisco.com/go/iotcvd

Customers and partners with an appropriate Cisco Account (CCO account) can access additional CCI sales collaterals and technical presentations via the CCI Sales Connect hub: https://salesconnect.cisco.com/#/program/PAGE-15434.
## Document Organization

The following table describes the chapters in this document:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Solution Overview, page 4</strong></td>
<td>Overview of the solution, including use cases and unique selling points</td>
</tr>
<tr>
<td><strong>Solution Architecture, page 7</strong></td>
<td>Describes architecture, building blocks, SD-Access fabric, access networks and edge compute, Next-Generation Firewall (NGFW) and De-militarized Zone (DMZ) network, and common infrastructure and shared services.</td>
</tr>
<tr>
<td><strong>Solution Components, page 34</strong></td>
<td>Describes the components in the CCI solution, including Policy Design and Network QoS Design.</td>
</tr>
<tr>
<td><strong>CCI Security Architecture and Design Considerations, page 38</strong></td>
<td>Describes the CCI Security Architecture and Design Considerations for network and endpoint security.</td>
</tr>
<tr>
<td><strong>CCI Network QoS Design, page 48</strong></td>
<td>Describes the Quality-of-Service (QoS) design considerations for the CCI network architecture.</td>
</tr>
<tr>
<td><strong>CCI Network Data Flow Diagrams, page 67</strong></td>
<td>Provides a pictorial representation of device and client onboarding data flows and east–west and south–north data flows, along with the role of different network components on the path.</td>
</tr>
<tr>
<td><strong>CCI Network High Availability, page 81</strong></td>
<td>Discusses High-Availability (HA)/redundancy design for the entire solution.</td>
</tr>
<tr>
<td><strong>CCI Network Scale and Dimensioning, page 86</strong></td>
<td>Illustrates scaling considerations and available options at different layers of the network and provides steps for computing dimensions for an CCI network deployment.</td>
</tr>
<tr>
<td><strong>CCI Ethernet Access Network Solution, page 93</strong></td>
<td>Discusses design of the CCI Ethernet Access Network for endpoint connectivity.</td>
</tr>
<tr>
<td><strong>CCI Wi-Fi Access Network Solution, page 96</strong></td>
<td>Discusses design of the CCI Wi-Fi Access Network for Wi-Fi client connectivity.</td>
</tr>
<tr>
<td><strong>CCI DSRC Access Network Solution, page 120</strong></td>
<td>This chapter discusses design of the CCI DSRC Access Network for endpoint connectivity.</td>
</tr>
<tr>
<td><strong>CCI LoRaWAN Access Network Solution, page 128</strong></td>
<td>This chapter discusses design of the CCI LoRaWAN Access Network for endpoint connectivity.</td>
</tr>
<tr>
<td><strong>CCI Rail Trackside Access Network Solution, page 136</strong></td>
<td>This chapter describes design of the CCI Rail Trackside Access Network for endpoint connectivity.</td>
</tr>
<tr>
<td><strong>Fluidmesh and CCI Network Integration and Considerations, page 146</strong></td>
<td>This chapter discusses the integration considerations for Fluidmesh network with CCI.</td>
</tr>
<tr>
<td><strong>CCI Remote Point-of-Presence Design, page 154</strong></td>
<td>This chapter discusses the design of CCI Remote Point-of-Presence (RPoP) for secure, multi-service and highly available RPoP connectivity to CCI network.</td>
</tr>
<tr>
<td><strong>Validated Use Case Solutions, page 163</strong></td>
<td>This chapter describes CCI Validated Use Case Solutions like Smart Street Lighting, Public Wi-Fi services and IP security camera with CCI Wi-Fi and CCI Safety and Security solution</td>
</tr>
<tr>
<td><strong>Conclusions, page 182</strong></td>
<td>This chapter recaps the major features of this solution.</td>
</tr>
<tr>
<td><strong>Acronyms and Initialisms, page 183</strong></td>
<td>This appendix lists the acronyms and initialisms used in this document.</td>
</tr>
</tbody>
</table>
Solution Overview

This chapter includes the following major topics:

- Cisco Connected Communities Infrastructure, page 4
- CCI Network Architecture, page 4
- CCI Validated Use Case Solutions, page 5
- CCI Unique Selling Points, page 5

Cisco Connected Communities Infrastructure

The Cisco CCI Cisco Validated Design (CVD) is a network for Campus/Metropolitan area/Geographic region/Roadways. It delivers an Intent-based Networking solution by leveraging Cisco’s Software-defined Access (SD-Access) with the Cisco DNA Center management and Identity Services Engine (ISE), along with ruggedized edge hardware, to enable a scalable, segmented, and secure set of services to be deployed:

- Overlay network(s) for segmentation and policy enforcement
- Underlay network for basic IP forwarding and connectivity
- Access to the Overlay Fabric via Industrial Ethernet (IE) switches as Extended Nodes (EN) and Policy Extended Nodes (PEN)
- Services delivered are a mix of standard enterprise and IoT specialized
- Deployable in modules
- Multiple access technologies are catered for; specifically:
  - Wired Ethernet
  - Wi-Fi
  - Long Range WAN (LoRaWAN)
  - Cisco Resilient Mesh (CR-Mesh) / Wi-SUN
  - Vehicle-to-Infrastructure (V2X)
  - Cisco Fluidmesh Wireless
- Three options for backhaul:
  - Fiber
  - Multiprotocol Label Switching (MPLS)
  - VPN over Public Internet (typically Cellular or xDSL)

CCI Network Architecture

The CCI Network Architecture is a horizontal architecture. Instead of being in support of a specific, limited vertical set of use cases, CCI facilitates many different use cases and verticals. Some of these you will find examples of in this Design Guide, but in general, CCI is non-prescriptive as to what applications and use cases customers can achieve using CCI.

The CCI Network Architecture helps customers design a multi-service network that can be distributed over a large geographical area with a single policy plane, offers multiple access technologies, and is segmented end to end.
Solution Overview

CCI Validated Use Case Solutions

As discussed in CCI Network Architecture, page 4, CCI can be used as an architecture to deliver a variety of use cases. CCI is agnostic to any particular use case(s) and enables multiple use cases to be delivered in parallel. Each use case can use a fundamentally different or multiple access technologies and/or can be effectively isolated within the CCI multi-service network using segmentation.

CCI Unique Selling Points

CCI leverages Cisco DNA Center to provide a next generation management experience: streamlining network device onboarding, providing security, and troubleshooting. In some use cases, additional management applications may also be used to provide a specialized management experience for example, Cisco Field Network Director (FND) or Actility ThingPark Enterprise.

CCI also leverages Cisco SD-Access and ISE with Scalable Group Tags (SGTs) to allow end-to-end network segmentation and policy control across multiple access technologies, various network devices, and physical locations. Cisco DNA Center and SD-Access together allow the customer to take an Intent-based Networking approach, which is to be concerned less with the IT networking and more with the operational technology/line-of-business (OT/LOB) requirements:

“I need to extend connectivity for smart parking to a different part of my city, but I want the existing policies to be used.” – CCI helps enable you to do this.

“I need to add a weather stations along my roadway, but they need to be segregated from the tolling infrastructure.” – CCI helps enable you to do this.

CCI gives you the end-to-end segmentation, made easy through Software-Defined Access, for provisioning, automation, and assurance at scale. Distributing IP subnets across a large geographical area is made simpler than ever before.
Solution Architecture

This chapter includes the following major topics:

- CCI Overall Network Architecture, page 7
- CCI Major Building Blocks, page 8
- CCI’s Cisco Software-Defined Access Fabric, page 14
- Access Networks and Edge Compute, page 24
- Next-Generation Firewall (NGFW) and DMZ Network, page 25
- Common Infrastructure and Shared Services, page 27

CCI Overall Network Architecture

CCI comprises the building blocks shown in Figure 3 and Figure 4.

CCI Modularity

The intent of this CVD is to provide the reader with the best infrastructure guidance for where they are today. Each layer of the CCI architecture is designed to be consumed in modules. The reader only needs to deploy the access technologies that are relevant for them and can add other network access technologies as needed.

CCI brings intent-based networking out to fiber-connected locations (Points of Presence (PoPs)) and VPN-connected locations (Remote Points of Presence (RPoPs)); all of these locations connect back to some centralized infrastructure via a backhaul, which is where they also access the Internet.
Additional access technologies, such as Wi-Fi, LoRaWAN, CR-Mesh and V2X, can similarly be implemented in a modular approach and will leverage the connectivity provided by CCIs PoPs and RPoPs.

CCI Major Building Blocks

With reference to Figure 3 and Figure 4, what follows is a detailed description of the major building blocks of which CCI is comprised, in terms of the functions, the quantities, the hardware, and interconnection between blocks.

Centralized Infrastructure

Qty 1 of Centralized Infrastructure:

Designs are based on a centralized infrastructure at a single physical site/location. CCI 2.0 works within the boundaries and design rules for SD-Access 2.1.2.0. For more information, please refer to the Cisco Validated Design Software-Defined Access Design Guide at the following URL:


The Centralized Infrastructure is comprised of:

- Qty 1 of Application Servers, which are comprised of DC-specific networking, compute, and storage.
The following are required:

- Cisco UCS 6300 Series Fabric Interconnects (FI) (as resilient pair(s)) to provide Data Communications Equipment (DCE) and management of Cisco Unified Computing System (UCS).
- Cisco Nexus 5600 converged DC switches to provide Fiber Channel (FC), Fiber Channel over Ethernet (FCoE), and IP.
- Cisco UCS B and C-series servers connected at a minimum of 10Gbps to FIs.
- Storage, connected at a minimum of 8Gbps to Nexus, via FC, FCoE, or Internet Small Computer Systems Interface (iSCSI).

**Note:** Application Layer may optionally be entirely delivered from the Public Cloud; if so, no on-premises Application Server infrastructure is required.

**Qty 1 of Super Core,** which is comprised of a pair of suitably sized Layer 3 boxes, which provide resilient core and fusion routing capabilities; note that these may be switches even though they are routing.
The Super Core connects to multiple components and this should be as resilient $\geq 10$Gbps L3 links:

- Shared Services
- DMZ and Internet
- Application Servers
- Point of Presence (PoP) Backhaul

**Qty 1 of De-militarized Zone (DMZ) and Internet:**
DMZ is comprised of resilient pairs/clusters of firewalls on both the Internet and DMZ sides, and also a resilient pair/cluster of IPSec headend routers for FlexVPN tunnel termination:

- DMZ can optionally contain other servers/appliances that are required by customer for various use cases.

- Qty 1 of Internet connection:
  - Internet should ideally connect from two different ISPs, or separate A and B connections from a single ISP.

**Qty 1 of Shared Services:**

- Qty 1 DNA-C cluster (1 or 3 appliances)
- Qty ≥ 1 ISE PAN
- Qty ≥ 1 ISE PSN
- Qty 1 IPAM

**Point of Presence (PoP)**

**Qty ≤ 499 of Point(s) of Presence**

PoPs are typically required, although in some deployments of CCI no PoPs may be required. Note that, a CCI deployment may consist entirely of Remote PoPs (RPoPs) if all-cellular connectivity is used for backhaul.
Points of Presence are comprised of:

- **Qty 1 of PoP Distribution Infrastructure:**
  - Distribution Infrastructure is comprised of Cisco Catalyst 9000-series switches that are capable of being Fabric in a Box (FiaB); typically 2 x Catalyst 9300 in a physical stack or 2 x Catalyst 9500 switches in a virtual stack (n.b. only the non-High-performance variants of the Catalyst 9500 family are supported).
  - Multi-chassis EtherChannel (MEC) is employed for downlinks to Extended Nodes (ENs) and Policy Extended Nodes (PENs)
  - Layer 3 P2P uplinks used for connection to the backhaul:
    - to PE routers, in the case of IP Transit (likely SP MPLS)
    - to (likely) Catalyst 9500s, in the case of SD-Access Transit, over dark fiber (or equivalent)

- **Qty ≥ 1 Access Rings**, which are comprised of:
  - Qty 2 Cisco Industrial Ethernet (IE) switches as extended nodes or policy extended nodes; these switches are either end of a closed Resilient Ethernet Protocol (REP) ring, plus
  - Qty ≥ 1 ≤ 29 Cisco Industrial Ethernet (IE) switches as DNA-C–managed switches (but they are not extended nodes nor part of a Fabric). For more detail, please see Extended Nodes and Policy Extended Nodes, page 19.
  - IE switches are connected together in a closed ring topology via fiber or copper Small Form-Factor Pluggables (SFP).

- **Qty 2 SFP** per switch for a 1Gbps ring:
Extended nodes and/or Policy Extended Nodes are connected to uplink Catalyst 9300 stack or Catalyst C9500 StackWise Virtual switches via fiber or copper (Note: only the non-High-performance variants of the Catalyst 9500 family are supported):

- A ring can be comprised uniformly of all IE-3300, Cisco Embedded Services 3300 Series switches (ESS 3300), IE-4000, or IE-5000 switches, or a mixture of these switches; each operating as Extended Nodes
- A ring can alternatively be comprised exclusively of all IE-3400 switches, these operating as Policy Extended Nodes.
  - **Note:** It is not recommended to mix PENs and ENs in the same access ring.
- Per Figure 8, nodes of the ring not directly connected to the FiaB are either Daisy-Chained Extended nodes (DC-EN) or Daisy-Chained Policy Extended Nodes (DC-PENs) provisioned through Cisco DNA Center Day N templates, but Cisco Industrial Ethernet (IE) switches directly connected into the Catalyst 9300 stack or Catalyst 9500 StackWise Virtual (FiaB), are only shown as Extended nodes in SD Access fabric in Cisco DNA Center UI. Please note that it is not possible to mix PENs and ENs in the same access ring.
- SR or LR SFPs can be used, giving fiber distances of <100m to 70km, with RGD optics allowing deployment in the ~40 degrees centigrade +85 degrees centigrade temperature range.
  - **Note:** Although the SFPs have this operating temperature range, the real-world operating temperature range will be determined by a number of factors, including the operating temperature range of the switches they are plugged into.
  - Different segments of a ring can be different physical lengths/distances and fiber types.

### Backhaul for Points of Presence

To connect the PoPs back to the Centralized Infrastructure, a Metropolitan Area Network (MAN) is used.

**Figure 9  Backhaul for Points of Presence**

When deploying CCI, you may have access to dark fiber, in which case you can build your own MAN, which is a transparent backhaul entirely within the SD-Access fabric domain that uses SD-Access Transit. Alternatively, or additionally, an SP might be involved or you might have your own MPLS network; this is an opaque backhaul and the traffic must leave the SD-Access fabric domain on an IP Transit and come back into the SD-Access fabric domain at the far side.

- Qty 0 or 1 SD-Access Transit
Solution Architecture

- Qty 0 or 1 IP Transit

Remote Point of Presence (RPoP)

- Qty $\leq 1000$ of Remote Points-of-Presence (RPoPs); although in some deployments of CCI no RPoPs may be required.

- An RPoP is a Connected Grid Router (CGR) or Cisco Industrial Router (IR) and is typically connected to the Public Internet via a cellular connection (although any suitable connection can be used (such as xDSL or Ethernet), over which FlexVPN secure tunnels are established to the HE in the DMZ.

- The RPoP router may provide enough local LAN connectivity, or an additional Cisco Industrial Ethernet (IE) switch may be required.

CCI's Cisco Software-Defined Access Fabric

The SD-Access Fabric Network Layers of CCI

The CCI Network design based on the SD-Access framework follows the design principles and best practices associated with a hierarchical design by splitting the network into modular groups, as described in the Campus LAN and Wireless LAN Design Guide. The modular building blocks can be replicated, which makes it an optimal and scalable architecture. The network is a multi-tier architecture with access, distribution, core, data center, application server, DMZ, and Internet layers. The overall CCI network architecture with IP Transit is shown in Figure 10.

At the heart of the CCI network is the Cisco DNA Center with SD-Access, which is the single-pane-of-glass management and automation system. The CCI network spreads across a large geographical area, logically divided into several PoPs. Each PoP is designed as a fabric site.

Each fabric site (PoP) consists of the Fabric in a Box (FiaB), which is a consolidated fabric node. FiaB plays the role of a distribution layer by consolidating the access layer traffic and acting as the fabric site gateway to the core. The access layer consists of one or more REP rings of Cisco Industrial Ethernet Switches.

Multiple fabric sites across the city or along the roadway are interconnected by either SD-Access Transit or IP Transit to give a multi-site/distributed topology. A CCI Network deployment can have IP Transit or SD-Access Transit or both. The CCI Network Design with IP Transit, page 14 illustrates a CCI Network design with only IP Transit, whereas The CCI Network Design having both SD-Access and IP Transit, page 15 shows a CCI Network design with both SD-Access transit and IP-Transit.

A fusion router interconnects the fabric and all fabric sites with the shared services and Internet.

The application servers are hosted in an exclusive fabric site for end-to-end segmentation. The Internet breakout is centralized across all the fabric sites and passes through the firewall at the DMZ. The Cisco DNA Center needs to have Internet access for regular cloud updates. Important design considerations such as redundancy, load balancing, and fast convergence are to be ensured at every layer/critical node/critical link of the network. This will ensure uninterrupted service and optimal usage of the network resources.

Upcoming sections in this document elaborate each of these components. For more information, please refer to the Campus LAN and Wireless LAN Design Guide at the following URL:


The CCI Network Design with IP Transit

Figure 10 shows the CCI Network design with IP Transit. Multiple network sites (PoP locations) are interconnected by an IP/MPLS backbone configured by SD-Access as IP Transit. IP Transit Network, page 23 elaborates on IP Transit.
The CCI Network Design having both SD-Access and IP Transit

Figure 11 shows the CCI Network design having both SD-Access and IP Transit. The network sites that have a campus like connectivity (high speed, low latency, and Jumbo MTU support) with Cisco DNA Center are interconnected with SD-Access Transit. The network sites that have a WAN like IP/MPLS backbone are interconnected with IP Transit. A core device called a Fusion Router interconnects shared services and Internet to all fabric sites in the network, regardless of their backhaul.
In order to set up an SD-Access-managed network, all managed devices need to be connected with a routed underlay network, thus being IP reachable from the Cisco DNA Center. This underlay network can be configured manually or with the help of the Cisco DNA Center LAN Automation feature. Note that Cisco DNA Center LAN automation has a maximum limit of two hops from the configured seed devices and does not support Cisco Industrial Ethernet (IE) Switches. Because the CCI network has Cisco Industrial Ethernet (IE) switches and most CCI network deployments will have more than two hops, manual underlay configuration is recommended for CCI.

The SD-Access design recommendation is that the underlay should preferably be an IS-IS routed network. While other routing protocols can be used, IS-IS provides unique operational advantages such as neighbor establishment without IP protocol dependencies, peering capability using loopback addresses, and agnostic treatment of IPv4, IPv6, and non-IP traffic. It also deploys both a unicast and multicast routing configuration in the underlay, aiding traffic delivery efficiency for services built on top. However, other routing protocols such as Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF) can also be deployed, but these may require additional configuration.

Underlay connectivity spans across the fabrics, covering Fabric Border Node (BN), Fabric Control Plane (CP) node, Intermediate nodes, and Fabric Edges (FE). Underlay also connects the Cisco DNA Center, Cisco ISE, and the fusion router. However, all endpoint subnets are part of the overlay network.

Note: The underlay network for the SD Access fabric requires increased MTU to accommodate additional overlay fabric encapsulation header bytes. Hence, you must increase the default MTU to 9100 bytes to ensure that Ethernet jumbo frames can be transported without fragmentation inside the fabric.

Refer to the SD-Access Design and Deployment Guides for further underlay design and deployment details.
Overlay Network

An SD-Access fabric creates virtualized networks (VNs) on top of the physical underlay network, called overlay. These VNs can span the entire fabric and remain completely isolated from each other. The entire overlay traffic, including data plane and control plane, are contained fully within each VN. The boundaries for the fabric are the BN and FE nodes. BN is the ingress and egress point to the fabric, FE is the entry point for wired clients, and Fabric Wi-Fi AP is the entry point for Wi-Fi wireless clients.

The VNs are realized by virtual routing and forwarding (VRF) instances and each VN appears as a separate instance for connectivity to the external network. SD-Access overlay can be either Layer 2 overlay or Layer 3. For the CCI network, Layer 3 overlay is chosen as the default option. The Layer 3 overlay allows multiple IP networks as part of each VN. Overlapping IP address space across different Layer 3 overlays is not recommended in the CCI network for administrative convenience and to avoid the need for network address translation (NAT) for shared services that span across VNs.

Within the SD-Access fabric, the user and control data are encapsulated and transported using the overlay network. The encapsulation header carries the virtual network and SGT information, which is used for traffic segmentation within the overlay network.

Segmentation allows granular data plane isolation between groups of endpoints within a VN and allows simple-to-manage group-based policies for selective access. The SGTs also aid scalable deployment of policy avoiding cumbersome IP-based policies.

VNs provide macro-segmentation by isolation of both data and control plane, whereas segmentation with SGT provides micro-segmentation by selective separation of groups within a VN.

By default, no communication between VNs is possible. If communication is needed across VNs, a fusion router outside the fabric can be employed with appropriate “route-leaking” configuration for selective inter-VN traffic communication; however, communication within a VN (same or different SGT) is routed within the fabric.

Following the SD-Access design recommendations, minimizing the number of IP subnets is advised to simplify the Dynamic Host Configuration Protocol (DHCP) management. The IP subnets can be stretched across a fabric site without any flooding concerns, unlike large Layer 2 networks. IP subnets should be sized according to the services that they support across the fabric. However, based on the deployment needs of enabling optional broadcast feature, the subnet size can be limited. In this context, a “service” may be a use case: for example, how many IPv4 Closed Circuit Television (CCTV) cameras am I going to deploy across my entire city (now and into the future), and how many back-end servers in my DC do I need to support them?

Fabric Data Plane and Control Plane

This section provides a detailed explanation of how the fabric data and control plane work. All of this is automated by SDA and largely hidden from the administrator; therefore, this section can be skipped unless the reader wishes to go very deep.

Within the SD-Access fabric, SD-Access configures the overlay with fabric data plane by using Virtual Extensible LAN (VXLAN). RFC 7348 defines the use of VXLAN as a way to overlay a Layer 2 network on top of a Layer 3 network. VXLAN encapsulates and transports Layer 2 frames across the underlay using UDP/IP over Layer 3 overlay. Each overlay network is called a VXLAN segment and is identified by a VXLAN Network Identifier (VNI). The VXLAN header carries VNI and SGT needed for macro- and micro-segmentation. Each VN maps to a VNI, which, in turn, maps to a VRF in the Layer 3 overlay.

Along with VXLAN data plane, SD-Access uses Location/IP Separation Protocol (LISP) as control plane. From a data plane perspective, each VNI maps to a LISP Instance ID. LISP helps to resolve endpoint-to-location mapping. LISP does perform routing based on End Point Identifier (EID) and Routing Locator (RLOC) IP addresses. An EID could be either an endpoint IP address or MAC. An RLOC is part of underlay routing domain, which is typically the Loopback address of the FE node to which the EID is attached. The RLOC represents the physical location of the endpoint. The combination of EID and RLOC gives device ID and location; thus, the device can be reached even if it moves to a different location with no IP change. The RLOC interface is the only routable address that is required to establish connectivity between endpoints of the same or different subnets.
Within the SD-Access fabric, LISP provides control plane forwarding information; therefore, no other routing table is needed. To communicate external to the SD-Access fabric, at the border each VN maps to a VRF instance. Outside the fabric path, isolation techniques such as VRF-Lite or MPLS may be used to maintain the isolation between VRFs. EIDs can be redistributed into a routing protocol such as Border Gateway Protocol (BGP), EIGRP, or OSPF for use in extending the virtual networks.

To provide forwarding information, LISP map server, located on the CP node, maintains EID (host IP/MAC) to RLOC mapping in its map-server. The local node queries the control plane to fetch the destination EID route.

Fabric Border

Figure 12 depicts different fabric roles and terminology in Cisco SD-Access design. Fabric Border (BN) is the entry and exit gateway between the SD-Access fabric site and networks external to the fabric site. Depending on the types of outside networks it connects to, BN nodes can be configured in three different roles: Internal Border (IB), External Border (EB), and Anywhere Border (AB). The IB connects the fabric site to known areas internal to the organization such as the data center (DC) and application services. The EB connects a fabric site to a transit as an exit path for the fabric site to outside world, including other fabric sites and the Internet. AB, however, connects the fabric site to both internal and external locations of the organization. The aggregation point for the exiting traffic from the fabric should be planned as the border; traffic exiting the border and doubling back to the actual aggregation point results in sub-optimal routing. In CCI, each PoP site border is configured with EB role connecting to a transit site and HQ/DC fabric site border is configured with AB role to provide connectivity to internal and external locations.

In general, the fabric BN is responsible for network virtualization interworking and SGT propagation from the fabric to the rest of the network. The specific functionality of the BN includes:

- Gateway for the fabric to reach the world outside the fabric
- Advertising EID subnets of the fabric to networks outside the fabric for them to communicate with the hosts of the fabric, via BGP
- Mapping LISP instances to VRF instances to preserve the virtualization
- Propagating SGT to the external network either by transporting tags using SGT Exchange Protocol (SXP) to Cisco TrustSec-aware devices or using inline tagging in the packet
Solution Architecture

The EID prefixes appear only on the routing tables at the border; throughout the rest of the fabric, the EID information is accessed using the fabric control plane (CP).

Fabric Edge

Fabric edge nodes (FEs) are access layer devices that provide Layer 3 network connectivity to end-hosts or clients addressed as endpoints. The fundamental functions of FE nodes include endpoint registration, mapping endpoints to virtual networks, and segmentation and application/QoS policy enforcement.

Endpoints are mapped to VN by assigning the endpoints to a VLAN associated to a LISP instance. This mapping of endpoints to VLANs can be done statically (in the Cisco DNA Center user interface) or dynamically (using 802.1X and MAB). Along with the VLAN, an SGT is also assigned, which is used to provide segmentation and policy enforcement at the FE node.

Once a new endpoint is detected by the FE node, it is added to a local host tracking database EID-Table. The FE node also issues a map-registration message to the LISP map-server on the control plane node to populate the Host Tracking Database (HTDB).

On receipt of a packet at the FE node, a search is made in its local host tracking database (LISP map-cache) to get the RLOC associated with the destination EID. In case of a miss, it queries the map-server on the control plane node to get the RLOC. In case of a failure to resolve the destination RLOC, the packet is sent to the default fabric border. The border forwards the traffic using its global routing table.

If the RLOC is obtained, the FE node uses the RLOC associated with the destination IP address to encapsulate the traffic with VXLAN headers. Similarly, VXLAN traffic received at a destination RLOC is de-encapsulated by the destination FE.

If traffic is received at the FE node for an endpoint not locally connected, a LISP solicit-map-request is sent to the sending FE node to trigger a new map request; this addresses the case where the endpoint may be present on a different FE switch.

Fabric-in-a-Box (FiaB)

For smaller fabric sites, such as a CCI PoP, all three fabric functions (Border, Control, and Edge) can be hosted in the same physical network device; this is known as “Fabric in a Box” (FiaB).

In the current release of CCI, the FiaB model is recommended based on the size of the network and size of the traffic to be supported from a fabric site. For size calculations, see CCI Network Access Layer Dimensioning, page 89.

Extended Nodes and Policy Extended Nodes

Extended Node

The SD-Access fabric can be extended with the help of extended nodes. Extended nodes are access layer Ruggedized Ethernet switches that are connected directly to the Fabric Edge/FiaB. The list of DNA Center 2.1.2-supported extended node devices used in CCI network include the Cisco IE 4000 series, the Cisco IE 5000 series switches the Cisco IE3300 series switches and the Cisco ESS 3300 switches.

Cisco IE3400 series switches can be configured as Policy Extended Node (PEN) being a superset of Extended Node. Refer to the “Policy Extended Node, page 20” section below for more details on IE3400 switches role in CCI PoP. These Ruggedized Ethernet switches are connected to the Fabric Edge or FiaB in a daisy-chained ring topology for Ethernet access network high availability. Refer to the section “Ethernet Access Network, page 93” in this document, for more details on Ethernet access ring topology design in CCI.

Extended nodes support VN based macro-segmentation in the Ethernet access ring. These devices do not natively support fabric technology. Therefore, policy enforcement for the traffic generated from the extended node devices is done by SD-Access at the Fabric Edge.
The Cisco Industrial Ethernet (IE) switches (IE4000, IE5000, IE3300, and ESS 3300 Series) in the ring connected directly to the Fabric Edge/FiaB are referred as extended nodes (EN) and the Cisco Industrial Ethernet (IE) switches which are indirectly connected to Fabric Edge/FiaB via daisy-chained ring topology are referred as Daisy-Chained Extended Nodes (DC-EN). The DC-EN switches in the Ethernet access ring topology are discovered and provisioned using CLI templates feature in Cisco DNA Center. Refer to the chapter, “Create Templates to Automate Device Configuration Changes” at the following URL for more details on CLI aka Day N templates in Cisco DNA Center.


The ENs do all of the endpoint onboarding connected to its ports, but policy is applied only to traffic passing through the FE/FiaB nodes. The extended nodes support 802.1X or MAB based Closed Authentication for Host Onboarding in Cisco DNA Center Fabric provisioning. However, the closed authentication (802.1X or MAB) configuration for DC-ENs in the ring, are provisioned using Day N templates.

The rationale for recommending ring topology with REP for Cisco Industrial Ethernet (IE) switches to provide Ethernet access is discussed in Ethernet Access Network, page 93. Both ends of REP ring are terminated at FE/FiaB, such that all Cisco Industrial Ethernet (IE) switches in the ring and FiaB are part of closed REP segment.

Policy Extended Node

Cisco DNA Center 2.1.2 also supports “Policy Extended Node” which is a construct at Ethernet access ring capable of doing group based micro-segmentation for improved Ethernet access ring security. Cisco IE3400 series switches support this functionality with Network Advantage and DNA Advantage licenses. IE3400 switches must have Network Advantage and DNA advantage licenses to operate as Policy Extended Node. The policy extended nodes are capable of doing Scalable Group Tag (SGT) based inline tagging and enforcing SGACL based security policies for device to device communication within a VN or domain.

The IE3400 series switches in the Ethernet access ring connected directly to the Fabric Edge/FiaB are referred as Policy Extended Nodes (PEN). The IE3400 switches which are indirectly connected to Fabric Edge/FiaB via daisy-chained ring topology are referred as Daisy-Chained Policy Extended Nodes (DC-PEN). These DC-PENs in the ring are discovered and provisioned using Day N templates in Cisco DNA Center.

Cisco TrustSec (CTS) architecture consists of authentication, authorization and services modules like guest access, device profiling etc., TrustSec is an umbrella term and it covers anything to do with endpoint’s identity, in terms of IEEE 802.1X (dot1x), profiling technologies, guest services, Scalable Group based Access (SGA) and MACSec (802.1AE). CTS simplifies the provisioning and management of secure access to network services and applications. Compared to access control mechanisms that are based on network topology, Cisco TrustSec defines policies using logical policy groupings, so secure access is consistently maintained even as resources are moved in mobile and virtualized networks.

CTS classification and policy enforcement functions are embedded in Cisco switching, routing, wireless LAN, and firewall products. By classifying traffic based on the contextual identity of the endpoint versus its IP address, Cisco TrustSec enables more flexible access controls for dynamic networking environments. At the point of network access, a Cisco TrustSec policy group called a Security Group Tag (SGT) is assigned to an endpoint, typically based on that endpoint’s user, device, and location attributes. The SGT denotes the endpoint’s access entitlements, and all traffic from the endpoint will carry the SGT information.

The PEN supports CTS and 802.1X or MAB based Closed Authentication for host onboarding along with dynamic VLAN and SGT attributes assignment for endpoints, in Cisco DNA Center Fabric provisioning. It requires the policy extended nodes to communicate with ISE to authenticate and authorize the endpoints for downloading the right VLANs and SGT attributes. However, the CTS & closed authentication (802.1X or MAB) configuration for DC-PENs in the ring, are provisioned using Day N templates.

A feature comparison of Extended Node, DC-EN, and Policy Extended Node, and DC-PEN devices is shown in Table 1. The comparison in provisioning of DC-ENs and DC-PENs with ENs and PENs are also highlighted in the table wherever applicable.
Table 1  Comparison of Extended Node, Policy Extended Node, Daisy-Chained Extended Node and Daisy-Chained Policy Extended Node features

<table>
<thead>
<tr>
<th>Features</th>
<th>Extended Node (EN)</th>
<th>Policy Extended Node (PEN)</th>
<th>Daisy-Chained Extended Node (DC-EN)</th>
<th>Daisy-Chained Policy Extended Node (DC-PEN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classification and list of devices supported</td>
<td>Any Cisco IE4000, IE5000, IE3300 and ESS 3300 Series switches directly connected to Fabric Edge/FIAB access port is an EN.</td>
<td>Cisco IE4000 series switches directly or indirectly connected to Fabric Edge/FIAB access port is a PEN.</td>
<td>Any Cisco IE4000, IE5000, IE3300, and ESS 3300 Series switches indirectly connected to Fabric Edge/FIAB via daisy chaining is a DC-EN.</td>
<td>Cisco IE3400 series switches indirectly connected to Fabric Edge/FIAB via daisy chaining is a DC-PEN.</td>
</tr>
<tr>
<td>Configuration and Provisioning</td>
<td>Automatically discovered and provisioned using Cisco DNA Center Extended Node Onboarding procedure leveraging PnP.</td>
<td>Automatically discovered and provisioned using Cisco DNA Center Extended Node Onboarding procedure leveraging PnP.</td>
<td>Discovered and configured using Cisco DNA Center Day N templates.</td>
<td>Discovered and configured manually. CCI Implementation guide covers detailed steps for manual provisioning and configuration on DC-PENs.</td>
</tr>
<tr>
<td>Endpoints supported</td>
<td>Any endpoint having Ethernet (PoE/Non PoE, Fiber/Copper) can be connected to EN.</td>
<td>Any endpoint having Ethernet (PoE/Non PoE, Fiber/Copper) can be connected to PEN.</td>
<td>Any endpoint having Ethernet (PoE/Non PoE, Fiber/Copper) can be connected to DC-EN</td>
<td>Any endpoint having Ethernet (PoE/Non PoE, Fiber/Copper) can be connected to DC-PEN.</td>
</tr>
<tr>
<td>Management</td>
<td>Managed through Cisco DNA Center for Software life cycle and switch configuration.</td>
<td>Managed through Cisco DNA Center for Software life cycle and switch configuration.</td>
<td>Managed through Cisco DNA Center for Software life cycle and switch configuration.</td>
<td>Managed through Cisco DNA Center for Software life cycle and switch configuration.</td>
</tr>
<tr>
<td>Support for Host Onboarding in Cisco DNA Center</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Support for QoS Application Policies Provisioning using Cisco DNA Center</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
Related Terminology

Endpoints

The clients or user devices that connect to the Fabric Edge Node are called Endpoints; supported downstream switches are Extended Nodes or Policy Extended Nodes. In the case of CCI Network, wired and wireless clients connect directly or indirectly via APs or gateways to access switches that are either ENs or PENs or DC-ENs or DC-PENs. For uniformity in this document, we refer to all of the wired and wireless clients as “Endpoints.”

Transit Network

Fabric domain is a single fabric network entity consisting of one or more isolated and independent fabric sites. Multiple fabric sites can be connected with a transit network. Depending on the characteristics of the intermediate network interconnecting the fabric sites and Cisco DNA Center, the transit network can either be SD-Access Transit or IP Transit. Typically, an IP-based Transit connects a fabric site to an external network whereas SD-Access Transit connects one or more native fabric sites.

SD-Access Transit Network

The key consideration for using SD-Access transit is that the network between the fabric sites and the Cisco DNA Center should be created with campus-like connectivity. The connections should be high-bandwidth and low latency (less than 10ms) and should accommodate jumbo MTUs (9100 bytes). These are best suited when dark fiber is available between fabric sites. The larger MTU size is needed to accommodate an increase in packet size due to VXLAN encapsulation, therefore, avoiding fragmentation and reassembly.

An SD-Access Transit consists of a domain-wide control plane node dedicated to the transit functionality, connecting to a network that has connectivity to the native SD-Access (LISP, VXLAN, and CTS) fabric sites that are to be interconnected as part of the larger fabric domain. Aggregate/summary route information is populated by each of the borders connected to the SD-Access Transit control plane node using LISP.
SD-Access Transit carries SGT and VN information, with native SD-Access VXLAN encapsulation, inherently enabling policy and segmentation between fabric sites; in that way, segmentation is maintained across the fabric sites in a seamless manner.

End-to-end configuration of SD-Access Transit is automated by the Cisco DNA Center. The control, data, and policy plane mapping across the SD-Access Transit is shown in Figure 13. Two SD-Access Transit Control (TC) plane nodes are required, but these are for control plane signaling only and do not have to be in the data plane path.

**Note:** SD Access Transit does not support multicast communications.

**Figure 13** SD-Access Transit Data, Control, and Policy Plane Mapping

---

**IP Transit Network**

IP Transit is the choice when the fabric sites are connected using an IP network that doesn’t comply to the desired network specification of SD-Access Transit, such as latency and MTU. This is often the choice when the fabric sites are connected via public WAN circuits.

Unlike SD-Access Transit, the configurations of intermediate nodes connecting fabric sites in IP-Transit are manual and not automated by Cisco DNA Center.

IP Transits offer IP connectivity without native SD-Access encapsulation and functionality, potentially requiring additional VRF and SGT mapping for stitching together the macro- and micro-segmentation needs between sites. Traffic between sites will use the existing control and data plane of the IP Transit area. Thus, the ability to extend segmentation across IP transit depends on the external network.

Unlike SD-Access transit, no dedicated node does IP Transit functionality. Instead, the traditional IP handover functionality is performed by the fabric border node. Border nodes hand off the traffic to the directly connected external domain (BGP with VRF-LITE or BGP with MPLS VRF). BGP is the supported routing protocol between the border and external network. The router connecting to the border at the HQ site is also configured for fusion router functionality with selective route leaking. Fusion router is explained in the next section below. The list of VNs that need to communicate with the external network are selected at the border IP Transit interface.

The list of VNs that need to communicate with the external world are selected at the border IP Transit interface.

As discussed previously, IP Transit is outside of the fabric domain, therefore SXP is used to re-apply the correct markings (VXLAN and SGT) that are stripped off during the transit.
The control, data, and policy plane mapping from the SD-Access fabric to the external domain is shown in Figure 14. Multiple fabric sites can interconnect via external network using IP Transit.

**Figure 14  IP Transit Data, Control, and Policy Plane Mapping**

Fusion Router

Most of the networks will need to connect to the Internet and shared services such as DHCP, DNS, and the Cisco DNA Center. Some networks may also have a need for restricted inter-VN communication. Inter-VN communication is not allowed and not possible within a Fabric Network.

To accommodate the above requirements at the border of the fabric, a device called a fusion router (FR) or fusion firewall is deployed. The border interface connecting to FR is an IP Transit. The FR/fusion firewall is manually configured to do selective VRF route leaking of prefixes between the SD-Access virtual networks and the external networks. The FR governs the access policy using ACLs, between the VRFs and the Global Routing Table (GRT). Use of the firewall as a FR gives an additional layer of security and monitoring of traffic between virtual networks.

Access Networks and Edge Compute

CCI is versatile and modular, allowing it to support different kinds of access networks. Different CCI solutions such as Smart Lighting, Smart Parking, Safety and Security, and Connected Roadways have different access networks needs and can seamlessly use CCI as a common network infrastructure.

The list of access networks included in this release are:

- CCI Ethernet access network solution
- CCI Wi-Fi 802.11 access network solution
- CCI CR-Mesh (802.154g/e) access network solution (Wi-SUN certified)
- CCI LoRaWAN access network solution
CCI DSRC access network solution

**Note:** The physical installation of access networking around or on the street/roadway is very different than that of a typical enterprise network; extra care should be taken with respect to environment conditions and rating of equipment (and associated enclosures), as well as the physical security of the network equipment: for example, is it pole-mounted high enough out of reach? Is the enclosure securely locked?

Edge Compute capabilities are available across many hardware platforms in CCI, routers, and switches. For details on this, refer to the Platform Support Matrix at https://developer.cisco.com/docs/iox/#!platform-support-matrix, and for an example of how edge compute can be used in CCI, refer to DSRC Vertical Solution, page 124.

**Disclaimer:** While this document describes best practices and details on deploying and utilizing IOx, custom IOx applications (micro-services and containers) are neither created nor supported by Cisco. The customer assumes all responsibility and risk associated with the development and use of such custom applications.

**Next-Generation Firewall (NGFW) and DMZ Network**

A DMZ in the CCI infrastructure provides a layer of security for the internal network by terminating externally-connected services from the Internet and Cloud at the DMZ and allowing only permitted services to reach the internal network nodes.

Any network service that runs as a server requiring communication to an external network or the Internet are candidates for placement in the DMZ. Alternatively, these servers can be placed at the data center and be only reachable from the external network after being quarantined at DMZ.

The DMZ in the CCI architecture is where headend routers (e.g., Cisco Cloud Services Router 1000V) reside that are used to terminate VPN tunnels from external network. **Figure 15** illustrates the DMZ design with dual-firewall in CCI:

In **Figure 15**, the DMZ is protected by two firewalls (with redundancy) and the external network-facing firewall (perimeter firewall) is set up to allow traffic to pass to the DMZ only. For example, in CCI, FlexVPN traffic (UDP port 500 and 4500) is allowed. The internal network-facing firewall (internal firewall) is set up to allow certain traffic from the DMZ to the internal network.

The dual-firewall model of DMZ design allows for the creation of two distinct and independent points of control for all traffic into and out of all internal network. No traffic from the external network is permitted directly to the internal network. Some implementations suggest adoption of two different firewall models by two different vendors to reduce the likelihood of compromise because of the low probability of the same security vulnerability existing on both firewalls. Because of the cost and complexity of the dual-firewall architecture, it is typically implemented in environments with critical security requirements such as banking, government, finance, and larger medical organizations.
Alternatively, a three-legged model of DMZ design uses a single firewall (with redundancy) with a minimum of three network interfaces to separate the external network, internal network, and DMZ.

**Figure 16  DMZ Design in CCI Architecture Single-Layer Firewall Model**

A number of headend routers are placed in the DMZ to terminate the FlexVPN tunnels. The recommended platform is Cisco Cloud Services Router 1000V; the dimension is based on the number and type of VPN clients expected to connect to the CCI infrastructure.

Traditional stateful firewalls with simple packet filtering capabilities efficiently blocked unwanted applications because most applications met the port-protocol expectations. However, in today’s environment, protection based on ports, protocols, or IP addresses is no longer reliable or workable. This fact led to the development of an identity-based security approach, which takes organizations a step beyond conventional security appliances that bind security to IP addresses.

NGFW technology offers application awareness that provide system administrators a deeper and more granular view of network traffic in their systems. The level of information detail provided by NGFW can help with both security and bandwidth control.

Cisco’s NGFW (Firepower appliance) resides at the network edge to protect network traffic from the external network. In the CCI design, a pair of Firepower appliances (Firepower 2140) are deployed as active/standby units for high availability. The Firepower units have to be the same model with the same number and types of interfaces running the exact same software release. On the software configuration side, the two units have to be in the same firewall mode (routed or transparent) and have the same Network Time Protocol (NTP) configuration.

The two units communicate over a failover link to check each other’s operational status. Failovers trigger by events such as the primary unit losing power, primary unit interface link physical down, or primary unit physical link up but has connection issue. During a stateful failover, the primary unit continually passes per-connection state information to the secondary unit. After a failover occurs, the same connection information is available at the new primary unit. Supported end-user applications (i.e., TCP/UDP connections and states, SIP signaling sessions) are not required to reconnect to keep the same communication session.

For more details, refer to the Firepower documentation at the following URL:


The CCI Network architecture or CCI vertical use cases leverages the following Cisco NGFW features:

- **Standard Firewall Features:**
  - These include the traditional firewall functionalities such as stateful port/protocol inspection, Network Address Translation (NAT), and Virtual Private Network (VPN).
Solution Architecture

- **URL Filtering:**
  - This is to set access control rules to filter traffic based on the URL used in an HTTP or HTTPS connection. Since HTTPS traffic is encrypted, consider setting SSL decryption policies to decrypt all HTTPS traffic that the NGFW intends to filter.

- **Application Visibility & Control (AVC):**
  - Discover network traffic with application-level insight with deep packet visibility into web traffic.
  - Analyze and monitor application usages and anomalies.
  - Build reporting for capacity planning and compliance.

- **Next-Generation Intrusion Prevention System (NGIPS):**
  - Collected and analyzed data includes information about applications, users, devices, operating systems, and vulnerabilities.
  - Build network maps and host profiles to provide contextual information.
  - Security automation correlates intrusion events with network vulnerabilities.
  - Network weaknesses are analyzed and automatically generate recommended security policies to put in place to address vulnerabilities.

- **Advanced Malware Protection (AMP):**
  - Collects global threat intelligence feeds to strengthen defenses and protect against known and emerging threats.
  - Uses that intelligence coupled with known file signatures to identify and block policy-violating file types and exploit attempts and malicious files trying to infiltrate the network.
  - Upon detection of threats, instantly alert security teams with an indication of compromise and detail information of malware origin, system impacted, and what the malware does.
  - Update the global threat intelligence database with new information.

**Common Infrastructure and Shared Services**

This section covers various common Infrastructure components and shared services in the CCI Network.

Shared services, as the name indicates, are a common set of resources for the entire network that are accessible by devices/clients across all VNs and SGTS. Shared services are kept outside the fabric domain(s). Communication between shared services and the fabric VN/SGTs are selectively enabled by appropriate route leaking at the fusion router. Usually shared services are located at a central location. Major shared services of the CCI network include DNA Center, ISE, DHCP, DNS, FND, and NGFW.

**Cisco DNA Center**

The Cisco Digital Network Architecture Center (Cisco DNA Center) is an open and extensible management platform for the entire CCI Network solution to implement intent-based networking. It also provides network automation, assurance, and orchestration.

Cisco DNA Center with SD-Access enables management of a large-scale network of thousands of devices. It can configure and provision thousands of network devices across the CCI network in minutes, not hours or days.
The major concerns for a large network such as CCI are security, service assurance, automation, and visibility. These requirements are to be guided by the overall CCI network intent. Cisco DNA Center with SD-Access enables all these functionalities in an automated, user-friendly manner.

Cisco DNA Center Appliance

The Cisco DNA Center software application package is designed to run on the Cisco DNA Center Appliance, configured as a cluster. The Cisco DNA Center cluster is accessed using a single GUI interface hosted on a virtual IP, which is serviced by the resilient nodes within the cluster.

Identity Services Engine (ISE)

The Cisco Identity Services Engine (ISE) is a policy-based access control system that enables enterprises, Smart Cities, and alike to enforce compliance, enhance infrastructure security, and streamline their service operations.

The Cisco ISE consists of several components with different ISE personas:

- Policy Administration Node (PAN):
  - Single pane of glass for ISE admin
  - Replication hub for all database configuration changes

- Monitoring Node (MNT):
  - Reporting and logging node
  - Syslog collector for ISE nodes

- Policy Services Node (PSN):
  - Makes policy decisions
  - RADIUS/TACACS+ servers

- Platform Exchange Grid Node (PXG):
  - Facilitates sharing of context

In the CCI architecture, ISE is deployed centralized in the standalone mode together with the Cisco DNA Center (in the Shared Services segment) with redundancy. Optionally, distributed PSNs can be deployed within fabric sites and in CCI PoP and RPoPs to provide faster response time.

Depending on the size of the deployment, all personas can be run on the same device (standalone mode) or spread across multiple devices (multi-node ISE) for redundancy and scalability. The detailed scaling information and limits for ISE can be found at the following URL:


ISE integrates with the Cisco DNA Center via the Platform eXchange Grid (pxGrid) interface to enable network-wide context sharing. pxGrid is a common method for network and security platform to share data about devices through a secure publish-and-subscribe mechanism. A pxGrid subscriber registers to PXG to subscribe to "topic" information. A pxGrid Publisher publishes topics of information to PXG and pxGrid Subscriber receives the topic information once it is available. Examples of "topics" include:

- TrustSecMetaData—Provides pxGrid clients with exposed scalable group tag (SGT) information
- EndpointProfileMetaData—Provides pxGrid clients with available device information from ISE
- SessionDirectory—Session directory table
The main roles of ISE in the CCI infrastructure is to authenticate devices, perform device classification, authorize access based on policy, and support SGT tag propagation.

- **Device classification:**
  - Classifies a device based on the device profile information gathered. For example, detect a device plugged in matches IP Camera profile and assign the device to the video VLAN.
  - Dynamic classification:
    - Performs 802.1X or MAC Address Bypass (MAB) for devices connected to nodes attached to the access switches in the PoP ring.
  - Static classification:
    - Currently an access port on extended node is automated from the Cisco DNA Center with a pre-defined service VLAN. A trunk between the extended node and fabric edge carries all the VLAN’s traffic. The recommended method is to do VLAN-to-SGT binding statically at the fabric edge for device classification. This can be automated via the Cisco DNA Center.

- **Access authorization:**
  - The PSN will authorize device access capability based on the policy defined for the class of devices.

- **SGT tag propagation:**
  - SGT tag information shall be propagated from one fabric site to another to maintain consistent end-to-end policy throughout the network.
  - However, packets that transport over nodes that don’t support VXLAN or that don’t have inline tagging capability will lose SGT tagging information.
  - SGT tag propagation methods:
    - SGT eXchange Protocol (SXP)
    - As Figure 17 shows, “Router A” has no inline capability. Any SGT tag from “Switch A” to “Router B” will not be carried over because “Router A” is not inline capable.
    - In order to restore the SGT tag at “Router B,” leverage the SXP protocol where the “Switch A” is the speaker and “Router B” is the listener.
      - The SXP protocol sends the SGT tag (5) assigned to the end device (IP 10.0.1.2) from “Switch A” to “Router B.”
      - The SXP protocol uses TCP as the transport protocol over TCP port 64999.
      - Cisco ISE can be an SXP speaker/listener. It is recommended to establish SXP from Fabric Border to ISE for ease of configuration.

- **A list of Cisco switches and routers support SXP can be found at the following URL:**

- **In the CCI context, SXP is essential for exchanging SGT in the IP Transit environment.**
pxGrid (Cisco Platform eXchange Grid):

- As described in *Identity Services Engine (ISE), page 28*, ISE and the Cisco DNA Center are integrated using pxGrid to share users and device contexture information.

- Besides the Cisco DNA Center, a number of Cisco and third-party products have integrated with pxGrid based on the Cisco published integration guide. More details can be found at the following URL:
  

- In the CCI infrastructure, the pxGrid can integrate ISE with NGFW to improve network visibility.

Once the SGT is propagated, it can be carried to the policy enforcement node for access control decisions.

*Figure 18* illustrates the interworking of each component of ISE and the Cisco DNA Center:
Application Servers Network

Application servers are dedicated for specific services; for example, Video Surveillance Manager (VSM) is dedicated for video services management. Only the devices and users having access to the specific service should be able to communicate with the application server. In the case of VSM, the cameras, media servers, and users having video access can communicate with the VSM server.

In the case of a fabric-supported network, this is achieved by placing the application servers in one of the fabric sites. The application servers are connected to a Nexus switch behind the Fabric Edge. The access port on the FE/FiaB is configured as a Server Port. Appropriate Subnets and VLANs are configured on the Nexus ports connecting the application servers that match the respective service Subnet/VLAN auto allocated by the Cisco DNA Center. In the Fabric Site, the desired VNs, Subnets, and Static SGTs are configured matching various services. As the application servers and corresponding clients are assigned, the same SGT and VN access is provided. Any other service that is part of the same VN, but is of a different SGT, will require appropriate group-based access policy for communication. In an exception case, if a device/client of one VN needs access to the application server of a different VN, appropriate route leaking needs to be done at the FR in order for it to become accessible.

Field Network Director (FND)

The Cisco FND is a software platform that can monitor and manage several solutions including IR8x9/1101 routers, and CR-Mesh and LoRaWAN access network solution. It provides enhanced fault, configuration, accounting, performance, and security (FCAPS) capabilities for highly scalable and distributed systems such as smart street lighting controllers and power meters.

Additional capabilities of the FND are:

- Zero Touch Deployment for CGRs, IR8x9, IR1101 and IXM gateways
- Network topology visualization and integration with existing Geological Information System (GIS)
- Simple, consistent, and scalable network layer security policy management and auditing
- Extensive network communication troubleshooting tools
- Northbound APIs are provided for integration with third party applications
Solution Architecture

- Third party device management with IoT Device Agent (IDA)

FND provides the necessary backend infrastructure for policy management, network configuration, monitoring, event notification services, network stack firmware upgrade, Connected Grid Endpoint (CGE) registration, and maintaining FAR and CGE inventory. FND uses a database that stores all the information managed by the FND. This includes all metrics received from mesh endpoints, and all device properties, firmware images, configuration templates, logs, and event information.

For more information on using FND, refer to the latest version of *Cisco IoT Field Network Director User Guide* at the following URL:


**Network Time Protocol (NTP) Server**

Certain services running within the CCI network require accurate time synchronization between the network elements. Many of these applications process a time-ordered sequence of events, so the events must be time stamped to a level of precision that allows individual events to be distinguished from one another and correctly ordered. A Network Time Protocol (NTP) version 4 server running over the IPv4 and IPv6 network layer can act as a Stratum 1 timing source for the network.

Applications that require time stamping or precise synchronization include:

- Time stamps for asynchronous notifications for log entries and events
- Validation of X.509 certificates used for device authentication, specifically to ensure that the certificates are not expired

**Cisco Prime Network Registrar (CPNR)**

Cisco Prime Network Registrar (CPNR) provides integrated, scalable, and reliable Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and IP Address Management (IPAM) services for both IPv4 and IPv6. DHCPv6 is the desired address allocation mechanism for highly scalable outdoor systems consisting of many endpoints, as an example CGE mesh endpoints for streetlights or energy meters.

CPNR is a full featured, scalable DNS, DHCP, and Trivial File Transfer Protocol (TFTP) implementation for medium-to-large IP networks. It provides the key benefits of stabilizing the IP infrastructure and automating networking services, such as configuring clients and provisioning cable modems. This provides a foundation for policy-based networking.

A DHCP Server is a network server that dynamically assigns IPv4 or IPv6 addresses, default gateways, and other network parameters to client devices. It relies on the standard protocol known as DHCP to respond to broadcast queries by clients. This automated IP address allocation help IP planning and avoid manual IP configuration to network devices and clients.

The DNS service is a hierarchical and decentralized service for translating domain names to the numerical IP addresses.

**Headend Routers (HER)**

The primary function of a HER is to aggregate the WAN connections coming from the field-deployed devices, including Connected Grid Routers, Cisco 809 Industrial Integrated Services Routers, and Cisco 829 Industrial Integrated Services Router, and Cisco IR1101 Integrated Services Router Rugged. A HER can be a dedicated hardware appliance or a hosted CSR 1000v. The HER terminates the FlexVPN IPSec and GRE tunnels. HER may also enforce QoS, profiling (Flexible NetFlow), and security policies.
Solution Architecture

Multiple Cisco CSR 1000V routers can be configured in clusters for redundancy and to facilitate increased scalability of tunnels. In the case of a cluster configuration, a single CSR acts as the primary and load balances the incoming traffic among the other HERs. Alternately, the Hot Standby Router Protocol (HSRP) can be configured for active/standby redundancy.


Authentication, Authorization, and Accounting (AAA)

A framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services.

Remote Authentication Dial-In User Service (RADIUS)

RADIUS is a networking protocol, operating on Port 1812 that provides centralized authentication, authorization, and accounting management for users who connect and use a network service.

Public Key Infrastructure (PKI)

A Public Key Infrastructure (PKI) supports the distribution, revocation and verification of public keys used for public key encryption and enables linking of identities with public key certificates. It enables users and systems to securely exchange data over the network and verify the legitimacy of certificate-holding entities, such as servers, endpoints, and individuals. The PKI enables users to authenticate digital certificate holders, as well as to mediate the process of certificate revocation, using cryptographic algorithms to secure the process.

Certificate Authority

The Certificate Authority (CA) is part of a public key infrastructure and is responsible for generating or revoking digital certificates assigned to the devices and mesh endpoints. The CAs are unconditionally trusted and are the root of all certificate chains.

RSA Certification Authority

An RSA Certificate Authority (RSA CA) provides signed certificates to network components such as routers and servers like FND.

ECC Certification Authority

The Elliptic Curve Cryptography Certificate Authority (ECC CA) provides signed certificates for endpoint devices like power meters and street lighting controllers.

Cisco Kinetic for Cities (CKC)

Cisco Kinetic for Cities (CKC) is a special type of application server hosted in cloud-based or on-premises-based platform. It helps customers extract, compute, and move data from connected things to IoT applications in order to deliver better outcomes and services. More explicitly, it gets the right data to the right applications at the right time—across edge, private cloud, public cloud, and hybrid environments—while executing policies to enforce data ownership, privacy, security, and even data sovereignty laws.

Cisco Kinetic for Cities is Cisco’s IoT solution for Smart Cities that addresses various city digitization programs. It brings policy-based control and automation to city infrastructure features, such as smart streetlights, parking sensors, traffic and crowd monitoring, environmental sensors, and video (CCTV) cameras. It is a powerful digital platform for aggregating, normalizing, and analyzing the wealth of community data from a myriad of intelligent sensors and city assets. The platform is generic and flexible in its ability to onboard any smart city solutions or digitization programs.
Solution Components

Cisco Wireless LAN Controller (WLC)

Cisco WLCs may be located in the Shared Services segment, or as part of PoP distribution infrastructure; please see It is recommended to configure the Policy Extended Node ring (PEN ring) with DC-PENs manually due a limitation on template-based approach for provisioning PEN feature on DC-PENs. A high-level summary of steps for manual provisioning of the PEN ring is explained below. Refer to the CCI Implementation Guide for detailed step-by-step instructions for configuring PEN ring, page 76 for details on location.

The WLC role is to be in control of Cisco Lightweight APs, using the CAPWAP protocol (Control and Provisioning of Wireless Access Points); managing software versions and settings, handoff of traffic at the edge, or tunneling of traffic back to the WLC.

WLCs may be appliances or embedded as software components in another Cisco networking device. Deploying WLCs as HA pairs is recommended.

Cisco Prime Infrastructure

Cisco Prime Infrastructure (PI) is used for management of a Cisco Unified Wireless Network (CUWN) Mesh. Although PI is capable of performing network management for other devices and systems within CCI, its role in CCI 2.0 is limited to just the Wi-Fi Mesh – DNAC being used for everything else.

Cisco DNA Spaces

Cisco DNA Spaces is a location services platform, delivered as a cloud-based service. Wireless LAN Controllers (WLCs) integrate with DNA Spaces, and as such must have an outbound path to the Public Internet.

DNA Spaces generates Wi-Fi client computed location, tracking and analytics, with visualization and the ability to export all this data; also provides captive portal, hyper-location, advanced analytics and API/SDK integration possibilities.

In general DNA Spaces is an optional component with the CVD, however for the Public Wi-Fi services with CCI Wi-Fi, page 167 it is a mandatory component, because it is used to provide the Guest portal.

Solution Components

The components of the CCI network are listed in this chapter. Several device models can be used at each layer of the network. The suitable platform of devices for each role in the network and the corresponding CVD-validated software versions are presented in Table 2. To find a list of supported devices, refer to the SD-Access 2.x product compatibility matrix at the following URL:


The exact suitable model can be chosen from the suggested platform list to suit specific deployment requirements such as size of the network, cabling and power options, and access requirements. The components for various CCI verticals are listed in their respective sections.
Note: In addition to the compatibility matrix, it is recommended to research any product vulnerabilities discovered since publication, via https://tools.cisco.com/security/center/publicationListing.x. This is especially important for ISE and the FlexVPN headend.

Table 2  CCI Network Components

<table>
<thead>
<tr>
<th>CCI Network Function + Cisco DNA Center (SD-Access) Device Role</th>
<th>Cisco Platform</th>
<th>Version</th>
<th>Description</th>
<th>CVD Verified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distribution layer switch + Fabric Function: Edge + Control + Border ( Fabric in a Box) DNAC Fabric Role: BORDER</td>
<td>Cisco Catalyst 9500 Series Switches***</td>
<td>IOS-XE 17.3.1</td>
<td>480 Gbps stacking bandwidth. Sub-50-ms resiliency. UPOE and PoE+. 24-48 multigigabit copper ports. Up to 8 port fiber uplinks. AC environment.</td>
<td>Yes</td>
</tr>
<tr>
<td>Core layer switch + Fabric Function: Non-Fabric, IP Transit, SD-Access Transit and Fusion Router and Cisco StackWise Virtual (SVL) DNAC Fabric Role: CORE and/or BORDER</td>
<td>Cisco Catalyst 9500 Series Switches</td>
<td>IOS-XE 17.3.1</td>
<td>Core and aggregation.</td>
<td>Yes</td>
</tr>
<tr>
<td>Access layer switch + Function: &quot;Fabric: Extended Node or DC-EN&quot; DNAC Fabric Role: ACCESS</td>
<td>Cisco IE 5000 Series Switches</td>
<td>15.2(7)E3</td>
<td>Ruggedized One RU multi-10 GB aggregation switch with 24 Gigabit Ethernet ports plus 4 10–Gigabit ideal for the aggregation and/or backbones, 12 PoE/PoE+ enabled ports.</td>
<td>Yes</td>
</tr>
<tr>
<td>Access layer switch + Function: &quot;Fabric: Extended Node or DC-EN&quot; DNAC Fabric Role: ACCESS</td>
<td>Cisco IE 4000 Series Switches</td>
<td>15.2(7)E3</td>
<td>Ruggedized DIN rail-mounted 40 GB Industrial Ethernet switch platform. IE4010 Series Switches with 28 GE interfaces and up to 24 PoE/PoE+ enabled ports.</td>
<td>Yes</td>
</tr>
<tr>
<td>Access layer switch + Function: &quot;Policy Extended Node (PEN) and DC-PENs&quot; DNAC Fabric Role: ACCESS</td>
<td>Cisco Catalyst IE 3400 Rugged Series</td>
<td>17.3.1</td>
<td>Ruggedized full Gigabit Industrial Ethernet with a modular, expandable up to 26 ports. Up to 16 PoE/PoE+ ports.</td>
<td>Yes</td>
</tr>
<tr>
<td>Access layer switch + Function: &quot;Fabric: Extended Node or DC-EN&quot;</td>
<td>Cisco Catalyst IE 3300 Rugged Series</td>
<td>17.3.1</td>
<td>Ruggedized full Gigabit Industrial Ethernet with a modular, expandable up to 26 ports. Up to 16 PoE/PoE+ ports.</td>
<td>Yes</td>
</tr>
<tr>
<td>Data Center Switch + Function: Non-Fabric DNAC Fabric Role: ACCESS</td>
<td>Nexus 9000 series *</td>
<td>7.0(3)I7(7)</td>
<td>--</td>
<td>No</td>
</tr>
</tbody>
</table>
| Remote PoP Aggregation Router with Cellular backhaul | Cisco 809/829 Industrial Integrated Services Router  
Cisco 1100 Series Industrial Integrated Services Router | 15.8(3)M3  
17.03.01 | Ruggedized 3G/4G LTE WAN Cellular and Wireless LAN connectivity for Remote/mobile environments  
Ruggedized 5G Ready, modular, dual active LTE- capable (two cellular networks for WAN redundancy) ISR | Yes          |
### Table 2  CCI Network Components (continued)

<table>
<thead>
<tr>
<th>CCI Network Function + Cisco DNA Center (SD-Access) Device Role</th>
<th>Cisco Platform</th>
<th>Version</th>
<th>Description</th>
<th>CVD Verified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote PoP Aggregation Router with Cellular backhaul + CR-Mesh Access Gateway</td>
<td>Cisco 1000 Series Connected Grid Router</td>
<td>15.9(3)M2</td>
<td>Ruggedized, modular platform with Ethernet, serial, cellular, RF mesh and Power Line Communication (PLC)</td>
<td>Yes</td>
</tr>
<tr>
<td>Wireless LAN Controller</td>
<td>Cisco Catalyst 9800 - 9800-40 - 9800 Embedded</td>
<td>17.3.1</td>
<td>Wireless LAN Controller for CUVN (in the case of 9800-40) and SDA Wireless (in the case of 9800 Embedded)</td>
<td>Yes</td>
</tr>
<tr>
<td>Wireless Access Points</td>
<td>Cisco Aironet - AP1562 - AP1572 - ESW6300 - IW3702</td>
<td>17.3.1</td>
<td>Outdoor 802.11ac APs</td>
<td>Yes</td>
</tr>
<tr>
<td>Next Generation Firewall</td>
<td>Cisco Firepower 2100 Series*</td>
<td>6.6.0</td>
<td>Next Generation Firewall at DMZ</td>
<td>Yes</td>
</tr>
<tr>
<td>DMZ Switch</td>
<td>Cisco Catalyst 9200L Series*</td>
<td>17.1.1</td>
<td>L2 DMZ switch stack (StackWise 80)</td>
<td>No</td>
</tr>
<tr>
<td>FlexVPN Headend Router</td>
<td>CSR-1000v*</td>
<td>17.3.1a</td>
<td>VM</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco DNA Center Appliance</td>
<td>DN2-HW-APL</td>
<td>Not applicable</td>
<td>U - 44 core, L - 56 core (RET) 2x Two 10 Gbps Ethernet ports, One 1 Gbps management port</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco DNA Center</td>
<td>Software</td>
<td>2.1.2.0</td>
<td>Centralized, Single Pane of Glass network management for Cisco’s intent-based network with foundation controller and analytics platform</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco Identity Services Engine (ISE)</td>
<td>Cisco SNS-3655 or SNS-3695 Secure Network Server or Virtual Appliance</td>
<td>ISE 2.4 Patch 13</td>
<td>Authentication, Authorization and Accounting (AAA) server and Policy Engine</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco WPAN Industrial Router for CR-Mesh and SCADA</td>
<td>Cisco IR510</td>
<td>6.2.19</td>
<td>CR-Mesh WPAN gateway for CCI lighting and SCADA use cases</td>
<td>Yes</td>
</tr>
<tr>
<td>CR-Mesh Range Extender</td>
<td>Cisco IR530</td>
<td>6.2.19</td>
<td>CR-Mesh WPAN RF range extender</td>
<td>Yes</td>
</tr>
</tbody>
</table>

* These are recommended platform families; however no part of this CVD relies on specific capabilities in these platforms, and other platform choices are available. Please discuss alternative platforms with your Cisco seller.

*** Only the non-high-performance variants of the Catalyst 9500 family are supported for SVL FiaB; for other uses of Catalyst 9500 within CCI, the high-performance and standard-performance variants are supported.
### Table 3  Fluidmesh Components

<table>
<thead>
<tr>
<th>Trackside Network Function</th>
<th>Fluidmesh Platform</th>
<th>Version</th>
<th>Fluidmesh Role</th>
<th>CVD Verified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trackside Radio</td>
<td>FM 3500</td>
<td>9.1.2</td>
<td>Mesh Point / Mesh End</td>
<td>Yes</td>
</tr>
<tr>
<td>Train Radio*</td>
<td>FM 4500</td>
<td>9.1.2</td>
<td>Mobile Radio</td>
<td>Yes</td>
</tr>
<tr>
<td>Trackside Gateway</td>
<td>FM 1000</td>
<td>1.3.1</td>
<td>Mesh End / Global Gateway (no radio function)</td>
<td>Yes</td>
</tr>
<tr>
<td>Datacenter Gateway</td>
<td>FM 10000</td>
<td>2.0.1</td>
<td>Global Gateway</td>
<td>Yes</td>
</tr>
<tr>
<td>Antenna</td>
<td>FM Tube, Panel</td>
<td>N/A</td>
<td>Trackside/Tunnel antenna</td>
<td>No</td>
</tr>
<tr>
<td>Device Provisioning</td>
<td>Configurator, RACER</td>
<td>N/A</td>
<td>Local or Cloud provisioning</td>
<td>Yes</td>
</tr>
<tr>
<td>Network Monitoring</td>
<td>Monitor</td>
<td>N/A</td>
<td>Network Monitoring</td>
<td>No</td>
</tr>
</tbody>
</table>

* The Train Radio is not part of the trackside infrastructure. The FM 4500 resides on the train to communicate with the FM 3500 on the trackside.
CCl Security Architecture and Design Considerations

This chapter includes the following major topics:

- Security Segmentation Design, page 38
- Network Visibility and Threat Defense using Cisco Stealthwatch, page 42
- Secure Connectivity, page 46

Security Segmentation Design

Network segmentation is the practice of dividing a larger network into several small sub-networks that are isolated from one another.

Advantages of Network Segmentation

- **Improved Security**—Network traffic can be segregated to prevent access between network segments.
- **Better Access Control**—Allows users to only access specific network resources.
- **Improved Monitoring**—Provides an opportunity to log events, monitor allowed and denied internal connections, and detect suspicious behavior.
- **Improved Performance**—With fewer hosts per subnet, local traffic is minimized. Broadcast traffic can be isolated to the local subnet.
- **Better Containment**—When a network issue occurs, its effects are limited to the local subnet.

In the SD-Access environment, fabric uses LISP as the control plane and VXLAN for the data plane (as mentioned earlier in this guide, the intricacies of LISP and VXLAN are hidden from the administrator, as SD-Access automates both as part of VNs).

- The LISP control plane has the following functions:
  - Endpoints register to the fabric edge, obtain an EID
  - Fabric edge places the EID into the Host Tracking Database (HTDB)
  - Control Plane node resolves EID to RLOC mappings
  - Control plane node provides default gateway when no mapping exists

- The VXLAN data plane serves the following function:
  - VXLAN header includes VN information (24 bit VN index called VNI)
  - VXLAN header also includes Scalable Group (SG) information (16 bit SG tag called SGT)

Traffic segmentation in SD-Access are accomplished through the following:

- **Macro-segmentation:**
  - Defines VN
  - Control plane by LISP uses VN ID to maintain separate VRF topologies
  - Each VN instance maintains a separate routing table to ensure no communication takes place between one VN with another

- **Micro-segmentation:**
CCI Security Architecture and Design Considerations

- Defines Security Group (SG)
- Scalable policies (SGACL) are defined
- Policy enforcement nodes request policies relevant to them
- ISE classification associates a device with an SGT when a device is detected in the network
- SGT is encapsulated in the VXLAN header of the packet associated with the device traffic
- SGT is propagated from one fabric node to another when traffic from a device traverses the network
- Policy enforcement nodes enforce Security Group ACL (SGACL) policies

Dynamic policy download:

- New User/Device/Server provisioned
- Switch requests policies for assets they protect
- Policies are downloaded and applied dynamically
- Result: All controls centrally managed:
  - Security policies de-coupled from network topology
  - No switch-specific security configs needed
  - One place to audit network-wide policies

A Virtual Network can be defined by an access technology such that, for example, DSRC traffic will not be mixed with LoRaWAN traffic, but a VN can also be defined across access technologies. In each VN, Security Groups can be identified, and access control policy can be enforced. Following section describes micro-segmentation in detail.

Micro Segmentation Design in Ethernet Access Ring

The CCI security design also supports micro-segmentation for securing traffic flow within a VN in CCI network. Endpoints connected to the access rings can be configured to allow access only to specific services/servers in the HQ/DC site also known as South-to-North traffic flow and vice-versa in CCI network. The traffic within endpoints connected to a given ring is defined as East-to-West traffic or vice-versa depending on the source and destination traffic flow.

In the CCI architecture, SGACL policies are enforced at destination Fabric Edge/FiaB for the South-to-North traffic (endpoints to server in DC). Server to endpoints/device communication (North-to-South) traffic (if any required) SGACL policies can be defined and enforced on destination Fabric Edge/FiaB.

See Table 4 for an example of micro-segmentation enforcement deployed in Extended Node and Policy Extended Node rings.
Table 4  Micro-segmentation enforcement for Extended Node and Policy Extended Node rings

<table>
<thead>
<tr>
<th>Destination is...</th>
<th>Source in an EN PoP access ring</th>
<th>Source in an PEN PoP access ring</th>
<th>Source is an Application server (located behind HQ FiaB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>In the same PoP access ring</td>
<td>No enforcement</td>
<td>Enforcement on the destination PEN</td>
<td>n/a</td>
</tr>
<tr>
<td>In a different PoP access ring at the same PoP site</td>
<td>Enforcement at FiaB</td>
<td>Enforcement at FiaB</td>
<td>n/a</td>
</tr>
<tr>
<td>At a different PoP site</td>
<td>Enforcement at other site’s FiaB</td>
<td>Enforcement at other site’s FiaB</td>
<td>Enforcement at other site’s FiaB</td>
</tr>
<tr>
<td>Application Server</td>
<td>Enforcement at HQ FiaB</td>
<td>Enforcement at HQ FiaB</td>
<td>Enforcement at HQ FiaB</td>
</tr>
</tbody>
</table>

In cases where there are Ethernet access rings with a mixture of IE4000 and/or IE5000 and/or IE3300 series switches, all micro-segmentation policy enforcement is done at Fabric Edge/FiaB on such mixed switches rings. Refer to Table 1, for a detailed feature comparison of EN, PEN, DC-EN, and DC-PEN switches.

Note that micro-segmentation of South-to-North and North-to-South traffic is supported in Extended Nodes Ring in CCI PoP. East-to-West and West-to-East traffic enforcement for the endpoints connected within EN is not supported. It is recommended to deploy Policy Extended Nodes ring, discussed in the next section, for the East-to-West or West-to-East traffic enforcement within the access ring.

Micro Segmentation Design in Policy Extended Nodes Ring

An Ethernet access ring consisting of Policy Extended Nodes and DC-PENs (aka PEN ring) supports micro-segmentation using Scalable Group Tags (SGT) and SGACL device to device communication policies. Endpoints connected to Policy Extended Nodes ring download the right VLAN and SGT attributes from Cisco ISE upon successful authentication and authorization by ISE, so that device to device communication polices for micro segmenting the traffic can be defined and enforced on the Policy Extended Node.

In the ring of PENs and DC-PENs, East to West and vice versa traffic SGACL policies can be defined and enforced on destination PEN or DC-PEN, as shown in Figure 19. Note that, the SGACL policy enforcement always happens at the destination switch in the ring. It is recommended to deploy PEN rings for use cases where East-to-West and vice-versa traffic enforcement is needed within the access ring.

The PEN ring must be configured with all IE3400 (PEN capable) switches with DNA Advantage licensing. The PEN ring is configured manually as one Gigabit Ethernet Access ring (without Port Channel), as shown in Figure 19, for the successful configuration of CTS commands and SGACL policies within the ring.
As shown in Figure 19, there is an SGACL policy matrix on ISE, which denies the traffic between SGT100, SGT200 and SGT 300, SGT 400. All other communication between these SGTs are allowed. This SGACL policy is enforced on destination DC-PEN in the ring to which the SnS sensor device is connected. An SnS IP Camera (SGT 100) is trying to communicate with the SnS Sensor (SGT 300). Such East-to-West traffic in the PEN ring is denied and traffic is dropped at DC-PEN.

Also, in this example, North-to-South traffic from SnS sensor applications (SGT400) in DC site to an SnS IP Camera (SGT 100) connected to a DC-PEN in the ring is denied. All such traffic is dropped at destination DC-PEN in the ring on which the micro segmentation policy is enforced.

**Note:** Policy is enforced (such as SGACL permit or deny) on the destination port.

**Note:** Although Cisco DNA Center UI allows the administrator to build out a policy matrix, this policy may not be enforced in the case of Extended Nodes, depending on where the source and destination devices are connected. If both devices are connected within the same access ring, and this ring is comprised of Extended Nodes, then traffic between these devices has policy enforced only if that traffic passes through the FiaB.

### SGT Derivation and Propagation in a Network with IP Transit and SD-Access Transit

As discussed earlier, micro-segmentation within a VN is achieved with the help of Security Groups represented by SGT. The micro-segmentation policy is defined by SGACL. For policy enforcement, both source and destination SGTs are derived and SGACLs are applied. The source fabric edge derives the source SGT from binding information. In the case of IP transit, SXP configuration needs to be done manually on the fabric edge to retrieve SGT binding information from ISE. In case of SD-Access transit, manual SXP configuration is not needed as the system automates configuration at the fabric edge to retrieve SGT binding information from ISE.

Propagation of SGT information also differs between IP and SD-Access transit. In the case of SD-Access transit, the SGTs are propagated from the source fabric to the destination fabric through inline tagging within the VXLAN header.
In the case of IP transit, inline tagging (VXLAN header) is not supported and SGT tags are lost at the fabric border. The destination fabric needs to derive both source SGT and destination SGT from the binding information, obtained from ISE using SXP.

Network Visibility and Threat Defense using Cisco Stealthwatch

Network visibility is the foundation for continuous monitoring to gain awareness of what is happening in the network. Complete visibility is critical to making proactive decisions and getting to resolutions as quickly as possible. Network threat defense is for preventing threats from the external network entering the internal network or to identify suspicious network traffic patterns within the network.

Cisco Stealthwatch Enterprise provides network visibility and applies advanced security analytics to detect and respond to threats in real time. Using a combination of behavioral modeling, machine learning, and global threat intelligence, Cisco Stealthwatch Enterprise can quickly, and with high confidence, detect threats such as command-and-control (C&C) attacks, ransomware, DDoS attacks, illicit cryptomining, unknown malware, and insider threats. With a single, agentless solution, you get comprehensive threat monitoring across the entire network traffic, even if it is encrypted.

Cisco Stealthwatch enlists the network to provide end-to-end visibility of traffic. This visibility includes knowing every host—seeing who is accessing which information at any given point. From there, it is important to know what normal behavior for a particular user or “host” is and establish a baseline from which you can be alerted to any change in the user’s behavior the instant it happens.

Cisco Stealthwatch offers many advantages when deployed, including:

- **Network Visibility** - Cisco Stealthwatch is the security analytics solution that can provide comprehensive visibility in the private network as well as the public cloud and without deploying sensors everywhere.
- **Threat Detection** - Cisco Stealthwatch is constantly monitoring the network in order to detect advanced threats in real time. Using the power of behavioral modeling, multi-layered machine learning, and global threat intelligence, Cisco Stealthwatch reduces false positives and alarms on critical threats affecting your environment.
- **Incident Response/Threat Defense** - Protects network and critical data with smarter and effective network segmentation. Using the Stealthwatch integration with Cisco Identity Services Engine (ISE) to create and enforce policies, and keep unauthorized users and devices from accessing restricted areas of the network.

Flexible NetFlow Data Collection

NetFlow is a network protocol system created by Cisco that collects active IP network traffic as it flows in or out of an interface. NetFlow is now part of the Internet Engineering Task Force (IETF) standard as Internet Protocol Flow Information eXport (IPFIX, which is based on NetFlow Version 9 implementation), and the protocol is widely implemented by network equipment vendors. NetFlow is an embedded instrumentation within Cisco IOS Software to characterize network operation. Visibility into the network is an indispensable tool for IT professionals. NetFlow is a protocol that creates flow records for the packets flowing through the switches and the routers in a network between the end devices and exports the flow records to a flow collector. The data collected by the flow collector is used by different applications to provide further analysis. In CCI, NetFlow is primarily used for providing security analysis, such as malware detection, network anomalies, and so on.

The Cisco Industrial Ethernet (IE) 3400, Cisco IE 3300, Cisco IE 4000, Cisco IE 4010, Cisco IE 5000, Cisco Catalyst 9300, and Cisco Catalyst 9500 support full Flexible NetFlow. Each packet that is forwarded within a router or switch is examined for a set of IP packet attributes. These attributes are the IP packet identity or fingerprint of the packet and determine if the packet is unique or similar to other packets.

Traditionally, an IP Flow is based on a set of 5 and up to 7 IP packet attributes, as shown in Figure 20. All packets with the same source/destination IP address, source/destination ports, protocol interface and class of service are grouped into a flow and then packets, and bytes are tallied. This methodology of fingerprinting or determining a flow is scalable because a large amount of network information is condensed into a database of NetFlow information called the NetFlow cache.
With the latest releases of NetFlow v9, the switch or router can gather additional information such as ToS, source MAC address, destination MAC address, interface input, interface output, and so on.

**Figure 20  CCI NetFlow Data Collection**

As network traffic traverses the Cisco device, flows are continuously created and tracked. As the flows expire, they are exported from the NetFlow cache to the Stealthwatch Flow Collector. A flow is ready for export when it is inactive for a certain time (for example, no new packets are received for the flow) or if the flow is long lived (active) and lasts greater than the active timer (for example, long FTP download and the standard TCP/IP connections). There are timers to determine whether a flow is inactive, or a flow is long lived.

After the flow times out the NetFlow record information is sent to the flow collector and deleted on the switch. Since the NetFlow implementation is done mainly to detect security-based incidents rather than traffic analysis, the recommended timeout for the Cisco IE 4000, Cisco IE 4010, Cisco IE 5000, and Cisco Catalyst 9300 switches is 60 seconds for the active timeout and 30 seconds for the inactive timeout. For the Cisco IE 3400, IE 3300, and ESS 3300 switches, the active is 1800 seconds, the inactive is 60 seconds, and the export timeout is 30 seconds.

In CCI, it is recommended to enable NetFlow monitoring for security on all the interfaces in the network i.e., within the PoP, between PoPs, interfaces to Data Center where application servers reside, interfaces to Fusion Router, Internet edge etc., The Configuration of NetFlow on CCI fabric devices is done through Cisco DNA Center and non–fabric devices (Eg., IE ring, FR, HER etc., can be done using Cisco DNA Center templates, which is discussed in more detail in the implementation guide.
As shown in Figure X, the main components of the Cisco Stealthwatch system are:

- Stealthwatch Flow Collectors (SFC)
- Stealthwatch Management Console (SMC)

**Note:** The respective systems reside on different virtual or hardware appliances.

The Stealthwatch Flow Collector (SFC) collects the NetFlow data from the networking devices, analyses the data gathered, creates a profile of normal network activity, and generates an alert for any behavior that falls outside of the normal profile. Based on volume of traffic, there could be one or multiple Flow Collectors in a network. The Stealthwatch Management Console (SMC) provides a single interface for the IT security architect to get a contextual view of the entire network traffic.

The SMC has a Java-based thick client and a web interface for viewing data and configurations. The SMC enables the following:

- Centralized management, configuration, and reporting for up to 25 Flow Collectors
- Graphical Charts for visualizing traffic
- Cisco Stealthwatch in CCI collects NetFlow information to gain visibility across all network conversations (North-South, East-West traffic) in order to detect internal and external threats
- Conducts security analytics to obtain context to detect anomalous behaviors
- Accelerates threat detection and incident response to reduce security risk
- Integrates with ISE, has visibility of device and user information

**Figure 21** shows Cisco Stealthwatch Management Console (SMC) Network Security dashboard to list the security insights like top alarming hosts, today’s alarms, flow collection trend and top applications in the network etc.,

Refer to the following URL for more information on Cisco Stealthwatch:
Because the Flow Collector and SMC are to be accessed by all endpoints in the CCI fabric network overlay, it is recommended to deploy the Flow Collector and SMC as common infrastructure devices in the CCI shared services network.

Cisco Stealthwatch Deployment Considerations

Some important considerations when deploying a Stealthwatch system include:

- Stealthwatch is available as both hardware (physical appliances) and virtual appliances.
- The resources allocation for the Stealthwatch Flow Collector are dependent on the number of Flows Per Second (FPS) expected on the network and the number of exporters (networking devices that are enabled with NetFlow) and the number of hosts attached to each networking device.
- The data storage requirements must be taken into consideration, which are again dependent on the number of flows in the network.
- A specific set of ports needs to be open for the Stealthwatch solution in both the inbound and outbound directions.

Refer to the following URL for installation of Stealthwatch, SFC scalability requirements, data storage and network inbound and outbound ports requirements:


Security using Cisco Stealthwatch for abnormal traffic detection

This use case describes how a CCI network security architect can use Cisco Stealthwatch along with NetFlow enabled on Cisco Industrial Ethernet (IE) switches (IE 4000, IE 5000, IE 3400, IE 3300) in the ring and Cisco Catalyst 9300/9500 switches acting as distribution switches to monitor the network flows in CCI. This use case also shows the integration between Cisco ISE and Cisco Stealthwatch, which helps a CCI network security architect to understand the context of traffic flows occurring in the network.

By integrating Stealthwatch and ISE, you can see a myriad of details about network traffic, users, and devices. Instead of just a device IP address, Cisco ISE delivers other key details, including username, device type, location, the services being used, and when and how the device accessed the network.

NetFlow is enabled on all CCI networking devices to capture the traffic flows that are sent to the Flow Collector, as shown in Figure 22. Flow records from the networking devices in CCI is exported to flow collectors in an underlay network VLAN (i.e., Shared Services VLAN). The Cisco Stealthwatch Management Console (SMC) retrieves the flow data from the Flow Collector and runs pre-built algorithms to display the network flows. It also detects and warns if there is any malicious or abnormal behavior occurring in the network.
Abnormal/malicious traffic detection in CCI using Cisco Stealthwatch

Stealthwatch has many inbuilt machine learning algorithms that can assist a network security professional in detecting abnormal/malicious traffic in the network. It can detect abnormal behavior and provide the IP address of the device that is causing the propagation. This information greatly simplifies the detection process.

- Stealthwatch detects a possible infiltration or abnormal traffic activity using NetFlow in the CCI network by raising an alarm under High Concern index
- SMC reports an alarm indicating that there is an abnormal/malicious activity in the network.
- CCI network security professional responds to the alarm by planning the remediation that involves further investigation and restricting access to the device causing the abnormal/malicious activity in the network
- The device/user causing abnormal/malicious activity in the network is identified with the help of Cisco ISE and the network security professional triggers policy action to quarantine the device access in the network

Secure Connectivity

- Secure Connectivity in the Access Network:
CCI Security Architecture and Design Considerations

- **LoRaWAN:**
  - LoRaWAN sensors and Network Server mutually authenticate in the Join procedure
  - LoRaWAN MAC messages are signed and encrypted
  - LoRaWAN payload information is encrypted

- **DSRC: Security Credential Management System (SCMS):**
  - Ensures integrity: users can trust that the message was not modified between sender and receiver
  - Ensures authenticity: users can trust that the message originates from a trustworthy and legitimate source
  - Ensures privacy: users can trust that the message appropriately protects their privacy
  - Interoperability: different vehicle makes, and models will be able to talk to each other and exchange trusted data without pre-existing agreements or altering vehicle designs
  - SCMS is one security concept under review for DSRC. SCMS is not documented in detail as part of CCI. More information can be found IN the *Security Credential Management System (SCMS) Proof Of Concept (POC)* at the following URL:

- **CR-Mesh:**
  - CR-Mesh Street Light Controllers (SLCs) are 802.1X authenticated endpoints
  - CR-Mesh perform 802.11i link layer encryption
  - CR-Mesh is an end-to-end encrypted access network
  - Control traffic between network elements is also encrypted

- **Security features at access switches:**
  - **Port-Based Authentication**
    - 802.1X is an IEEE standard for media-level (Layer 2) access control, offering the capability to permit or deny network connectivity based on the identity of the end user or device. 802.1X enables port-based access control using authentication. An 802.1X-enabled switch port can be dynamically enabled or disabled based on the identity of the user or device that connects to it. Refer to the following URL for more details on 802.1X:
    - MAC Authentication Bypass (MAB): MAB enables port-based access control using the MAC address of the endpoint. A MAB-enabled port can be dynamically enabled or disabled based on the MAC address of the device that connects to it. In a network that includes both devices that support and devices that do not support IEEE 802.1X, MAB can be deployed as a fallback, or complementary, mechanism to IEEE 802.1X. In CCI, endpoints that do not support IEEE 802.1X, MAB can be deployed as a standalone authentication mechanism.
  - It is recommended to enable 802.1X and MAB as fallback for 802.1X in each access port in CCI access network(s), for endpoints “host-on-boarding”, authentication and authorization using Cisco ISE.
CCI Network QoS Design

- Bandwidth control:
  - Rate limit and QoS policy to limit bandwidth for devices and/or types of traffic
  - Prevents a malicious user taking up the bandwidth and starve critical application traffic, a Denial of Service (DoS) attack

- Port security with static MAC:
  - Limits the number of MAC addresses that are able to connect to a switch and ensures only approved MAC addresses are able to access the switch
  - Packets with unknown source MAC address are dropped

  Trusted endpoint devices:

  - User Devices:
    - Umbrella: Umbrella is a service to set up endpoint devices to use the public Umbrella DNS servers where a set of policies is defined what endpoint devices are allowed to access or not
    - AMP for Endpoints: Cisco AMP for Endpoints prevents threats at point of entry and continuously tracks every file it lets onto the endpoint devices
    - Duo Beyond: Duo uses two-factor authentication secure single sign-on to provide end-users consistent user experience to access any cloud or on-premises application without go through a VPN

  - IoT Devices:
    - Certificates: ECC-based certificate for mutual authentication with network within which the device operates
    - Manufacture Usage Description (MUD) URI: Embedded MUD URI to download from MUD URI server for defining device default behavior. MUD information can be used with ISE to enforce policy.
    - MUD is fully described in RFC 8520.

CCI Network QoS Design

Quality of Service refers to the ability of a network to provide preferential or differential services to selected network traffic. QoS is required to ensure efficient use of network resources while still adhering to the business objectives. This chapter covers CCI QoS design considerations and recommendations for various CCI network traffic classes and it includes the following topics:

- CCI Wired Network QoS design, page 48
- CCI Wireless Network QoS Design, page 62
- QoS Considerations on RPoP, page 66

CCI Wired Network QoS design

QoS refers to network control mechanisms that can provide various priorities to different CCI endpoints or traffic flows or to guarantee a certain level of performance of a traffic flow in accordance with requests from the application program. By providing dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics, QoS can ensure better service for selected network traffic.

The CCI network architecture consists of different kinds of switches and routers with different feature sets. In order to streamline traffic flow, differentiate network services and reduce packet loss, jitter and latency, a well-designed QoS model is very important to guarantee network performance and operation. This section discusses the CCI QoS design considerations taken into account for various traffic classes in the CCI wired network architecture.
It includes QoS design considerations on fabric devices of CCI i.e. Cisco Catalyst 9300 Switches stack and 9500 switches StackWise Virtual (SVL) and Ethernet access rings consisting of Cisco Industrial Ethernet (IE) switches.

**QoS Design for Fabric Devices**

You can configure QoS in CCI fabric devices in CCI PoPs, transit site and HQ/DC site Fabric-in-a-Box (FiAB) switches using Cisco DNA Center. These fabric devices are Cisco Catalyst 9300 Series Switches stack and Cisco Catalyst 9500 Switches SVL and Cisco DNA Center uses application policies to configure QoS on these devices in the network.

**Note:** QoS application classes and queuing profile design recommendations discussed in this section are based on application traffic-classes and output queuing profile templates available in Cisco DNA Center application policy feature, as shown in Figure 2. The queuing profile configuration in Cisco DNA Center requires a minimum of at least 1% bandwidth allocation for each of the application traffic-class.

**Figure 23  Cisco DNA Center Application Queuing Profile Template**

Refer to the following URL, for more details on Cisco DNA Center QoS policies:


Cisco DNA Center Application policies comprise these basic parameters:

- **Application Sets**—Sets of applications with similar network traffic needs. Each application set is assigned a business relevance group (business relevant, default, or business irrelevant). For applications in the Relevant Business category, Cisco DNA Center assigns traffic classes to applications based on the type of application. It is recommended that QoS parameters in each of the three groups are defined based on this Cisco Validated Design (CVD). You can also modify some of these parameters to more closely align with your objectives.

- **Site Scope**—Sites to which an application policy is applied. If you configure a wired policy, the policy is applied to all the wired devices in the site scope. Likewise, if you configure a wireless policy for a selected service set identifier (SSID), the policy is applied to all of the wireless devices with the SSID defined in the scope.
Cisco DNA Center takes all of these parameters and translates them into the proper device CLI commands. When you deploy the policy, Cisco DNA Center configures these commands on the devices defined in the site scope.

Cisco DNA Center Application Policy constructs and their organization are depicted in Figure 24 below:

**Figure 24  Cisco DNA Center Application Policy Constructs**

- **Applications and Application Sets**: Applications are the software programs or network signaling protocols. Cisco DNA Center recognizes over 1400 distinct applications listed in the Cisco Next Generation Network-Based Application Recognition (NBAR2) library, including over 150 encrypted applications. Each application is mapped into similar industry standards-based traffic classes, as defined in RFC 4594. The traffic classification defines a Differentiated Services Code Point (DSCP) marking, queuing, and dropping policy to be applied based on the business relevance group to which it is assigned.

- **Custom applications** can be defined for wired devices that are not included in NBAR2. Custom applications can be defined based on server name, IP address and port, or URL. DSCP and port can also be specified for custom applications.

  **Note**: Given the specialist nature of many of the typical applications and use cases supported by CCI, there is a significant likelihood that there will be important or business critical applications that are not part of NBAR2 and hence it is recommended that special attention be paid to the potential need to define Custom Applications for Policy purposes.

- **Queuing Profile**: Queueing profiles define an interface’s bandwidth allocation based on the interface speed and the traffic class.

- **Business-Relevance**: Three classes of business-relevance groups are defined:
  - **Business Relevant**: Maps to industry best-practice preferred-treatment recommendations prescribed in IETF RFC 4594.
  - **Default**: Maps to a neutral-treatment recommendation prescribed in IETF RFC 2474 as “Default Forwarding.”
  - **Business Irrelevant**: Maps to a deferred-treatment recommendation prescribed in IETF RFC 3662

  **Note**: RFC 4594 QoS provides guidelines for marking, queuing, and dropping principles for different types of traffic. Cisco has made a minor modification to its adoption of RFC 4594, namely the switching of Call-Signaling and Broadcast Video markings (to CS3 and CS5, respectively).
- **Unidirectional and Bidirectional Application Traffic:** By default, the Cisco DNA Center configures all applications on switches and wireless controllers as unidirectional, and on routers as bidirectional. However, any application within a particular policy can be updated as unidirectional or bidirectional.

- **Consumers and Producers:** A traffic relationship between applications (a-to-b traffic flow) can be defined that needs to be handled in a specific way. The applications in this relationship are called producers and consumers. Setting up this relationship allows you to configure specific service levels for traffic matching this scenario.

- **Cisco DNA Center** configures QoS policies on devices based on the QoS feature set available on the device. For more information about QoS implementation, refer to the Cisco DNA Center User Guide at the following URL:


**Note:** QoS configuration using Cisco DNA Center application policy is currently not supported (as of SD Access release 2.1.2) on Extended Nodes (Cisco Industrial Ethernet 4000, IE 5000, IE 3300 and ESS 3300 series switches) and Policy Extended Node (IE 3400 switch) devices and DC-ENs and DC-PENs in the ring. This Cisco DNA Center bases its marking, queuing, and dropping treatments on IETF RFC 4594 and the business relevance category that you have assigned to the application.
QoS Classification, Marking and Queuing Policy

Cisco DNA Center bases its marking, queuing, and dropping treatments based on Cisco’s implementation of RFC 4594 and the business relevance category that you have assigned to the application. Cisco DNA Center assigns all of the applications in the Default category to the Default Forwarding application class and all of the applications in the Irrelevant Business category to the Scavenger application class. For applications in the Relevant Business category, Cisco DNA Center assigns traffic classes to applications based on the type of application.

Application Policy feature in Cisco DNA Center provides a non-exhaustive list of all applications or traffic classes in a network, as shown in Table 5 below. Table 5 also shows CCI network applications or traffic classes that are mapped to the applications classes in Cisco DNA Center for deploying QoS ingress classification, marking and egress queuing policies in fabric devices.
Table 5  Cisco DNA Center QoS Application Classification and Queuing Policy
<table>
<thead>
<tr>
<th>Business Relevance</th>
<th>Application Class</th>
<th>Per-Hop Behavior</th>
<th>Queuing and Dropping</th>
<th>Application Description</th>
<th>CCI Traffic Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relevant</td>
<td>Voice</td>
<td>Expedited Forwarding (EF)</td>
<td>Priority Queuing (PQ)</td>
<td>VoIP telephony (bearer-only) traffic; for example, Cisco IP phones</td>
<td>IoT Voice traffic</td>
</tr>
<tr>
<td></td>
<td>Broadcast Video</td>
<td>Class Selector (CSS)</td>
<td>PQ</td>
<td>Broadcast TV, live events, video surveillance flows, and similar inelastic streaming media flows; for example, Cisco IP Video Surveillance and Cisco Enterprise TV. (Inelastic flows refer to flows that are highly drop sensitive and have no retransmission or flow-control capabilities or both.)</td>
<td>IoT Video traffic. (Eg., CCTV camera traffic)</td>
</tr>
<tr>
<td>Real-time Interactive</td>
<td>CS4</td>
<td>PQ</td>
<td>Priority Queuing (PQ)</td>
<td>Inelastic high-definition interactive video applications and audio and video components of these applications; for example, Cisco TelePresence.</td>
<td>IoT real-time interactive video traffic. (Eg., Video enabled interactive Station Kiosk)</td>
</tr>
<tr>
<td>Multimedia Conferencing</td>
<td>Assured Forwarding (AF) 41</td>
<td>Bandwidth (BW) Queue and Differentiated Services Code Point (DSCP) Weighted Random Early Detect (WRED)</td>
<td>Desktop software multimedia collaboration applications and audio and video components of these applications; for example, Cisco Jabber and Cisco WebEx.</td>
<td>IoT audio &amp; video conferencing traffic.</td>
<td></td>
</tr>
<tr>
<td>Multimedia Streaming</td>
<td>AF31</td>
<td>BW Queue and DSCP WRED</td>
<td>Video-on-Demand (VoD) streaming video flows and desktop virtualization applications, such as Cisco Digital Media System.</td>
<td>Not business relevant, move to Default</td>
<td></td>
</tr>
<tr>
<td>Network Control</td>
<td>CS6</td>
<td>BW Queue only</td>
<td>Network control-plane traffic, which is required for reliable operation of the enterprise network such as EIGRP, OSPF, BGP, HSRP, and Internet Key Exchange (IKE).</td>
<td>IT &amp; OT Network control &amp; NetFlow traffic. (Eg., WLC-AP CAPWAP control traffic)</td>
<td></td>
</tr>
<tr>
<td>Signaling</td>
<td>CS3</td>
<td>BW Queue and DSCP</td>
<td>Signaling protocol like SCCP, SIP, H.323 etc., IP voice and video telephony signaling.</td>
<td>IT signaling protocols traffic</td>
<td></td>
</tr>
<tr>
<td>Operations, Administration, and Management (OAM)</td>
<td>CS2</td>
<td>BW Queue and DSCP</td>
<td>Network operations, administration, and management traffic, such as SSH, SNMP, and syslog.</td>
<td>IT &amp; OT Network Management traffic</td>
<td></td>
</tr>
<tr>
<td>Transactional Data &amp; All other IoT traffic</td>
<td>AF21</td>
<td>BW Queue and DSCP WRED</td>
<td>Interactive (foreground) data applications, such as enterprise resource planning (ERP), customer relationship management (CRM), and other database applications.</td>
<td>All remaining IoT traffic in CCI. (includes SCADA, Lighting, Parking sensor traffic)</td>
<td></td>
</tr>
</tbody>
</table>
CCI Network QoS Design

<table>
<thead>
<tr>
<th>Business Relevance</th>
<th>Application Class</th>
<th>Per-Hop Behavior</th>
<th>Queuing and Dropping</th>
<th>Application Description</th>
<th>CCI Traffic Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Default Forwarding</td>
<td>DF</td>
<td>Default Queue and RED</td>
<td>Default applications and applications assigned to the default business–relevant group. Because only a small number of applications are assigned to priority, guaranteed bandwidth, or even to differential service classes, the vast majority of applications continue to default to this best-effort service.</td>
<td>All default traffic classes</td>
</tr>
<tr>
<td>Irrelevant</td>
<td>Scavenger</td>
<td>CS1</td>
<td>Minimum BW Queue</td>
<td>Non business–related traffic flows and applications assigned to the business–irrelevant group, such as data or media applications that are entertainment-oriented. Examples include YouTube, Netflix, iTunes, and Xbox Live.</td>
<td>All other traffic not categorized and CCI quarantine network traffic</td>
</tr>
</tbody>
</table>

**Note:** As per RFC 4594, the Broadcast Video service class is recommended for applications that require near–real–time packet forwarding with very low packet loss of constant rate and variable rate inelastic traffic sources that are not as delay sensitive as applications using the Real–Time Interactive service class. Such applications include broadcast TV, streaming of live audio and video events, some video–on–demand applications, and video surveillance.

**Queuing Profile Bandwidth Allocation and Policing**

The policing function limits the amount of bandwidth available to a specific traffic flow or prevents a traffic type from using excessive bandwidth and system resources. A policer identifies a packet as in or out of profile by comparing the rate of the inbound traffic to the configuration profile of the policer and traffic class. Packets that exceed the permitted average rate or burst rate are out of profile or nonconforming. These packets are dropped or modified (marked for further processing), depending on the policer configuration.

The following policing forms or policers are supported for QoS:

- Single–rate two–color policing
- Dual–rate three–color policing

Application Policy makes use of a queuing profile with bandwidth allocation for each class of traffic defined in Table 5 and configures QoS commands on devices as per the queuing profile defined. Cisco DNA Center QoS application policy configures single rate two–color policing on the egress interfaces. Based on different classes of traffic in CCI (as shown in Table 5), it is recommended to allocate bandwidth in queuing profile for each of these traffic classes as shown in Table 6.
CCI Network QoS Design

Table 6  CCI QoS Traffic Profile

<table>
<thead>
<tr>
<th>Business Relevance</th>
<th>Application Class</th>
<th>CCI Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relevant</td>
<td>Voice</td>
<td>5%</td>
</tr>
<tr>
<td></td>
<td>Broadcast Video</td>
<td>15%</td>
</tr>
<tr>
<td></td>
<td>Real-time Interactive</td>
<td>10%</td>
</tr>
<tr>
<td></td>
<td>Multimedia Conferencing</td>
<td>10%</td>
</tr>
<tr>
<td></td>
<td>Multimedia Streaming</td>
<td>1%</td>
</tr>
<tr>
<td></td>
<td>Network Control</td>
<td>5%</td>
</tr>
<tr>
<td></td>
<td>Signaling</td>
<td>2%</td>
</tr>
<tr>
<td></td>
<td>Operations, Administration, and Management (OAM)</td>
<td>3%</td>
</tr>
<tr>
<td></td>
<td>Transactional Data, IoT Traffic</td>
<td>30%</td>
</tr>
<tr>
<td></td>
<td>Bulk Data</td>
<td>3%</td>
</tr>
<tr>
<td></td>
<td>(High-Throughput Data)</td>
<td></td>
</tr>
<tr>
<td>Default</td>
<td>Default Forwarding (Best Effort)</td>
<td>Remaining 15%</td>
</tr>
<tr>
<td>Irrelevant</td>
<td>Scavenger</td>
<td>1%</td>
</tr>
</tbody>
</table>

CCI QoS Considerations

- Each port in Cisco Catalyst 9300 and 9500 Series switches in supports eight egress queues, of which two can be given a priority (i.e., 2P6Q3T Queuing model). Table 3 shows an egress queuing and policing policy for different classes of traffic in CCI network.

- It is recommended to classify CCI network traffic as shown in Table 3. Classification and Marking should be applied to all traffic types at its entry point into the network, on the ingress port, for the entire network hierarchy, regardless of available bandwidth and expected traffic.

- Classify IoT use case traffic into Transactional data class and provide QoS treatment both in terms of bandwidth and priority. If distinction is possible, IoT control traffic needs to get priority similar to network control traffic and IoT management traffic similar to network management/telemetry data. If distinction is not possible, classify all IoT traffic similar to transactional data traffic. However, it is preferable to not mix IoT traffic with network control traffic, but instead keep a separate queue for IoT traffic.

- Limit total priority queuing traffic (LLQ) to 33% of link capacity, apply unconditional policing, to bound application response time of non-priority applications. No strict priority traffic recommended.

- Select only desired applications and corresponding application sets from the NBAR2 library. Most of the enterprise apps can be found in NBAR2 library.

- Custom applications may be defined when source marking is not done. This is based on destination “Server IP/Port or URL.” Producer-Consumer-based classification can be used in specific cases.

  **Note:** NBAR2-based traffic classification and marking is configured in the ingress policy. Ingress policy is applied only to devices in access role on access port. For devices with non-access role (distribution, border, and core), only the queuing profile is applied at the egress port.

- Traffic from different IoT CCI solutions (e.g., Smart Street Lighting with CR-Mesh, LoRaWAN, DSRC for Roadways, LoRaWAN for parking, or IP Camera traffic for Safety and Security). As per the recommendation of this guide, this traffic is marked distinctly as IoT Traffic for QoS treatment. This is only a sample list for IoT traffic; the operator can refine the list to match specific deployment needs.
Note: The application policy defined by the Cisco DNA Center can be deployed to all desired sites for the selected devices and ports, except for IE switches. Thus, the application policy is applied to the uplink traffic from IE switches starting from distribution switches to the Fabric Edge.

Ethernet Access Ring QoS Design

This section covers QoS design for CCI Ethernet access ring consisting of Cisco Industrial Ethernet (IE) 4000, IE 5000, IE 3300, ES 3300, and IE 3400 Series switches in the daisy-chained ring topology configuration in CCI PoP. Cisco DNA Center does not support application policy (QoS) provisioning on these switching platforms in SD Access release 2.1.2.0. Hence, it is recommended to configure QoS on these platforms using Cisco DNA Center Day N templates feature.

IE4000 and IE5000 Series Switches QoS Design

Classification and Marking

Classification distinguishes one kind of traffic from another by examining the fields in the packet header. When a packet is received, the switch examines the header and identifies all key packet fields. A packet can be classified based on an ACL, on the DSCP, the CoS, or the IP precedence value in the packet, or by the VLAN ID. You use a Modular QoS CLI (MQC) class map to name a specific traffic flow (or class) and to isolate it from all other traffic. A class map defines the criteria used to match against a specific traffic flow to further classify it. If you have more than one type of traffic that you want to classify, you can create another class map and use a different name.

You can use packet marking in input policy maps to set or modify the attributes for traffic belonging to a specific class. After network traffic is organized into classes, you use marking to identify certain traffic types for unique handling. For example, you can change the CoS value in a class or set IP DSCP or IP precedence values for a specific type of traffic. These new values are then used to determine how the traffic should be treated. You can also use marking to assign traffic to a QoS group within the switch.

Traffic marking is typically performed on a specific traffic type at the ingress port. The marking action can cause the CoS, DSCP, or precedence bits to be rewritten or left unchanged, depending on the configuration. This can increase or decrease the priority of a packet in accordance with the policy used in the QoS domain so that other QoS functions can use the marking information to judge the relative and absolute importance of the packet. The marking function can use information from the policing function or directly from the classification function.

- In CCI, it is recommended to mark QoS DSCP values at the source endpoint of the traffic flow, when the source endpoints support QoS DSCP marking. Source DSCP marking is trusted at ingress port on the IE switch to which the endpoint is connected.

- It is recommended to classify and mark the packets (for all other traffic types that cannot be source marked) at its entry point into the network, on the ingress port, for the entire network hierarchy, regardless of available bandwidth and expected traffic.

- For IoT application/sensor data traffic for which if the device source marking is not possible, it is suggested to classify and mark the IoT traffic using Classification based on QoS ACL method (IP ACLs)

- Depending on the traffic class and marking (if source marking is done) at the ingress IE switch port, you can trust/re-mark the ingress Layer 3 DSCP marking and set the QoS group for egress output policy classification in the switch. A QoS group is an internal label used by the switch to identify packets as a member of a specific class. The label is not part of the packet header and is restricted to the switch that sets the label. QoS groups provide a way to tag a packet for subsequent QoS action without explicitly marking (changing) the packet.

  Note: NBAR2 based classification and marking is not supported on Cisco Industrial Ethernet Switching platforms.

- It is recommended to classify and configure DSCP value of CS1 (Scavenger class) marking for the unknown hosts/endpoints in the quarantine VN. All endpoints/hosts which connect to IE ring are initially assigned with a quarantine VLAN (in quarantine VN) if initial 802.1X/MAB does not allocate to a trusted VN, or if the access port is
not statically mapped to a trusted VN. The endpoints/hosts that are successfully authenticated (using 8021.X/MAB) and authorized (i.e., become trusted endpoints) for network access in a respective VN in CCI. Hence, the endpoints must do source DSCP marking once it is authorized in the network so that source marking is trusted and not changed at IE switch ingress port. For QoS policy for both the untrusted quarantined endpoints, and the trusted endpoints that can’t do source marking, it is recommended to match on the IP subnets (IP ACL).

Queuing and Policing

Queuing establishes buffers to handle packets as they arrive at the switch (ingress) and leave the switch (egress). Each port on the switch has ingress and egress queues. Both the ingress and egress queues use an enhanced version of the tail-drop congestion-avoidance mechanism called weighted tail drop (WTD). WTD is implemented on queues to manage the queue lengths and to provide drop precedence for different traffic classifications. Each queue has three thresholds to proactively drop packets before queues fill up. Traffic classes assigned to thresholds 1 or 2 will be dropped if the queue buffer has reached the assigned threshold. Traffic classes assigned to a threshold of 3 for a specific queue will only be dropped if that queue has filled its buffer space.

Both Cisco Industrial Ethernet (IE) 4000 and 5000 Series switches in access ring support four egress queues, out of which one queue can be given a priority (i.e., 1P3Q3T Queuing model). Voice and CCTV Camera or other real-time interactive video traffic classes in the CCI network are prioritized with unconditional policing at 30% of interface bandwidth rate.

- Limit total priority queuing traffic (LLQ), apply unconditional policing with bandwidth percent (30% of link capacity), to bound application response time of non-priority applications. No strict priority traffic recommended.
- Class-Based Weighted Fair Queuing (CBWFQ) with Waited Tail Drop (WTD) is recommended for remaining classes of traffic in the rest of the egress queue.

Figure 25 shows traffic classes (input policy) and queue mapping (output policy) design for Cisco Industrial Ethernet (IE) 4000 and 5000 Series in the access ring.
Table 7 shows QoS configuration with WTD recommendation for output queue buffer for Cisco Industrial Ethernet (IE) 4000 and IE 5000 Series switches in the access ring.

<table>
<thead>
<tr>
<th>Application Class</th>
<th>Per-Hop Behavior</th>
<th>Queuing and Dropping</th>
<th>Queue and Queue-limit</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice IoT traffic</td>
<td>Expedited Forwarding (EF)</td>
<td>Priority Queuing (PQ)</td>
<td>Priority Queue (Queue 1)</td>
<td>30%</td>
</tr>
<tr>
<td>Broadcast Video IoT Traffic</td>
<td>Class Selector (CS) 5</td>
<td>Priority Queuing (PQ)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Real-time Interactive IoT Traffic</td>
<td>Class Selector 4 (CS4)</td>
<td>Priority Queuing (PQ)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 7  CCI QoS Configuration for Cisco IE 5000/4000 Series Switches

<table>
<thead>
<tr>
<th>Application Class</th>
<th>Per-Hop Behavior</th>
<th>Queuing and Dropping</th>
<th>Queue and Queue-limit</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Control</td>
<td>CS7</td>
<td>CBWFQ Queue and WTD</td>
<td>Queue 2 queue-limit 272</td>
<td>51%</td>
</tr>
<tr>
<td>Internet Control</td>
<td>CS6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Signaling</td>
<td>CS3</td>
<td>CBWFQ Queue and WTD</td>
<td>Queue 2 queue-limit 128</td>
<td></td>
</tr>
<tr>
<td>Multimedia Conferencing</td>
<td>AF4</td>
<td>CBWFQ Queue and WTD</td>
<td>Queue 2 queue-limit 48</td>
<td></td>
</tr>
<tr>
<td>Multimedia Streaming</td>
<td>AF3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operations, Administration, and Management (OAM)</td>
<td>CS2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transactional Data, other IoT Traffic (lighting, parking etc.,)</td>
<td>AF2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bulk Data (High-Throughput)</td>
<td>AF1</td>
<td>CBWFQ Queue and WTD</td>
<td>Queue 3 queue-limit 272</td>
<td>4%</td>
</tr>
<tr>
<td>Scavenger &amp; Quarantine Traffic</td>
<td>CS1</td>
<td>CBWFQ Queue and WTD</td>
<td>Queue 3 queue-limit 128</td>
<td></td>
</tr>
<tr>
<td>Default Forwarding (Best Effort)</td>
<td>DF</td>
<td>Class-default</td>
<td>Default Queue</td>
<td>15%</td>
</tr>
</tbody>
</table>

Refer to the following URL for more details on configuring QoS on Cisco Industrial Ethernet (IE) 4000 and IE 5000 series switches:


IE3300, ESS 3300, and IE3400 Series Switches QoS Design

Classification and Marking

Cisco Industrial Ethernet (IE) 3300 and IE 3400 Series switches in the Ethernet access ring support 1P7Q2T egress queuing model. The traffic classification and marking design (input policy) for these switches in the access ring are same as Cisco Industrial Ethernet (IE) 4000 and IE 5000 Series, discussed in the section “IE4000 and IE5000 Series Switches QoS Design , page 57”.

Note: Cisco Industrial Ethernet (IE) 3300, ESS 3300, and IE 3400 Series switches support ingress policing. However, ingress policing along with NetFlow are mutually exclusive and it is not supported together on a switch port. Hence, it is recommended to configure only ingress classification and marking based QoS input policy, for these switches in the ring.

Class-Based Weighted Fair Queuing

Cisco Industrial Ethernet (IE) 3300, ESS 3300, and IE 3400 Series switches support only strict priority in the egress switch port. With strict priority queuing, the priority queue is constantly serviced. All packets in the queue are scheduled and sent until the queue is empty. Priority queuing allows traffic for the associated class to be sent before packets in other queues are sent. Strict priority queuing (priority without police) assigns a traffic class to a low-latency queue to ensure that packets in this class have the lowest possible latency. When this is configured, the priority queue is continually serviced until it is empty, possibly at the expense of packets in other queues. For fair egress queuing all the traffic classes in CCI network, it is recommended to configure CBWFQ in egress policy on these switching platforms.

You can configure class-based weighted fair queuing (CBWFQ) to set the relative precedence of a queue by allocating a portion of the total bandwidth that is available for the port. You use the bandwidth configuration command to set the output bandwidth for a class of traffic as a percentage of total bandwidth.
When you use the bandwidth configuration command to configure a class of traffic as a percentage of total bandwidth, this represents the minimum bandwidth guarantee (CIR) for that traffic class. This means that the traffic class gets at least the bandwidth indicated by the command but is not limited to that bandwidth. Any excess bandwidth on the port is allocated to each class in the same ratio in which the CIR rates are configured.

Figure 26 shows traffic classes (input policy) and queue mapping (output policy) design for Cisco Industrial Ethernet (IE) 3300, ESS 3300, and IE 3400 Series in the access ring.

Table 8 shows QoS configuration with bandwidth percent recommendation for output queue for Cisco Industrial Ethernet (IE) 3300 and IE 3400 Series switches in the access ring.
This section covers the QoS design for Wireless LAN (WLAN) access networks in CCI. Cisco Unified Wireless & Industrial Wireless products support Wi-Fi MultiMedia (WMM), a QoS system based on IEEE 802.11e that has been published by the Wi-Fi Alliance. Cisco Unified Wireless Network (CUWN) mesh over-the-top on CCI fabric and SD-Access Wireless designs support WLAN QoS based on QoS profiles, WMM policy used by WLC in the CCI.

Wireless LAN QoS features are an implementation of the Wi-Fi Alliance WMM certification, based on the IEEE 802.11e amendment. Any wireless client that is certified WMM can implement Wireless LAN QOS in the upstream direction (from the wireless client to the AP). Any client certified 802.11n or 802.11ac is also certified WMM.

Regardless of the client support (or lack of support) for WMM, Cisco access points support WMM and can be configured to provide wireless QoS in the downstream direction (from the AP toward the wireless clients), and in the upstream direction when forwarding wireless frames to the wired interface.

For more details on WLAN QoS and WMM, refer to the Cisco Unified Wireless QoS chapter in Enterprise Mobility Design Guide at the following URL:


### CCI Wireless Network QoS Design

This section covers the QoS design for Wireless LAN (WLAN) access networks in CCI. Cisco Unified Wireless & Industrial Wireless products support Wi-Fi MultiMedia (WMM), a QoS system based on IEEE 802.11e that has been published by the Wi-Fi Alliance. Cisco Unified Wireless Network (CUWN) mesh over-the-top on CCI fabric and SD-Access Wireless designs support WLAN QoS based on QoS profiles, WMM policy used by WLC in the CCI.

Wireless LAN QoS features are an implementation of the Wi-Fi Alliance WMM certification, based on the IEEE 802.11e amendment. Any wireless client that is certified WMM can implement Wireless LAN QOS in the upstream direction (from the wireless client to the AP). Any client certified 802.11n or 802.11ac is also certified WMM.

Regardless of the client support (or lack of support) for WMM, Cisco access points support WMM and can be configured to provide wireless QoS in the downstream direction (from the AP toward the wireless clients), and in the upstream direction when forwarding wireless frames to the wired interface.

For more details on WLAN QoS and WMM, refer to the Cisco Unified Wireless QoS chapter in Enterprise Mobility Design Guide at the following URL:


### Cisco Unified Wireless Mesh Access Network QoS Considerations

Following are key QoS considerations taken into account for WLAN QoS in CCI:

- WMM uses IEEE 802.1P Classification scheme which has eight user priorities (UP 0–7) that WMM maps to four access categories Voice (AC_VO), Video (AC_VI), Best Effort (AC_BE) and Background (AC_BK).

- WLC QoS profiles can be configured as "Metal Policies":
  - Platinum - Voice Applications
  - Gold - Video applications
  - Silver - Best effort
  - Bronze - Background

- CAPWAP control frames require prioritization so they are marked with a DSCP classification of CS6.
IoT WMM-enabled Wi-Fi clients have the classification of their frames mapped to a corresponding DSCP classification for CAPWAP packets to the WLC. Based on WLAN/SSID QoS profile setting, the CAPWAP outer DSCP marking is capped to a maximum DSCP value allowed for that QoS profile. Eg., In a Video profile, DSCP would be capped to 34. When a WMM-enabled Wi-Fi client has a DSCP marking of EF and associates to a SSID with Video QoS profile settings, the CAPWAP packets DSCP value would be set to 34 for upstream traffic (AP -> WLC).

- This DSCP value is translated at the WLC to a CoS value on 802.1Q frames leaving the WLC interfaces.

- It is recommended to trust DSCP upstream on the WLC. When you trust DSCP upstream at WLC, DSCP is used instead of UP. DSCP is already used to determine the CAPWAP outer header QoS marking downstream. Therefore, the logic of downstream marking is unchanged. In the upstream direction though, trusting DSCP compensates for unexpected or missing UP marking. The AP will use the incoming 802.11 frame DSCP value to decide the CAPWAP header outer marking. The QoS profile ceiling logic still applies, but the marking logic operates on the frame DSCP field instead of the UP field.

- IoT Non-WMM Wi-Fi clients have the DSCP of their CAPWAP tunnel set to match the default QoS profile for that WLAN (SSID). For example, the QoS profile for a WLAN supporting Wi-Fi Cameras would be set to Gold, resulting in a DSCP classification of 34 (AF41) for data frames packets from that AP WLAN.

- The WMM classification used for traffic from the AP to the WLAN client is based on the DSCP value of the CAPWAP packet, and not the DSCP value of the contained IP packet. Therefore, it is critical that an end-to-end QoS system be in place.

- For WLAN (SSID) traffic which are locally switched at IE switch in the access ring, FlexConnect APs mark 802.1p value (UP) in the 802.1Q VLAN tag for upstream traffic. For downstream traffic, FlexConnect APs use the incoming 802.1Q tag from the Ethernet side and then use this to queue and mark the WMM values on the radio of the locally-switched VLAN.

**Wireless LAN QoS Model**

The QoS for the wireless traffic at the CCI wireless (Wi-Fi) LAN is enabled through QoS policies also known as metal policies (Platinum, Gold, Silver and Bronze) at Centralized WLC or Per PoP WLC. The WLAN for each Wi-Fi Service in CCI (Ex. Wireless Cameras, Public Wi-Fi etc..) is associated with a QoS policy. The QoS policy supports WMM UP and DSCP marking for the Wi-Fi traffic, as shown in Figure 27.
Figure 27  WLAN QoS Model for CCI

Figure 28 also represents the Wi-Fi traffic queuing and mapping in the radio backhaul interface for each MAP in a Centralized or Per–PoP WLC based CUWN Wi-Fi mesh access network in CCI.

Note: Ethernet Bridged Traffic of the endpoints connected to the Ethernet ports of MAPs are not CAPWAP encapsulated (no outer header for bridged Ethernet packets). DSCP marking of such end points is used to map the traffic to the right queue in the Wi-Fi backhaul. Hence, it is recommended to classify and mark the DSCP at source of Ethernet Bridged Traffic to ensure appropriate QoS treatment for the traffic in the radio backhaul.

- It is recommended to source mark CCTV Cameras connected to MAPs with DSCP value of CS5 to ensure appropriate QoS treatment for this traffic in CCI wired network, as discussed in the previous section. If source DSCP marking is not possible on the device, Ethernet access ring QoS should classify the device using ACLs and mark the packet with DSCP value of CS5 at the ingress port of the Ethernet switch in the ring.

- Wireless CCTV Camera traffic in a WLAN should be source marked with UP value of 5 (if UP marking is supported) with DSCP value of CS5 to ensure appropriate QoS egress queuing (AC_VI) in the radio backhaul. This ensures Wireless CCTV Cameras traffic QoS treatment as per CCI wired network QoS design.

- Any IoT Wi-Fi sensors or gateways connecting to WLAN should be configured with WMM UP value 2 (if WMM is supported) and DSCP value AF21 for Best Effort queuing in radio backhaul. Non–WMM based Wi-Fi sensors or gateways would be have the DSCP of their CAPWAP tunnel set to match the default QoS profile for that WLAN.

- Public Wi-Fi users or WLAN in the network is classified with UP value 1 and DSCP value CS1 for Background queuing in radio backhaul and QoS treatment in wired network.

SD-Access Wireless Network QoS Considerations

SD-Access wireless network architecture in CCI uses Fabric-enabled WLC (eWLC on C9300 Switch stack FiaB) which is part of fabric control plane and fabric enabled APs encapsulates fabric SSID or WLAN traffic in VXLAN, Hence QoS design and behavior for SD-Access Wi-Fi clients in CCI, is same as Wired QoS policy design considerations which are discussed in the section CCI Wired Network QoS design, page 48.

This section covers the SD-Access Wireless QoS design considerations between Fabric APs and WLC in CCI PoP for QoS treatment of Wi-Fi traffic. SD Access Wireless network with Fabric APs and WLC follow WLAN QoS and AVC policy model with WMM metal policies for traffic classification and remarking at WLC.
Fabric APs acts as access edge trust boundaries to trust upstream DSCP marking of Wi-Fi traffic and Fabric WLC (eWLC) acts as WLAN/SSID policy enforcement point (PEP) for remarking upstream Wi-Fi traffic DSCP using QoS policy. 

It is recommended to remark DSCP value at WLC using AVC policy as shown in Figure 27 for each class of Wi-Fi traffic to ensure appropriate QoS treatment for each class of traffic as per CCI wired network QoS design.

Wi-Fi traffic QoS treatment at wireless or radio access medium is based on DSCP (i.e, upstream DSCP trusting enabled at WLC) and DSCP-to-UP (downstream) mapping at AP.

Figure 28 shows an overview of SD Access Wireless QoS policy operation for Fabric WLC as PEP.

Figure 28    SD-Access Wireless QoS Policy Overview

Policy Overview Device Type = WLC

- Upstream
  - Trust DSCP at the Access Point
  - DSCP re-marked as per the AVC policy on WLC

- Downstream
  - DSCP re-marked as per the AVC policy on WLC
  - DSCP → UP mapping at the Access Point

CCI QoS Treatment for CR-Mesh and LoRaWAN Use Cases Traffic

The CCI network is used by several IoT use cases. Each IoT use case can generates different types of traffic. This section discusses QoS treatment specific to CR-Mesh (Eg., Cimcon Street Lighting and LoRaWAN FlashNet Street Lighting) use cases traffic.

CCI QoS Design Considerations for CR-Mesh Traffic

The CR-Mesh use case traffic to/from the Connected Grid Endpoint (CGE) passes through the FAR. The FAR router is connected to an IE series switch in Ethernet Access ring or connects to CCI via an RPoP cellular link. All traffic from the FAR is encrypted and tunneled to the headend router (HER) located at the DMZ. Individual CR-Mesh traffic flows are hidden to all intermediate nodes.

Entire tunneled traffic originating from a FAR can be given a single QoS treatment at the IE access switch to which the FAR is connected. Classification and marking can be done based on the interface to which the FAR is connected or based on the FAR subnet (ACL based classification). The FAR subnet is the source IP subnet used for tunneling the CR-Mesh traffic. As discussed earlier, since CR-Mesh is IoT traffic, all CR-Mesh traffic passing through the tunnel is marked with IP DSCP AF21. A minimum of 30% of the uplink port bandwidth is guaranteed for all IoT traffic marked with IP DSCP AF21 in the entire path. The IP DSCP marking is done on the outer header of the encapsulated packet. This outer header marking is used for QoS policy enforcement in the rest of the network.

QoS classification and marking is applied to CR-Mesh traffic at IE series switches and queuing policy is applied thereafter from the fabric edge onwards. As per customer’s needs, and where relevant, MPLS QoS mapping needs to be done at the service provider edge.
CCI QoS Design Considerations for LoRaWAN Traffic

Cisco Wireless Gateway for LoRaWAN access network aggregates all LoRaWAN Sensors traffic (Eg. FlashNet Lighting Controller) to ThingPark Enterprise (TPE) Network Server (NS) in CCI HQ/DC site. Since the LoRaWAN gateway is connected to an IE switch port in Ethernet access ring in a CCI PoP, it is recommended to follow Ethernet Access Ring QoS design, discussed previously in this section for the appropriate QoS treatment of LoRaWAN IoT traffic in CCI network.

LoRaWAN traffic from gateway is classified at IE switch ingress port using ACL similar to CR-Mesh traffic and marked with DSCP value of AF21 (IoT traffic) and egress queuing policy provides a minimum of 30% of interface bandwidth, as shown in Table 5 and Table 6.

QoS Considerations on RPoP

This section discusses the QoS design considerations on RPoP. RPoP multiservice network with dual-LTE cellular links have different upload/download bandwidth/throughput. QoS differentiation and prioritization of traffic must occur between RPoP and CCI headend, when forwarding sensitive data particularly when a WAN backhaul link offers a limited amount of bandwidth.

In the case of dual-WAN interfaces with different bandwidth capabilities (that is, cellular), QoS policies must be applied to prioritize the traffic allowed to flow over these limited bandwidth links, to determine which traffic can be dropped, etc.

On a multi-services RPoP, QoS DSCP can apply to traffic categorized as:

- CCTV Camera
- SCADA protocol translation (DNP3 Serial to DNP3/IP), FlashNet Street Lighting traffic via LoRaWAN access gateways
- Wi-Fi services
- Network Control (For example, CAPWAP control) & Management traffic (For example, FND traffic)

Table 9 lists the different traffic priorities and an example egress queue mapping at RPoP gateway among multiple services. Each of these services can be classified using DSCP marking.

Note: Table 9 lists an example egress queue mapping when all four of these services are required in RPoP. Depending on the services required at RPoP, the egress queue mapping at RPoP gateway can be configured among available egress queues.
Table 9  CCI RPoP QoS Policy for marking and queuing

<table>
<thead>
<tr>
<th>Application Class</th>
<th>Per-Hop Behavior</th>
<th>Queuing</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCTV Camera traffic, Traffic Signal Controller &amp; Network Control Traffic</td>
<td>CS5, CS4, CS6</td>
<td>High Priority Queue (LLQ)</td>
</tr>
<tr>
<td>SCADA &amp; LoRaWAN use cases</td>
<td>AF21</td>
<td>Medium Priority</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CBWFQ1</td>
</tr>
<tr>
<td>Wi-Fi Service &amp; Network Management</td>
<td>Client DSCP marking based on CCI traffic class &amp; QoS Profile at SSID, CS2</td>
<td>Medium Priority</td>
</tr>
<tr>
<td>Other</td>
<td>DF</td>
<td>Normal Priority</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default Queue</td>
</tr>
</tbody>
</table>

Note: QoS behavior is always on a per-hop basis. Even though the high priority traffic is prioritized at the RPoP Gateway, once the traffic enters the service provider’s network, the packets are subjected to the QoS treatment as defined by the service provider. In some scenarios, the service provider could even remark all the incoming packet’s priority to default priority. It is recommended to ensure an SLA if the QoS marking done at the gateway needs to be honored by the service provider (or) at least treated as per the SLA.

For more details on upstream and downstream QoS treatment between RPoP gateways and CCI headend (HER), refer to the following URL:


CCI Network Data Flow Diagrams

This chapter, which provides a pictorial representation of device and client onboarding data flows and east-west and south-north data flows, along with the role of different network components on the path, includes the following major topics:

- Onboarding Network Devices, page 68
- Onboarding Endpoints, page 70
- Data Flow within a Fabric Site, page 72
- Data Flow between Fabric Sites, page 75
- Data Flow between Host and Shared Services/Internet, page 76
Onboarding Network Devices

A fabric or a non-fabric device can be onboarded either through a discovery or a Plug and Play (PnP) process. PnP is a process for onboard ing a new device with Zero Touch Deployment (ZTD), without the need for pre-staging. PnP provisioning can be done for a planned device or unknown device. The planned process can be initiated for a known set of devices. A pre-stage device can be discovered and added to theCisco DNA Center-managed network with the discovery process.

In the case of CCI, extended node devices can be onboarded with the PnP process and remaining devices such as FiaB, IP-Transit, and Nexus (DC switch) can be onboarded with the discovery process.

Figure 29 Discovery and PnP Process Data Flow

Common Prerequisite Steps at Cisco DNA Center for Device Onboarding and Provisioning

1. Global configuration at Cisco DNA Center:
   a. Network: ISE for Network devices, ISE for Client devices, DHCP, DNS, Syslog, SNMP, NTP, and Time Zone
Connected Communities Infrastructure Solution Design Guide

CCI Network Data Flow Diagrams

b. Device credentials: CLI, SNMP, and HTTPS
c. IP Address Pools (global and sub-pools)

2. DHCP server configurations: Configure DHCP pools and Cisco DNA Center IP address in DHCP option 43.

Onboarding Devices with PnP Process

Devices, such as IE 4000, IE 5000, IE3300 and IE3400 series switches, operating as Extended Nodes (ENs) and Policy Extended Nodes (PENs), but not Daisy Chained Extended Nodes (DC-ENs) or Daisy Chained Policy Extended Nodes (DC-PENs), are onboarded with the PnP process. Steps for the PnP process are as follows:

Onboarding Extended Node/Policy Extended Node devices with Plug and Play

1. Write-erase PnP compatible device to be onboarded (PnP agent is part of IOS and IOS XE images), and plug in to the access switch having Layer 3 reachability to the Cisco DNA Center.

2. PnP agent initiates DHCP discovery with option 60 and “ciscopnp” string. Fabric Edge (FiaB) detects it to be an EN/PEN, initiates a DHCP relay with EN VLAN (Infra VN) and thus gets an IP from the EN pool.

3. DHCP server returns the Cisco DNA Center IP address in option 43. PnP agent initiates the PnP process with the Cisco DNA Center using https. Traffic is mapped to Infra VN.

4. Device appears in the Cisco DNA Center PnP list. If the device is an unknown device, its PnP state is set to unclaimed; if it is a planned device, the PnP state goes to onboarding.

5. For planned devices, onboarding workflow is initiated automatically. For unknown devices, the operator claims the device manually and follows the onboarding workflow.

6. On completion of onboarding, the PnP state is updated to provisioned.

Onboarding DC-ENs/DC-PENs with Plug and Play

DC-ENs or DC-PENs in the Ethernet access ring can be discovered and provisioned using Cisco DNA Center Day N templates. Refer to the section “Ring Topology, page 93” for more details on templates-based daisy-chained ring provisioning of DC-ENs and DC-PENs.

Onboarding Fabric Devices with Discovery

Fabric Nodes such as Cisco Catalyst 9300 and Cisco Catalyst 9400 series, Transit devices such as Cisco Catalyst 9500, Access switches are all onboarded to Cisco DNA Center with the discovery process. Steps for the discovery process are follows:

Prerequisites for Devices Discovery

1. Configure discovery credentials on the device (CLI, SNMP, SSH, HTTPS, and NETCONF) and plug in to an access switch that has Layer 3 reachability to the Cisco DNA Center.

2. Initiate the discovery process in the Cisco DNA Center choosing one of the discovery types (CDP, IP Range, or LLDP) by providing appropriate details (device credentials, CDP/LLDP: seed device IP, CDP/LLDP level, or IP Range).

3. Discovered devices added to Cisco DNA Center Inventory with last sync status as managed and provision state = not provisioned.

Following are the steps for device provisioning. All devices onboarded either through Discovery or PnP are added to the Cisco DNA Center inventory. All devices in inventory can be provisioned. The steps for provisioning devices present in the inventory are as follows:
Provisioning Devices in Cisco DNA Center Inventory

1. Site assignment only for discovered devices.
2. Provision devices in inventory (Assign Site - only for discovered devices, Apply Day N template).
3. Device provision status in inventory changes to Success.

Security Configuration During Onboarding Process

1. In the PnP process, device CLI credentials (username/passwords) are deployed by the Cisco DNA Center on the device. In a discovery process, the device credentials are manually configured.
2. The Cisco DNA Center pushes device identity credentials (username and password) to ISE, which matches the username and credentials that are pushed to the networking end device. These credentials are used by the Cisco DNA Center to authenticate itself to the networking device. Also, the other credentials such as RADIUS Secret for the networking device and CTS credentials are pushed to ISE so that the networking device can communicate with Cisco ISE using those credentials when using a respective protocol (for example, CTS credentials when using CTS protocols and RADIUS Secret when using the RADIUS protocol).
3. After the device is provisioned, the Cisco DNA Center authenticates the device with Cisco ISE. If Cisco ISE is not reachable (no RADIUS response), the device uses the local login credentials. If Cisco ISE is reachable, but the device does not exist in Cisco ISE or its credentials do not match the credentials configured in Cisco DNA Center, the device does not fall back to use the local login credentials. Instead, it goes into a partial collection state.

Onboarding Endpoints

Endpoints can be connected to CCI access switches in an EN ring or PEN ring. Cisco DNA Center supports Host Onboarding configuration for EN and PEN switches but not for DC-EN and DC-PEN switches in the ring. All DC-EN and DC-PENs switch port configurations for host onboarding can be automated and pushed using Day N template. The onboarding data flow is shown in Figure 30.
Groundwork for Onboarding Endpoints

1. Operator configures a policy set in ISE that specifies the conditions for authentication and authorization policies. A successful match in authentication policy allows access to the network, whereas a successful authorization policy results in downloading a policy element such as ACL, dACL, VLAN, or SGT. These policy elements aid an operator to define a network policy.

2. Operator configure SGTs and group-based access policy (SGACL) (security policy) in the Cisco DNA Center. The Cisco DNA Center auto-pushes SGT and group-based security policies to ISE.

3. Operator creates separate VNs for different service groups within a fabric domain where a service could be a use case or access technology, or however the CCI deployment is being segmented. Operator configures VNs for a fabric site by selecting IP-Pools. A separate IP-Pool is selected for each service within a VN. An EN IP Pool is selected for Infra-VN to enable infra-related communications.

4. Optionally, each IP-Pool operator can select a static SGT group.

5. While onboarding the fabric edge (FiaB), the Cisco DNA Center provisions specific configurations at the fabric edge (FiaB) device, including:
   - A separate VLAN interface is created for each configured IP-Pool in each VN, mandatory is Infra-VN. If an IP-Pool has a static SGT configured, it is pushed to the fabric edge (FiaB).
   - SGACL are provisioned with the help of ISE.
   - AAA and DHCP relay.

Onboarding Endpoints Connected to Cisco Industrial Ethernet (IE) Access Switch

From the Cisco DNA Center Host Onboarding process, only “No-Authentication” is supported as the authentication type for EN user ports. However, as stated earlier, it is recommended not to perform Host Onboarding for any EN ports from the Cisco DNA Center.
Through manual configuration using Day N templates, the following authentications can be enabled for an access port:

1. Pre-designated service port (No Authentication); respective Service-VLAN is pre-assigned to the port.
2. 802.1X/MAB authentication (Closed/Open loop); respective Service-VLAN is obtained from ISE on successful authentication.

**Technical Note:** The respective Service-VLAN assigned to Cisco Industrial Ethernet (IE) switch access port, either manually or through ISE on successful authentication, must be the same as the Service-VLAN auto selected by the Cisco DNA Center at the fabric edge (FiaB) for the given service IP-Pool.

### Data Flows

#### Data Flow for 802.1X Authentication and Service-VLAN Assignment

1. When the access port has 802.1X/MAB configured, endpoint will be requested to initiate 802.1X.
2. Endpoint at Fabric Site-A initiates 802.1X authentication. If the endpoint does not support 802.1X, after a timeout, the access switch will initiate MAB authentication request on behalf of the endpoint.
3. Cisco Industrial Ethernet (IE) access switch sends the request to ISE/AAA server, with VLAN: Infra VLAN, destination IP: AAA server.

   **Technical Note:** The same Infra VLAN number is configured as “radius source-interface vlan” on the Cisco Industrial Ethernet (IE) switch by the Day N template. (VLAN: Infra VLAN, Destination IP: AAA server)

5. ISE authenticates by matching credentials and assign authorization profile SGT or Service-VLAN as per user-group.
6. Response received by the fabric edge (FiaB) switch and forwarded to the Cisco Industrial Ethernet (IE) access switch.
7. Cisco Industrial Ethernet (IE) configures Service-VLAN on the access port and acknowledges 802.1X success to endpoint.

#### Data Flow for DHCP IP Assignment

As shown in previous steps, the access port is assigned with the respective Service-VLAN either statically or by ISE on successful authentication.

1. The endpoint initiates the DHCP request.
2. Access switch tags it with the respective Service-VLAN.
3. Fabric edge (FiaB) maps the respective Service-VLAN to the VN associated with the Service-VLAN. The DHCP relay is configured on the fabric edge (FiaB). The request is sent to the DHCP server with the source IP as Service-VLAN IP.
4. DHCP server allocates IP from Service-VLAN IP Pool.
5. Endpoint gets IP address.

#### Data Flow within a Fabric Site

As an example, for intra-fabric site data traffic flow, assume data flows between a source Endpoint-A1 in Fabric Site-A and a destination is Endpoint-A2 in Fabric Site-A. This is illustrated in Figure 31 and Figure 32.

2. Cisco Industrial Ethernet (IE) access switch tags with Service-VLAN.

3. If source and destination addresses are within the same Service-VLAN and are in one of the access switches en-route to FE/FiaB, then the destination is found in the local Forwarding Database of the destination switch, packet switched within the ring locally with no policy applied. Otherwise, packet is forwarded to the Fabric Edge (FiaB). (Figure 31).

4. Source Fabric Edge (FiaB) maps Service-VLAN to Service-VN, assigns Static SGT if configured. Derives binding information for the destination endpoint. Forwards the packet to destination Cisco Industrial Ethernet (IE) switch.

5. Performs access check consulting SGACL and takes forwarding decision. If permit, forwards the packet to destination Cisco Industrial Ethernet (IE) switch; if deny, drops the packet. (Figure 32).

6. Destination Cisco Industrial Ethernet (IE) switch forwards the packet to destination Endpoint-A2.
Figure 32  Data Flow within a Fabric Site and between Access Switches across same Fabric Edge

Figure 33  IP Transit: Data Flow between Access Switches across same Fabric Edge
Connected Communities Infrastructure Solution Design Guide

CCI Network Data Flow Diagrams

Data Flow between Fabric Sites

As an example, for the inter-fabric site data traffic flow, assume data flows between a source Endpoint-A1 in Fabric Site A and a destination Endpoint-B1 in Fabric Site B. This is illustrated in Figure 34.

Figure 34  Data Flow between Hosts of Different Fabric Sites across SD-Access Transit

2. Cisco Industrial Ethernet (IE) access switch tags Service-VLAN.
3. Source Fabric edge (FiaB) maps Service-VLAN to Service-VN.
4. Source Fabric edge tags source SGT either from static SGT configured for the IP-Pool or from dynamic SGT obtained from ISE. Forwards the packet to destination Fabric.
5. In the case of the SD-Access Transit, source SGT is carried via inline tagging from source fabric edge to destination fabric edge, as shown in Figure 34.
6. In the case of IP transit, source SGT is lost at the source fabric border. Destination fabric edge again derives the source SGT binding information, using SXP to ISE, as shown in Figure 35.
7. Both in SD-Access Transit and IP Transit cases destination fabric edge derives destination SGT binding information, performs access check consulting SGACL and takes forwarding decision. If permit, forward the packet to destination access switch; if deny, drop the packet.
8. Destination access switch forwards the packet to destination Endpoint-B1.

Data Flow between Host and Shared Services/Internet

As an example, for host-to-shared services/Internet data traffic flow, assume a data flow between a source Endpoint-A1 in Fabric-A and a destination is Endpoint-D1 either in the Data Center or in the Internet:

Figure 36 Data Flow between Host and Shared Services

1. Shared services and Internet are accessible to all endpoints in the network as they are outside of the fabric domain.

   **Note:** Access to the Internet can be blocked, of course, based on a number of techniques, but this is not covered in this CVD.


3. Cisco Industrial Ethernet (IE) access switch tags with Service-VLAN.

4. Source Fabric edge (FiaB) maps Service-VLAN to Service-VN, assigns Static SGT if configured. Forwards the request to transit. Transit forwards packet to shared services switch or Firewall. Packet switched/routed to destination.

5. No access check is performed at Transit, shared services switch, or Firewall. Note that firewall access rules can be defined, which are not related to security-group check.

CCI Multicast Network Traffic Design

Multicast is a group communication where data is transmitted to a group of destinations aka multicast receivers in a network. Protocol Independent Multicast (PIM) is a family of multicast routing protocols in IP networks that provides one-to-many and many-to-many distribution of data over a LAN or WAN. In CCI, the multicast streaming may be required to be enabled. For example, a use case in Cities need a Video Server (multicast source) in a DC site sending security or advisory video streams to a group of hosts (multicast destinations) in the PoP sites or a Content Server in a PoP sending messages to a group of Kiosks in that PoP. In CCI, the multicast source and destinations (or receivers) could be in the same PoP or across PoPs.

Cisco SD Access solution can support Protocol Independent Multicast Any Source Multicast (PIM-ASM) and Source Specific Multicast (PIM-SSM) protocols. The CCI multicast design leverages multicast packet forwarding design in SD Access fabric which supports multicast provisioning in two modes 1. Headend replication and 2. Native multicast.

Headend replication multicast forwarding in SD Access operates in the fabric overlay networks. It replicates each multicast packet at the Fabric border, for each Fabric edge receiver switch in the fabric site where multicast receivers are connected. This method of multicast traffic forwarding does not rely on any underlay multicast configurations in the SD Access network. It supports both PIM-ASM and SSM deployments.

Native multicast leverages an existing underlay network multicast configuration and the data plane in an SD Access network for multicast traffic forwarding. Each multicast group in the SD Access overlay (either PIM-ASM or PIM-SSM) maps to a corresponding underlay multicast group (PIM-SSM). This method significantly reduces load at fabric border
(head end) and reduces latency in a fabric site where fabric roles are distributed on different nodes. i.e., Border, Control Plane (CP) and Edge roles are on different fabric nodes with optional intermediate nodes in the fabric site. Note that, native multicast provisioning with PIM-ASM in the underlay is not supported by SD Access solution.

In CCI, each PoP is an SD Access fabric site with FiaB (i.e. Border, CP and Edge on same fabric node). Hence, there is no difference in these two deployment methods for multicast provisioning in CCI. Therefore, it is recommended to use “Headend replication” method in CCI. For example, a Greenfield CCI PoP deployment. This simplifies the multicast provisioning in CCI. The native multicast provisioning is preferred in a Brownfield field CCI PoP deployment if there is an existing PIM-SSM multicast configuration in the underlay network.

CCI supports following multicast designs:

- Multicast within a PoP
- Multicast between PoP Sites

Refer to “Multicast design within a PoP site, page 58” for multicast traffic forwarding within a CCI PoP in which both multicast source and destinations (or receivers) are connected.

Cisco SD Access solution does not support multicast forwarding between PoP sites interconnected via SD Access Transit. In CCI, multicast forwarding between PoPs can be enabled on a deployment where PoPs are interconnected via IP Transit. Refer to “Multicast design between PoP sites, page 62” for more details.

**Multicast Design in a PoP Site**

The multicast source can exist either within the overlay or outside the fabric. For PIM deployments, the multicast clients (receivers) in the overlay use a rendezvous point (RP) at the fabric border (FiaB in this case) that is part of the overlay endpoint address space. Cisco DNA Center configures the required multicast protocol support. The SD-Access solution supports both PIM source-specific multicast and PIM sparse mode (any-source multicast). Overlay IP multicast requires RP provisioning within the fabric overlay, typically using the border. When there are multiple borders, Cisco DNA Center will automatically configure Multicast Source Discovery Protocol (MSDP) between RPs.

PIM-ASM or PIM-SSM can be running in the PoP site overlay. In case of PIM-ASM, the RP is configured on FiaB (Fabric border of PoP site) as shown in Figure 37 & Figure 38. Each node (IE switch) in a PoP Ethernet access ring must be enabled with the IGMP feature by turning on IGMP snooping on each of the Cisco Industrial Ethernet (IE) switches in the L2 access ring. Enabling IGMP on Cisco Industrial Ethernet (IE) switches in the ring allows multicast traffic to be received only on the switch ports where multicast receiver(s) are connected. Multicast receivers sends either IGMP Join (in PIM-ASM) or IGMP v3 Join (in PIM-SSM) to the RP in the Fabric Edge for multicast forwarding.

**SD-Access Multicast Operation in PIM-ASM**

- Multicast receivers in the overlay and multicast source can be outside the fabric or in the fabric overlay within the PoP
- In PIM-ASM, wired multicast receiver(s) in the Ethernet access ring send IGMP join for a specific multicast group
- The PoP Fabric Edge (FiaB) receives it and does PIM Join fabric rendezvous point (RP) which is configured on the same FiaB border
- The RP needs to be present in the overlay network and its IP address is registered with Fabric control plane node (i.e. FiaB in a PoP)
- Fabric edge asks the fabric control plane for the location of RP address (IP-RLOC table) and based on the reply that the Fabric Edge sends PIM Join in the overlay to the RP
- From earlier, the RP now has a source and receiver information for a particular multicast group
- The FiaB will receive multicast source traffic, applied policy and then forwarded original IP multicast packet to Cisco Industrial Ethernet (IE) switch in the ring where the multicast receiver is connected.
In case of a distributed fabric roles deployment with intermediate nodes in the PoP site, The Fabric Border (FB) will send the multicast source traffic over a VXLAN tunnel to the RP and the RP will forward that traffic to the Fabric Edge (FE) over another VXLAN tunnel.

FS receives the VXLAN packets, decapsulates, applies policy and then sends original IP multicast packet to the port on which the receiver is connected.

Figure 37 illustrates the multicast network design for PIM-ASM configured in fabric overlay, for both multicast source and receiver(s) in the overlay network within a CCI PoP site.

**Figure 37  CCI Multicast within a PoP Site – PIM ASM**

Figure 38 illustrates the multicast network design for PIM-ASM configured in fabric overlay, for multicast receiver(s) in the overlay network within a CCI PoP site and multicast source is outside of the fabric.
In case of SDA wireless multicast clients (receivers):

- The client sends IGMP join for a specific multicast Group (G).
- AP encapsulates it in VXLAN and send it to the upstream switch.
- The Fabric Edge node (FE) receives it and does a PIM Join towards the Fabric Rendezvous Point RP (assuming PIM-SM is used).

**SD-Access Multicast Operation in PIM-SSM**

- Multicast client (receiver) is in the overlay, multicast source can be outside Fabric or in the overlay as well
- PIM-SSM needs to be running in the Overlay
- The client sends IGMP v3 join for a specific multicast Group (G)
- The Fabric Edge node (i.e FiaB) receives it and since the IGMP v3 join has the source address information for that multicast group it sends a PIM Join towards the source directly. In our case since the source is reachable through the border it sends the PIM join to the border.
- The fabric RP is not needed in a PIM SSM deployment
- In an SSM deployment, the source address is part of IGMP v3 join the edge will ask the control plane for the location of the source address (IP to RLOC Table) and based on the reply will send the PIM Join in the Overlay to the destination node.
If Border (i.e. FiaB) registered that source, then the PIM join is directly sent to Border.

If the source is not known in the fabric the PIM join is also sent to the Border (i.e. FiaB) as Border is the default exit point of the fabric.

From earlier, the FiaB (Border) knows clients which requested the specific multicast group and multicast traffic is sent to receivers connected to Edge or L2 access ring.

It works similarly for SDA wireless deployment as well.

Figure 39 illustrates the multicast network design for PIM-SSM configured in fabric overlay, for multicast receiver(s) in the overlay network within a CCI PoP site and multicast source is outside of the fabric or in the overlay in the fabric.

Figure 39  CCI Multicast PIM SSM – Multicast source outside of the Fabric

Note that RP is not needed in the fabric and multicast receivers sends IGMP v3 Join messages in PIM-SSM deployment.

**Multicast design between PoP Sites**

CCI network multicast receivers could be on different PoP sites and the multicast source could be in a PoP site or HQ site. In this case, multicast traffic must be forwarded across PoP sites interconnected via transit network in CCI. Since, SD Access transit provisioned in CCI network does not support multicast forwarding, IP transit-based multicast design across fabric is discussed and recommended in CCI for multicast traffic forwarding across PoP sites in CCI network.

Because each fabric or PoP site is considered as one multicast region, configuring PIM-ASM with RP provisioned on each PoP site fabric border (i.e. FiaB) via Cisco DNA Center and then configuring MSDP between RPs (connected via IP transit) for multicast traffic forwarding requires manual CLI configurations on fabric devices. Hence, it is recommended
to configure PIM-ASM with RP external and common to all PoP sites in CCI network i.e Fusion Router, as shown in Figure 40.

Figure 40  CCI Multicast design across PoPs interconnected via IP Transit

As shown in Figure 40, multicast is configured per Virtual Network (VN) on each PoP site with an external RP (RP on fusion router) common to all PoP site. A multicast source could be in HQ/DC site or shared services and receivers are in PoP sites. In this design, all IGMP messages from the multicast receiver(s) are forwarded to the central RP and RP anchors the multicast traffic forwarding to PoP sites where the receivers are connected as discussed in the section SD-Access Multicast operation in PIM-ASM page 56.

CCI Network High Availability

Failure of any part of the network (either network device or network link) can affect the availability of services. The impact of availability increases with the increase in the aggregation level of the failing node/link. Availability is improved by avoiding a single point of failure by means of high availability (HA) or redundancy. Therefore, every critical component and link in the overall network should have HA or redundancy designed-in and configured.

This chapter, which discusses HA/redundancy design for the entire solution, includes the following major topics:

- High Availability for the Access Layer, page 82
- High Availability for the PoP Distribution Layer, page 82
- High Availability for the Super Core Layer, page 85
- High Availability for the SD-Access Transit, page 85
- High Availability for the Shared Services Switch, page 85
- High Availability for the Shared Services Servers, page 85
High Availability for the Access Layer

The access layer connectivity is provided with Cisco Industrial Ethernet (IE) switches and REP ring, as shown in CCI Major Building Blocks, page 8. REP ring connectivity provides redundancy for the uplinks of the access switches. REP ring network converges within 100ms and provides an alternate path in case of a link failure. EtherChannel using Port Aggregation Protocol (PAgP) is configured between the ENs or PENs and Fabric Edge/FiaB, providing redundancy and load balancing.

Endpoint redundancy can be provided by duplicating the critical endpoints covering specific locations such as a camera.

For redundancy of vertical service gateways, refer to their respective vertical sections.

High Availability for the PoP Distribution Layer

In the case of a FiaB setup, control plane, edge, and border node functionality are all placed on a single switch device. No additional fabric devices are required or permitted for the FiaB deployment; solution resiliency depends on the redundant switches in a stack.

9300 StackWise 480

Thus, high availability is provided at the distribution layer for the Cisco Catalyst 9300 (FiaB) by configuring Cisco StackWise-480 as shown in Figure 41. Cisco StackWise-480 is an advanced Cisco technology with support for Non-Stop Forwarding with Stateful Switchover (NSF/SSO) for the most resilient architecture in a stackable (sub-50-ms) solution. For more details, please refer to the Cisco Catalyst 9300 Series Switches Data Sheet at the following URL:

Please refer to the caveat recorded in the Implementation Guide for convergence time in case of stack active switch failover.

HA and load balancing are provided by EtherChannel between access switches and Cisco Catalyst 9300 (FiaB). If any of the switches or links fail, the operation will continue with no interruption. Two uplinks of an access switch are connected to two different switches in the stack. Multiple switches in a stack are in active-active redundancy mode; they appear as a single aggregate switch to the peer. Thus, EtherChannel/PortChannel is configured between access switches (IE switches/Nexus switches) and Cisco Catalyst 9300 stack.

Redundant Layer 3 uplinks are configured between distribution layer stack switches and core layer switches. Load balancing and redundancy are ensured by the routing protocols.

9500 StackWise Virtual

Cisco Catalyst 9500 differs from the Catalyst 9300 (StackWise 480) insofar as the 9300 has physical backplane stacking cables, with a maximum distance of 30ft/10m, whereas the Catalyst 9500 (StackWise Virtual) uses Ethernet interfaces, and can be split across much greater distances, typically several miles/kilometers for a CCI deployment. Doing so provides geo-redundancy, as the FiaB stack is split across two disparate physical locations, and therefore helps mitigate against local power problems, fiber cuts, etc.
The StackWise Virtual Link (SVL) is typically comprised of multiple 10 or 40 Gbps interfaces (and associated transceivers (e.g. SFP+/QSFP) and cabling). These are dedicated to being SVL, provide a virtual backplane between the two physical Catalyst 9500 switches, and cannot be used for any other purpose. In CCI the design recommendation is two physical SVL links, and one Dual-Activity Detection (DAD) link. The DAD link is there to mitigate against both stack members becoming active in a failure scenario; care must be taken for fiber physical paths between two separate locations – if all fibers are taking the same physical path, then a fiber cut will likely nullify any geo-redundancy gained by using SVL.

In terms of sizing the SVL link(s) this must be done with respect to the upstream and downstream network requirements. For example, if the upstream (transit) links are 10Gbps, from each Catalyst 9500, then the SVL link should be 20Gbps or more.

It is recommended that the IE switches get connected to both stack members, using a Port Channel (which is automated by DNAC) as this results in lower L2 convergence times during failure conditions, however it is also supported to connect to just the nearest Catalyst 9500 stack member – this could be likely when there is insufficient fiber pairs between the two physical locations that each stack member is housed – however in this case a Port Channel is still used, even though it only has one bundle member; this aligns with SDA automation, and also allows the possibility of almost hitless upgrade should extra fiber capacity become available in the future.


**Note:** Only the non-high-performance variants of the Catalyst 9500 family are supported for SVL at CCI PoP.
High Availability for the Super Core Layer

Two core switches are configured for redundancy. All connections/links to core switches (downlinks and uplinks) are duplicated. A Layer 3 handoff is chosen between the Fabric Border and the IP transit. The Cisco DNA Center configures BGP as the exterior gateway protocol. Dual-Homed BGP connection with multiple interfaces at the Fabric Border terminating at different core switches (IP Transit) can be configured by the Cisco DNA Center for redundancy and load sharing.

Routing protocols such as EIGRP/OSPF are configured in the underlay for connecting core switch and the shared services network switches (Nexus 5000 series). By default, both EIGRP and OSPF support Equal-Cost Multi Path (ECMP) routing. EIGRP/OSPF with ECMP provide redundancy and load balancing over multiple paths.

A cross link at each aggregation layer is used for optimal routing in case of an uplink failure. EtherChannel is configured between the core switches for cross-link communication (from uplink of one core switch to downlink of the other core switch) and to choose an alternate path in case of a link failure.

High Availability for the SD-Access Transit

Two switches are configured for SD-Access Transit for redundancy. All connections/links to SD-Access transit nodes (downlinks and uplinks) are duplicated. The Cisco DNA Center auto configures communication between Fabric Border and redundant SD-Access Transit nodes ensuring redundancy and load-balancing.

Routing protocols such as EIGRP/OSPF are configured in the underlay for connecting SD-Access Transit nodes and the fusion router. By default, both EIGRP and OSPF support ECMP routing. EIGRP/OSPF with ECMP provide redundancy and load balancing over multiple paths.

A cross link at each aggregation layer is used for optimal routing in case of an uplink failure. EtherChannel is configured between the SD-Access transit nodes for cross-link communication and to choose an alternate path in case of a link failure.

High Availability for the Shared Services Switch

Redundant Nexus 5000 series switches are configured for providing HA to the server connectivity. Nexus switches are configured with vPC PortChannel redundancy connecting to various servers in the shared services network such as Cisco DNA Center and ISE.

<table>
<thead>
<tr>
<th>Table 10</th>
<th>Redundancy for Shared Services Switch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared Services Switch Redundancy</td>
<td>Redundancy Mechanism</td>
</tr>
<tr>
<td>Between Core and Nexus</td>
<td>EIGRP/OSPF with ECMP over redundant links</td>
</tr>
<tr>
<td>Between Nexus and DC servers (DNAC, ISE...)</td>
<td>vPC and redundant links to servers</td>
</tr>
</tbody>
</table>

High Availability for the Shared Services Servers

Redundancy should be configured for various critical servers in the network, i.e., Cisco DNA Center, ISE, FND, DHCP, DNAC, and CA. The Cisco DNA Center supports inherent redundancy with cluster.

Cisco DNA Center Redundancy

The Cisco DNA Center redundancy is provided by clustering three Cisco DNA Center appliances together. Clustering provides a sharing of resources and features and helps enable high availability and scalability. The Cisco DNA Center supports a single-host or three-host cluster configuration.

The three-host cluster provides both software and hardware high availability. The three-node cluster can inherently do service/load distribution, database, and security replication. The cluster will survive loss of a single node.
The single host cluster does not provide hardware high availability. Therefore, we recommend three-host cluster configuration to be used for the CCI Network. Detailed configuration is provided in the Cisco DNA Center Administration Guide at the following URL:


If the Cisco DNA Center appliance becomes unavailable, the network still functions, but automated provisioning and network monitoring capabilities are not possible until the appliance or cluster is repaired/restored.

Shared Services Application Servers Redundancy

Depending on the provisioning, UCS server level redundancy and/or application level redundancy can be configured for all critical application servers. Refer to the corresponding vertical sections for details.

Cisco ISE Redundancy

Cisco ISE has a highly available and scalable architecture that supports standalone and distributed deployments. In a distributed environment, you configure one primary Administration ISE node to manage the secondary ISE nodes that are deployed onto the network. Detailed information is provided in the Cisco Identity Services Engine Administrator Guide at the following URL:


NGFW Redundancy

Configuring high availability, also called failover, requires two identical Firepower Threat Defense devices connected to each other through a dedicated failover link and, optionally, a state link. Firepower Threat Defense supports Active/Standby failover, where one unit is the active unit and passes traffic. The standby unit does not actively pass traffic, but synchronizes configuration and other state information from the active unit. When a failover occurs, the active unit fails over to the standby unit, which then becomes active. The health of the active unit (hardware, interfaces, software, and environmental status) is monitored to determine if specific failover conditions are met. If those conditions are met, failover occurs.

Detailed information can be found in High Availability for Firepower Threat Defense at the following URL:


CCI Network Scale and Dimensioning

The CCI solution consists of the CCI access, distribution, core, data center, shared services, and DMZ layers. This chapter, which illustrates scaling considerations and available options at different layers of the network and provides steps for computing dimensions for an CCI network deployment, includes the following major topics:

- CCI Network Access, Distribution, and Core Layer Portfolio Comparison, page 87
- CCI Network Access Layer Dimensioning, page 89
- CCI Network Distribution and Core Layer Dimensioning, page 90
- Cisco DNA Center Scalability, page 91
- Cisco ISE and NGFW Scalability, page 91
CCI Network Access, Distribution, and Core Layer Portfolio Comparison

Table 11 shows the portfolio of devices used at different layers of CCI Network. The “CCI role” row in the table indicates the layer at which the device family of switches are used and in which building block. While core and distribution exist in the Centralized Infrastructure, each PoP is effectively its own LAN. The Cisco Catalyst 9300 stack is a collapsed core and distribution, with access done on the Cisco Industrial Ethernet (IE) switches.

The Cisco Industrial Ethernet Portfolio switches that are used in the access layer are modular in size with various form factors, port sizes, and features. Thus, the CCI PoP access layer is highly scalable from a very small to very large size with a suitable quantity of Cisco Industrial Ethernet (IE) switches. Similarly, the Catalyst series of switches used in the distribution layer have several models suited to different deployment needs and they support stacking, thus are highly scalable. The switches used in the core layer suit central deployment with high density fiber ports and high switching (6.4 Tbps) capacity. A summary of these switches is given in Table 11 as a reference, which can assist in the selection of suitable models based on deployment needs.

Technical Note: Different types of access switches can be combined in a single ring.

Table 11  CCI Network Access, Distribution, and Core Layer Portfolio Comparison

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CCI Role</td>
<td>Access at PoP or RPoP</td>
<td>Access at PoP or RPoP</td>
<td>Access at PoP or RPoP</td>
<td>Access at PoP or RPoP</td>
<td>Access at PoP or RPoP</td>
<td>Access at PoP or RPoP</td>
<td>Collapsed Core at PoP</td>
<td>Core and MAN/PoP aggregation</td>
</tr>
<tr>
<td>Form Factor</td>
<td>Modular DIN Rail</td>
<td>Mainboard, mountable with enclosure</td>
<td>Advanced Modular DIN Rail</td>
<td>DIN Rail</td>
<td>Rack mount</td>
<td>Rack mount</td>
<td>Rack mount</td>
<td>Rack mount</td>
</tr>
<tr>
<td>Total Ethernet Ports</td>
<td>Up to 26 ports of GE</td>
<td>Up to 24 ports of GE</td>
<td>Up to 26 ports of GE</td>
<td>Up to 20 GE ports</td>
<td>Up to 28 GE ports</td>
<td>Up to 28</td>
<td>Up to 48 per switch, 10/100/1000, MGig copper/SFP</td>
<td>Up to 48 10/10/25G SFP</td>
</tr>
<tr>
<td>PoE/PoE+</td>
<td>Yes (up to 24), 360W</td>
<td>Yes (up to 16), 240W</td>
<td>Yes (up to 24), 360W</td>
<td>Yes (8), 240W</td>
<td>Yes (24), 385W</td>
<td>Yes (12), 360W</td>
<td>Yes, but n/a</td>
<td>Yes, but n/a</td>
</tr>
<tr>
<td>SD-Access Extended Node</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No, and n/a</td>
<td>No, and n/a</td>
</tr>
<tr>
<td>SD-Access Policy Extended Node</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No, and n/a</td>
<td>No, and n/a</td>
</tr>
</tbody>
</table>
A comparison of the uplink capabilities of Cisco Industrial gateways suitable for CCI Remote PoP connectivity is shown in Table 12.

Table 12  CCI Remote PoP and IoT Gateways Portfolio Comparison

<table>
<thead>
<tr>
<th>Type of Gateway</th>
<th>Access Technologies Supported</th>
<th>Uplink Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>CGR1240</td>
<td>Direct: CR Mesh, Ethernet</td>
<td>Dual active 4G LTE, 802.11 b/g/n, 2 GE, 4 FE, 2 serial</td>
</tr>
<tr>
<td></td>
<td>Indirect: LoRaWAN (via Cisco Wireless Gateway for LoRaWAN)</td>
<td>Cisco advanced VPN technologies (FlexVPN, DMVPN)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Environmental Certificate: The routers are IEEE 1613 and IEC 61850-3 certified MTBF: 512,750 hours (58.5 years)</td>
</tr>
<tr>
<td>IR809</td>
<td>Direct: Ethernet</td>
<td>One active 4G LTE, 2 GE, 2 serial</td>
</tr>
<tr>
<td></td>
<td>Indirect: LoRaWAN (via Cisco Wireless Gateway for LoRaWAN)</td>
<td>Cisco advanced VPN technologies (FlexVPN, DMVPN)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MTBF: 440,000 hours (50.2 years)</td>
</tr>
<tr>
<td>IR829</td>
<td>Direct: Ethernet, Wi-Fi</td>
<td>Dual Active 4G LTE, 802.11a/b/g/n, 4 GE, 2 serial</td>
</tr>
<tr>
<td></td>
<td>(Not in scope for this CCI release.)</td>
<td>Cisco advanced VPN technologies (FlexVPN, DMVPN)</td>
</tr>
<tr>
<td></td>
<td>Indirect: LoRaWAN (via Cisco Wireless Gateway for LoRaWAN)</td>
<td>MTBF: 322,390 hours in fixed environment with PoE module (36.8 years)</td>
</tr>
</tbody>
</table>
Table 12  CCI Remote PoP and IoT Gateways Portfolio Comparison

<table>
<thead>
<tr>
<th>Type of Gateway</th>
<th>Access Technologies Supported</th>
<th>Uplink Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>IR1101</td>
<td>Direct: Ethernet</td>
<td>Dual active LTE-capable, 4 FE for LAN, 1GE Copper, 1GE SFP for WAN, 1 Serial interface, Edge Computing Cisco advanced VPN technologies (FlexVPN, DMVPN etc.,)</td>
</tr>
<tr>
<td></td>
<td>Indirect: LoRaWAN (via Cisco Wireless Gateway for LoRaWAN)</td>
<td></td>
</tr>
<tr>
<td>Cisco Wireless Gateway for LoRaWAN (Standalone IoT Gateway)</td>
<td>Direct: LoRaWAN</td>
<td>Ethernet</td>
</tr>
<tr>
<td>Cohda RSU Mk5 (Standalone IoT Gateway)</td>
<td>Direct: DSRC</td>
<td>Ethernet</td>
</tr>
</tbody>
</table>

CCI Network Access Layer Dimensioning

In Table 13, we show different types of endpoints and gateways connected to CCI PoP access ports, along with their port type and bandwidth requirements. Based on the deployment needs of a site (e.g., number of cameras, number of IoT gateways), access port and access ring requirements can be computed using information in Table 13 and Figure 42.

Table 13  Requirements for Endpoints/Devices Connected to Access Layer Switch

<table>
<thead>
<tr>
<th>Endpoint/Traffic Type Connected to Access Port</th>
<th>Application Bandwidth Requirement</th>
<th>Default Bandwidth Allocation per Access Ring</th>
<th>Switch Port Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video Surveillance Camera</td>
<td>6Mbps(HD), 3Mbps(SD)</td>
<td>300Mbps (50 to 100 cameras)1</td>
<td>One Fast Ethernet (FE) PoE/PoE+</td>
</tr>
<tr>
<td>IoT gateway such as Cisco Connected Grid Router (CGR), IC3000</td>
<td>IoT Traffic</td>
<td>300Mbps allocated for overall IoT traffic by CCI Network</td>
<td>One Fast Ethernet (FE) / Gigabit Ethernet (GE) per IoT gateway Copper/SFP depending on distance</td>
</tr>
<tr>
<td>REP ring ports</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Two Gigabit Ethernet (GE) Copper/SFP depending on distance</td>
</tr>
</tbody>
</table>

Technical Notes:

- Depending on the requirement of a specific site, the default bandwidth allocation in an access ring can be adjusted. For example, if only cameras are to be connected, the bandwidth allocated for camera traffic can be increased up to 900Mbps, thus approximately 150 to 300 cameras can be supported per ring.

- If the cumulative demand for various traffic generated from a ring is more than 1Gbps, separate rings can be laid to cater to the specific need.
CCI Network Scale and Dimensioning

CCI Network Distribution and Core Layer Dimensioning

The CCI system dimensioning chart is shown in Figure 42. Cisco Catalyst 9300 series switches have up to 48 ports and 8 switches can be stacked. Each ring including redundancy requires 4 ports for termination. With a minimum of 2 switches in a stack, up to 24 concurrent rings can be supported. Each ring can support up to 30 Cisco Industrial Ethernet (IE) switches. For further expansion, either additional switches can be added to the stack or additional PoPs can be created with a new stack of Cisco Catalyst 9300 series switches.

Every ring can generate traffic up to 1Gbps. Considering up to 24 concurrent rings, 24Gbps traffic is generated. The fixed uplink of Cisco Catalyst 9300 supports up to 4x10G and modular uplinks support 1/10/25/40G. Modular uplinks can also be added based on the necessity. As per standard Cisco QoS recommendation, the oversubscription ratio for distribution-to-core level is 4:1. However, considering most of the IoT traffic is device generated and is of constant bit rate, the oversubscription ratio at distribution-to-core should be kept low. Refer to Enterprise QoS Solution Reference Network Design Guide at the following URL:


The core Cisco Catalyst 9500 series switches support 48 1/10/25 Gigabit ports. Each PoP with redundancy needs 2 ports for termination at the core. Thus, with a pair of Cisco Catalyst 9500 series switches, up to 40 PoP locations can be supported (remaining ports are needed for uplink connection to Shared Services, Application Servers, and Internet). Further expansion can be done with additional Cisco Catalyst 9500 series switches. The Cisco Catalyst 9500 switches have very high (6.4Tbps) switching capacity. If the connection from Distribution to Core passes through intermediate nodes (IP/MPLS backhaul), the number of ports needed at the Core can be reduced. As per the standard Cisco QoS recommendation, the over-subscription at core layer should be 1:1, resulting in no over-subscription.

Thus, the CCI access, distribution, and core systems can be scaled from a small deployment to a large deployment in terms of number of endpoints connected, bandwidth requirement, and area to be covered.

The scale numbers are summarized below:

- Max number of access ports per node (IE switch): 20 (IE 4000), 26 (IE 3x00), 28 (IE 4010/5000), or 24 (ESS 3300)
- Max number of nodes per ring: 30
- Max bandwidth of an access ring: 1Gbps
- Max number of concurrent access rings per PoP (one pair of 9300): 24
- Max number of concurrent access rings per PoP (one pair of 9500): 48
- Max number Cisco Catalyst 9300 switches in a stack: 8
- Max number of Cisco Catalyst 9500 switches in a StackWise Virtual: 2
For Remote PoP infrastructure requirement, refer to Figure 43.

CCI Network SD-Access Transit Scale

In the case of SD-Access Transit, the PoP sites are connected to SD-Access Transit. Similar to the one shown in Figure 43, when the number of PoP sites pass 40, an additional pair of SD-Access Transit sites can be added to accommodate required ports and bandwidth.

Cisco DNA Center Scalability

The Cisco DNA Center scaling computation and hardware specification is given in the Cisco DNA Center data sheet. Cisco DNA Center numbers are per instance, which can be a single-node cluster or a three-node cluster. The maximum numbers are either the platform absolute limits or the recommended limit based on the most current testing of a single platform. Refer to Cisco Documentation for further details on scaling and sizing of Cisco DNA Center documentation.

For more information about Cisco DNA Center scaling, refer to the Cisco DNA Center User Guide at the following URL:


Cisco ISE and NGFW Scalability

Cisco ISE scaling is based on deployment model such as standalone or distributed. For more details, refer to the Cisco Identity Services Engine Installation Guide, Release 2.4 at the following URL:

Cisco NGFW scaling factor includes platform configuration and features enabled. For more details, refer to the Cisco documentation *Deploy a Cluster for Firepower Threat Defense for Scalability and High Availability* at the following URL:

CCI Ethernet Access Network Solution

This chapter discusses design for CCI Ethernet Access Network for endpoint connectivity.

Ethernet Access Network

Ethernet access is provided by connecting Cisco Industrial Ethernet (IE) Ethernet switches to Fabric Edge/FiaB. The Cisco's Industrial Ethernet series switches are modular and scalable with various options for 10/10/1000Mbps copper/fiber ports with PoE/PoE+ support. A snapshot of the Cisco Industrial Ethernet (IE) switch portfolio is given in Table 11. The distance covered and number of access ports provided by a single hop of Cisco Industrial Ethernet (IE) Ethernet switch can be highly limiting. Multi-hop ring network with REP ring technology is preferred in IoT applications due to distance covered, redundancy, and resiliency features.

The recommended Ethernet access network topology for CCI is a REP ring formed by Cisco Industrial Ethernet (IE) switches connected back to back that terminates both ends of the ring on a stack of Fabric Edge devices. Considering the Ethernet access ring of ≤30 and multiple such rings in the CCI deployments, it is recommended to use Cisco DNA Center templates for automated configuration and provisioning of daisy-chained rings for ease of use and quick deployment of access network. The REP topology is also configured with the help of Cisco DNA Center Day N templates.

Ring Topology

In this topology, the Cisco Industrial Ethernet (IE) switches are connected to the Fabric Edge in a ring form, as shown in Figure 45. REP is the preferred resiliency protocol for IoT applications. All configurations of the Cisco Industrial Ethernet (IE) switches, including REP configuration in the ring can be zero-touch provisioned (ZTP) using Cisco DNA Center templates feature. The manual configuration is simplified by the usage of Cisco DNA Center Day N templates. REP automatically selects the preferred alternate port. Altering preferred alternate port impacts recovery time in a REP ring fails; therefore, it is recommended to not manually override the preferred alternate port. The preferred alternate port selected by REP is blocked during normal operation of the ring. In case of a REP segment failure, the preferred alternate port is automatically enabled by REP, giving an alternate path for the disconnected segment. On recovery of the failed REP segment, the recovered port is made the preferred alternate port and blocked by REP. Thus, recovery happens with minimal convergence time. For CCI, the desired REP convergence time for a 30 node REP ring should be within 100ms, which is achievable based on the verified results.

Note that a mixed ring of IE4000/IE5000/IE3300/ESS3300 and IE3400 is not recommended and a mixed ring of EN/DC-EN and PEN/DC-PEN nodes is not supported.

Two uplinks of an Cisco Industrial Ethernet (IE) switch are to be connected to two access ports on FE, preferably terminating on two different switch members of the FiaB stack. The two ports to which an Cisco Industrial Ethernet (IE) switch is connected are auto configured into a port channel by Cisco DNA Center and marked as EN ports (or PEN ports in the case of IE3400 switches). The Cisco DNA Center also makes these ports as trunk ports allowing all VLANs. The VLANs in the REP segment can be configured in the ring using Day N templates to align with the VLANs in the fabric overlay VNs created by the Cisco DNA Center in the fabric. Based on the VLAN of the traffic entering the EN port of FE, it is tagged with appropriate SGT and VN and segmentation policy is applied.

Note: Fluidmesh Access Points that connect to Ethernet access ring requires MTU of >1500 bytes. Hence it is recommended to configure a system wide MTU of 2000 bytes on all of the IE switches in the ring to accommodate to higher MTU packets.

Provisioning Extended Node Ring using templates

Cisco DNA Center Day N templates could be configured to discover and provision all DC-EN Cisco Industrial Ethernet (IE) switches in the access ring. An example discovery and provisioning process of DC-ENs using templates is explained below. A detailed step-by-step instruction to configure daisy-chained ring topology and REP using Day N templates for the Extended Node ring will be covered in CCI Implementation Guide.

1. After onboarding two ENs in the ring, the physical connectivity of all Cisco Industrial Ethernet (IE) switches in ring should be done and one of the ENs uplink Port-Channel must be shutdown either manually or using a CLI template.
2. Creating local DHCP & TFTP Server on ENs or PENs: A DHCP pool template configures a local DHCP pool (on VLAN1) and TFTP server on one of the ENs in the ring. It also creates network-config and startup_config.tcl file files in ENs.

3. All DC-ENs in the ring to be factory reset by removing any existing configurations and reloading the switches to start auto-install process.

4. All DC-ENs will get the IP address assigned from local DHCP server on VLAN1 (native VLAN) and downloads network-config file and startup_config.tcl files from ENs along with Extended Node VLAN and Cisco DNA Center IP address.

5. Startup_config.tcl script creates Port-Channels with trunk configuration on every DC-EN in the ring and it starts PnP process with Cisco DNA Center as PnP server using extended node VLAN as PnP VLAN.

6. Once, PnP process is complete on all DC-ENs in the ring, these switches are in Cisco DNA Center Plug-n-Play list in "Unclaimed" state. These switches have to be claimed to the respective PoP site.

7. Using REP automation Day-N template, REP configuration along with other configurations as needed can be provisioned on these switches.

Once the ring is fully provisioned using the templates, the Cisco DNA Center fabric topology view of the ring is shown as in Figure 44 below.

Figure 44  CCI Access Network Ring Topology view on Cisco DNA Center

Note that the Extended Node and Policy Extended Nodes in the ring are represented as “x” in the topology and rest of the DC-ENs or DC-PENs are grayed as they are not part of SD-Access fabric and not managed by Cisco DNA Center. Refer to the Table 1: for the comparison of Extended Node, Policy Extended Node DC-EN and DC-PEN features for more details.

Note: The management SVIs for the Cisco Industrial Ethernet (IE) switches are in a special, predefined VN: INFRA–VN.

REP primary and secondary edge ports are configured on FiaB on a stack of C9300 Series switches or C9500 switches StackWise Virtual, thus forming a closed ring of Cisco Industrial Ethernet (IE) switches. This allows detection of any REP segment failure, including the uplink ports of EN or PENs on FiaB Stack or C9500 StackWise Virtual, and convergence.
takes place. Hence, it is recommended to provision REP as a closed ring topology as shown in Figure 45 in CCI for network high availability and better traffic convergence, in case of link failures within the REP segment.

**Figure 45  CCI Access Network Ring Topology**

Additionally, an Ethernet access ring network consisting of all IE3400 Series switches only can be formed as a Policy Extended Node ring, as shown in Figure 46.

Endpoints or hosts onboarded in the Policy Extended Node and DC-PENs in the ring will have the right VLAN and SGT tag attributes downloaded from ISE to enforce communication policy based on SGT for improved endpoint and ring security. Also, the Policy Extended Node and DC-PENs in the ring support 802.1X/MAB based closed authentication for endpoints.
Cisco DNA Center Day N templates can be configured to discover and provision all DC-PEN Cisco Industrial Ethernet (IE) switches in the access ring. The discovery and provisioning process of DC-PENs in the ring is same as DC-ENs in the Extended Node ring. Hence, refer to the section Provisioning Extended Node Ring using templates, page 93, for DC-PENs provisioning. The detailed step-by-step instructions to configure daisy-chained ring topology and REP using Day N templates for the Policy Extended Node ring are covered in the CCI Implementation Guide.

**Note:** REP Fast feature is capable of reducing L2 convergence times, however REP Fast is only supported on IE3x00 and ESS3300 switches (not IE4000, IE5000 nor Catalyst 9000), and is also not supported on Port Channel interfaces - because of this, REP Fast is not suitable for inclusion in the CCI CVD. For more information on REP Fast please see [https://www.cisco.com/c/en/us/products/collateral/switches/industrial-ethernet-switches/white-paper-c11-743432.html](https://www.cisco.com/c/en/us/products/collateral/switches/industrial-ethernet-switches/white-paper-c11-743432.html)

### CCI Wi-Fi Access Network Solution

802.11 Wi-Fi is an important access technology for CCI; it supports a number of use-cases, both in terms of outright access and also with Cisco Wi-Fi Mesh, to physically extend the reach and provide a transport path for other devices and access technologies.
CCI covers two different Wi-Fi deployment types: Cisco Unified Wireless Network (CUWN) with Mesh, and SDA Wireless as shown in Figure 46. It is not possible to mix both types at a single PoP, however it is possible to have shared SSIDs between say SDA Wireless in PoP1 and CUWN Mesh in PoP2, although it should be noted that there will not be seamless roaming between them, and this scenario is best suited when the neighboring PoPs are sufficiently apart that any Wi-Fi client will not “see” the SSID from both simultaneously.

![Figure 47 CUWN and SD Access Wi-Fi Networks](image)

Both deployment types are based on Cisco Wireless Lan Controllers (WLCs) being in control of Cisco Lightweight APs (LWAPP), using the Control and Provisioning of Wireless Access Points (CAPWAP) protocol.

Outdoor (IP67) APs supported and tested as part of CCI are listed and compared in the following table:

<table>
<thead>
<tr>
<th>Table 14</th>
<th>APs tested and supported in CCI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported for CUWN Mesh</td>
<td>Cisco AP1572</td>
</tr>
<tr>
<td>Supported for SDA Wireless</td>
<td>N</td>
</tr>
<tr>
<td>802.11 radio technology</td>
<td>AC Wave 1</td>
</tr>
<tr>
<td>2.4GHz radio</td>
<td>Y</td>
</tr>
<tr>
<td>5 GHz radio</td>
<td>Y</td>
</tr>
<tr>
<td>SFP port</td>
<td>Y</td>
</tr>
</tbody>
</table>
**Table 14** APs tested and supported in CCI

<table>
<thead>
<tr>
<th>PoE-in** (Watts)</th>
<th>Y (60W)</th>
<th>Y (60W)</th>
<th>Y (30W)</th>
<th>Y (30W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC-in</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>AC-in</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>PoE-out (Watts)</td>
<td>Y (30W)</td>
<td>N</td>
<td>Y (15.4W)***</td>
<td>Y x2 (30W in total)***</td>
</tr>
<tr>
<td>Internal antenna variant</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>External antenna variant</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>GPS antenna</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>IOx Edge Compute support</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>Temperature Range</td>
<td>-40 to +65°C</td>
<td>-40 to +65°C</td>
<td>-50 to +75°C</td>
<td>-40 to +85°C</td>
</tr>
</tbody>
</table>

* this AP is for embedded applications and requires a separate enclosure, and if outdoors recommend this enclosure be IP67 rated.

** for full performance; AP may run on less power with reduced performance.

*** PoE-out is only available if AP is powered by DC-in.

WLC scale numbers are shown below, but in addition there are overall DNAC Wi-Fi scale numbers, in terms of total numbers of APs and clients; please refer to:

Both SDA Wireless and CUWN Mesh will need outdoor antennas to go with the outdoor APs. Cisco has a wide selection of antennas available, with many variants based on frequency, gain, directionality etc.; see https://www.cisco.com/c/dam/en/us/products/collateral/wireless/aironet-antennas-accessories/solution-overview-c22-734002.pdf for more details. In general for SDA Wireless, omni-directional antennas are the usual choice, giving Wi-Fi coverage for clients in all directions from the AP, however in certain scenarios a directional antenna may be preferred. Similarly for CUWN Mesh directional antennas are the norm (certainly for forming the mesh topology itself), and omni-directional antennas may be used for client access. Cisco recommends an RF survey be performed prior to equipment selection and deployment, so that appropriate components can be selected.

**Cisco Unified Wireless Network (CUWN) with Mesh**

Cisco Unified Wireless Networking is used over-the-top (OTT) of the CCI SDA Fabric; neither the WLCs nor APs are fabric-enabled or aware. CUWN can be used to deliver macro-segmentation, where there is a mapping between Wi-Fi networks (SSIDs) and SDA Virtual Networks (VNs). CUWN is also necessary for Wi-Fi Mesh, which is a topology and technology not currently supported in SDA Wireless.
Wi-Fi Mesh is comprised of Root APs (RAPs) and Mesh APs (MAPs). RAPs are the handoff point between wired and wireless Ethernet networks; MAPs connect to RAPs and other MAPs purely over-the-air, in 802.11 RF bands.

For CCI RAPs will (wired) connect to either Fabric Edge ports, or more likely, Extended Node ports.

Three things the Wi-Fi Mesh can be setup to do:

- Provide wired LAN extension over Wi-Fi for a single VN
  
  For example: an IP CCTV camera (and the PoE-out capabilities of the AP are important here)

- Provide wired LAN extension over Wi-Fi for multiple VNs
  
  For example: a remote switch, supporting multiple segmented use-cases.

- Provide Wi-Fi client access
  
  For example: to extend Wi-Fi coverage to areas where there is no wired connectivity

  **Note:** Both RAPs and MAPs can be enabled or disabled for client access.

All the above have slightly different considerations, but in general the design should be for no more than 3 hops, from the RAP to the furthest MAP, and if Wi-Fi client access is enabled for these MAPs it should be done in different spectrum than that used to form the mesh itself; the CCI general recommendation is for 5GHz for mesh backhaul with directional antennas, and optionally for client access too with omnidirectional antennas, with 2.4GHz for client access, (2.4GHz typically increased range over 5GHz, especially outdoors).

Although it is possible to have the Mesh APs self-select 5GHz channels for backhaul, it is the CCI recommendation that channels be manually selected.

For Mesh RAPs, or for non-Mesh CUWN APs, FlexConnect mode is used. See https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/Enterprise-Mobility-8-5-Design-Guide/Enterprise_Mobility_8-5_Deployment_Guide/ch7_HREA.html for more details on FlexConnect. FlexConnect means that for control traffic CAPWAP is used between the WLC and the AP, but wireless data traffic is broken out onto the wired Ethernet network in the directly connected switch; in this way it can be mapped into the appropriate macro-segments, and have the chance to interact with other Ethernet traffic within a PoP, without having to be tunneled back to the WLC (which would be the default mode: Local mode).

The exception here are any SSID(s) associated with Public Wi-Fi, or some other untrusted Wi-Fi traffic; this traffic is tunneled back to the WLC inside CAPWAP packets, where it can be dealt with appropriately.

**Centralized WLC deployment**

Locating a HA WLC pair in the Shared Services segment means it is centralized and can shared across all PoPs. Consequently centralized WLC is typically a larger appliance:

**Table 15  Cisco Catalyst 9800 Series WLC Scale Comparison**

<table>
<thead>
<tr>
<th></th>
<th>Cisco Catalyst 9800–40</th>
<th>Cisco Catalyst 9800–80</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max number of APs</td>
<td>2,000</td>
<td>6,000</td>
</tr>
<tr>
<td>Max number of Wi-Fi clients</td>
<td>32,000</td>
<td>64,000</td>
</tr>
<tr>
<td>Max number of Wi-Fi networks (SSIDs)*</td>
<td>4096</td>
<td>4096</td>
</tr>
</tbody>
</table>

* Most APs support up to 16 SSIDs being beaconed (where the SSID name is visible to clients), however more SSID can be supported by an AP (but hidden), and typically more overall SSIDs can be supported by the WLC.
Per-PoP WLC deployment

Locating a HA WLC pair directly at a PoP, on a per-PoP basis (i.e. there is separate WLC infrastructure at each PoP that requires Wi-Fi) may be preferred for deployment than the centralized approach, especially if the RTT between the PoP and the Shared Service segment (where a centralized WLC would be located) is very large (>=150ms) If Per-PoP WLCs are required or preferred then the Cisco Catalyst 9800-L WLC is the only WLC model that is suitable, given other PoP scaling factors (e.g. maximum number of clients at a PoP).

**Table 16  Cisco Catalyst 9800-L WLC Scale**

<table>
<thead>
<tr>
<th>Max number of APs</th>
<th>Cisco Catalyst 9800-L</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>250</td>
</tr>
<tr>
<td>Max number of Wi-Fi clients</td>
<td>5,000</td>
</tr>
<tr>
<td>Max number of Wi-Fi networks (SSIDs)</td>
<td>4,096</td>
</tr>
</tbody>
</table>

Wi-Fi network management using Cisco Prime Infrastructure

DNAC currently does not understand mesh topologies, nor is able to set and report on the parameters specific to Wi-Fi Mesh, therefore Cisco Prime Infrastructure should be used to manage a Wi-Fi Mesh deployment, or any CUWN deployment as a part of CCI.

SDA Wireless

SDA Wireless main advantage over CUWN in a CCI deployment, is the ability to micro-segment (SGT TrustSec-based) at the Wi-Fi edge. There are client roaming advantages also, but these are more common in the Enterprise/Office environment, and less so in the environments for which CCI is designed.

For SDA Wireless the deployment model is a pair of WLCs at each PoP; the Cisco Catalyst 9800 Embedded WLC (eWLC) can be used. The eWLC runs as a software component in IOS-XE on the Catalyst 9000 family, specifically the 9300:

**Table 17  Cisco Catalyst 9800 eWLC Scale**

<table>
<thead>
<tr>
<th>Max number of APs</th>
<th>Cisco Catalyst 9800 Embedded (on Catalyst 9300 switch)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>200</td>
</tr>
<tr>
<td>Max number of Wi-Fi clients</td>
<td>4,000</td>
</tr>
<tr>
<td>Max number of Wi-Fi networks (SSIDs)</td>
<td>16</td>
</tr>
</tbody>
</table>

* The figures here are for a StackWise 480 pair of two Catalyst 9300 switches, per CCI deployment recommendations.

An SDA Wireless AP communicates with the WLC via CAPWAP, and with the nearest Fabric Edge via a VXLAN tunnel. The AP gets an IP address from a special AP address pool, part of the INFRA VN, as defined in DNAC; as such the LWAPP control signaling goes via CAPWAP, and the Wi-Fi traffic itself going via VXLAN. The Fabric Edge is where the macro and micro-segmentation is applied and policed - the AP does not inspect the traffic, it just forwards it, therefore there is no local switching of traffic on the AP itself. The traffic from SDA Wireless APs does not interact with ENs, PENs, DC-ENs or DC-PENs - it simply transits them on the way to the Fabric Edge.
SDA Wireless APs connect to either Fabric Edge (FE) ports, or Extended Node (EN) ports. Client roaming is anchored via the Fabric Edge regardless of whether the APs are directly connected to FE or EN ports (this is even true of Policy Extended Nodes (PENs)).

Wi-Fi network management using DNA Center

Although the WLC has CLI and Web GUI for wireless management, when doing SDA Wireless, DNA Center is the primary management point. Onboarding of APs, defining wireless networks (and associated attributes) and applying these to different physical locations, is all done via the DNAC user interface. Corresponding visibility, troubleshooting and general reporting is done via the Assurance component within DNAC. It is not recommended to make changes via the WLC CLI or Web UI, as these may be overwritten by DNAC.
Comparison of Wi-Fi Deployment types

The table below provides a comparison of Wi-Fi deployment types, depending on the use cases CCI is being used to achieve.

Table 18 Wi-Fi deployment comparison

<table>
<thead>
<tr>
<th>Connections</th>
<th>CUWN with Mesh</th>
<th>SDA Wireless</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client access (2.4GHz / 5GHz)</td>
<td>Y / Y</td>
<td>Y / Y</td>
</tr>
<tr>
<td>LAN extension over Wi-Fi</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Management</td>
<td>Prime Infrastructure</td>
<td>DNA Center</td>
</tr>
<tr>
<td>Segmentation available</td>
<td>Macro</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>Micro</td>
<td>Y</td>
</tr>
<tr>
<td>WLC locations</td>
<td>Per-Pop, at a PoP</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>Centralized in Shared Services</td>
<td>Y</td>
</tr>
<tr>
<td>Traffic directly into PoP Access Ring</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>DNA Spaces</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

Repeating the guidance above, it is not possible to mix both types at a single PoP, however it is possible to have shared SSIDs between say SDA Wireless in PoP1 and CUWN Mesh in PoP2, although it should be noted that there will not be seamless roaming between them, and this scenario is best suited when the neighboring PoPs are sufficiently apart that any Wi-Fi client will not “see” the SSID from both simultaneously.

Cisco DNA Spaces

Cisco DNA Spaces is a location services platform, delivered as a cloud-based service. WLCs integrate with DNA Spaces, and as such must have an outbound path to the Public Internet. See https://dnaspaces.cisco.com/faqs/#deployment for other deployment options and integration points, however these are not covered in this CVD.

DNA Spaces has two licensing levels (see https://dnaspaces.cisco.com/packages/ for full details): “See” and “Act”. Which level that is the best fit for your CCI deployment depends on the use cases, but in general “See” gives Wi-Fi client computed location, tracking and analytics, with visualization and the ability to export all this data; “Act” adds captive portal, hyper-location, advanced analytics and API/SDK integration possibilities.

In general DNA Spaces is an optional component with the CVD, however for the Public Wi-Fi use case it is a mandatory component, as it is used for the guest (captive) portal, and as such “Act” licensing is required. DNA Spaces works with both CUWN with Mesh, and SDA Wireless Wi-Fi deployment types, with both leveraging the Catalyst 9800 WLC integration (both embedded and appliance) with DNA Spaces cloud service.
CCI CR-Mesh Access Network Solution

This chapter, which discusses design of the CCI CR-Mesh Access Network for endpoint connectivity, includes the following major topics:

- CR-Mesh Network Overview, page 104
- CR-Mesh Access Network Architecture, page 104
- CR-Mesh Networking Components, page 106
- CR-Mesh Access Network Architecture, page 104

CR-Mesh Network Overview

A CR-Mesh network is a multi-service sub-gigahertz radio frequency solution. Cisco CR-Mesh networks are capable of supporting a large number of devices including but not limited to advanced metering, distributed automation, supervisory control and data acquisition (SCADA) networks, smart street lighting as well as a host of other use cases. In this section we cover the primary components and operation of a CR-Mesh network.

CR-Mesh is currently available for the 902–928Mhz band (and its subsets) only, therefore the countries where the band cannot be used are outside the scope of CR-Mesh usage.

CR-Mesh is Cisco deployment of IEEE 802.15.4g PHY and 802.15.4e MAC wireless mesh technology. Cisco CR-Mesh products are Wi-SUN Alliance certified starting with mesh version 6.1. The Wi-SUN Alliance is a global ecosystem of organizations creating interoperable wireless solutions. Though-out this document we will refer reference CR-Mesh and where applicable call out difference between CR-Mesh and Wi-SUN deployment strategies or implementation differences.

CR-Mesh is an IPv6 over Low power Wireless Personal Area Network (6LoWPAN). The 6LoWPAN adaptation layer adapts IPv6 to operate efficiently over low-power and lossy links such as IEEE 802.15.4g/e/v RF mesh. The adaptation layer sits between the IPv6 and IEEE 802.15.4 layers and provides IPv6 header compression, IPv6 datagram fragmentation, and optimized IPv6 Neighbor Discovery, thus enabling efficient IPv6 communication over the low-power and lossy links such as the ones defined by IEEE 802.15.4.

Routing Protocol for Low-Power and Lossy Networks (RPL) is a routing protocol for wireless networks with low power consumption and generally susceptible to packet loss. It is a proactive protocol based on distance vectors and operates on IEEE 802.15.4, optimized for multi-hop but supporting both star and mesh topologies.

CR-Mesh performs routing at the network layer using the Routing Protocol for Low-Power and Lossy Networks (RPL).

CR-Mesh implements the CSMP for remote configuration, monitoring, and event generation over the IPv6 network. The CSMP service is exposed over both the mesh and serial interfaces.

CR-Mesh Access Network Architecture

Cisco CR-Mesh networks consist of two major areas:

- Places in a CR-Mesh network
- Components of a CR-Mesh network

CR-Mesh in the CCI network

The CR-Mesh network components in CCI include:
Network Operation Center (NOC) and Data Centers (DC)

The NOC is typically in close proximity to the data center which hosts the various applications that are relevant to CR-Mesh components of the network. Together systems in the NOC and data center provide operational visibility for the system managers to view and control the status of the network. Application management platforms, network communications management systems, and security systems are key to the operation of the network and are located in the data center and are displayed in the operations center.

Demilitarized Zone (DMZ)

The DMZ is a security buffer where security policy is created allowing data to traverse from one security zone to another.

Wide Area Network (WAN)

The WAN is responsible for providing the communications overlay between the extended network to the core. It can contain communications technology that is either private or public network, which is either owned by the operator or outsourced to a service provider. Popular WAN backhaul options are Ethernet and Cellular.

Neighborhood Area Network (NAN)

The NAN is the last mile network infrastructure connecting CR-Mesh endpoints to the access network. Endpoints communicate in the NAN across an IEEE 802.15.4g/e/v RF wireless network and connect to an access layer router.

Personal Area Network (PAN)

A unique PAN identifier (ID) is configured in the wireless interface of the access router where the CR-Mesh RF network connects to the CCI network. The PAN ID is a 16-bit field, described in the IEEE 802.15.4 specification. It is received and used by all devices grouped in the same PAN.

Each PAN in a NANA refers to a specific IEEE 802.15.4 radio in an access router.

Public cloud Services

Services that are available over the internet and are not on the CCI network. (i.e. Cimcon LightingGale, Cisco Kinetic for Cities)

Figure 51 depicts the solution architecture that covers various layers or places in the CR-Mesh network, system components at each layer, and the end-to-end communication architecture.
CR-Mesh Networking Components

Networking components reside in different areas of the network and perform a function such as making communications decision, authenticating devices and services, or enforcing security policy.

Headend Router (HER)

In the CR-Mesh access solution, the HER terminates the FlexVPN IPSec and GRE tunnels from the access layer routers. It may also establish FlexVPN IPSEC tunnels to public services outside of the CCI network. The HER cluster must be able to grow to support the number of access layer routers and tunnels that the network will require and should have redundancy.

In the CCI solution, the HER can be a virtual router or a dedicated router depending on the needs of the network. Cisco Cloud Services Router 1000V (CSR1000V) or Aggregation Service Router Series (ASR) routers are used as HERs.

Field Area Router (FAR)

The FAR acts as a network gateway for CR-Mesh endpoints by forwarding data from the endpoint to the headend systems. It is a critical element of the architecture since it ties the NAN and the WAN tier together.

The Cisco Connected Grid Router (CGR) along with 802.15.4g/e/v WPAN module are the Field Area Routers.

Connected Grid Endpoints (CGE)

CGEs are IP-enabled grid devices with an embedded IPv6-based communication stack. The CGEs form an IEEE 802.15.4e/g/v RF-based mesh network.
A CR-Mesh network contains endpoints known as CGEs within a Neighborhood Area Network (NAN) that supports end-to-end IPv6 mesh communication. CR-Mesh supports an IEEE 802.15.4e/g/v wireless interface and standards-based IPv6 communication stack, including security and network management. The CR-Mesh network provides a communication platform for highly secured two-way wireless communication with the CGE.

There are several types of CGE devices available:

- Cisco IR509 and IR510 gateway
- Third party CGE endpoints (i.e. Cimcon Street Light Controller)
- Cisco IR529 and IR530 range extender

Cisco provides a CGE radio module for incorporation into third party mesh endpoints. Cisco has a Solution Development Kit (SDK) that allow manufacture to rapidly develop their own endpoint. As a benefit to using the Cisco SDK developers can also streamline their testing towards Wi-SUN certification. Refer to the Cisco developer network to find out more information regarding this program.

The current implementation supports frequencies in the range of 902-928 MHz, with 64 non-overlapping channels and 400 kHz spacing for North America. A subset of North America frequency bands for Brazil,

**Figure 52  Connected Grid Endpoint Standards-based Communications Stack**

Phy Mode 98 with FEC enabled is the recommended CGE configuration.
CCI CR-Mesh Access Network Solution

CR-Mesh WPAN interface in CGR Router

In the CCI architecture, Cisco 1000 Series Connected Grid Routers are used as FARs. The Cisco Connected Grid Router (CGR) 1240 is specifically designed for outdoor deployments while Cisco Connected Grid Router (CGR) 1120 is suited for indoor deployments. However, Cisco Connected Grid Router (CGR) 1120 with suitable enclosures can also be installed in outdoors in a field installation, with antennas mounted outside the enclosure.

The Cisco Connected Grid Router (CGR) is a modular platform providing flexibility to support several choices of interfaces to connect to a WAN backhaul, such as Ethernet and Cellular.

The Cisco Connected Grid Router (CGR) 1240 can be provisioned with up to two WPAN modules that provide IPv6-based, IEEE 802.15.4g/e/v compliant wireless connectivity to enable CCI applications. The two modules can act as independent WPAN networks with different SSIDs or can be in a primary-subordinate mode increasing the density of PHY connections. The module is ideal for standards based IPv6 multi-hop mesh networks and long reach solutions. It helps enable a high ratio of endpoints to the CGR.

Cisco has certified the WPAN physical interface (PHY) for Wi-SUN 1.0 compliance.

CR-Mesh Range Extension

Cisco range extenders provide unlicensed 902–928Mhz, ISM-band IEEE 802.15.4g/e/v wireless personal-area network (WPAN) communications. It extends the range of the RF wireless mesh network, providing longer reach between WPAN endpoints (CGEs) and the WPAN Field Area Routers (FARs). The Cisco IR530 range extender is a high performance, new generation of the Cisco RF Mesh range extender.

Key IR530 features:

- World class IPv6 Networking
- Highly Secure and Scalable
- IEEE 802.15.4, g/e/v, IETF 6LoWPAN
- Wi-SUN 1.0 PHY Certified
- IETF Routing Protocol for Low Power and Lossy Networks (RPL)
- IETF Constrained Application Protocol (CoAP)

CR-Mesh WPAN Industrial Router

Cisco industrial routers / gateways provide unlicensed 902–928Mhz, ISM-band IEEE 802.15.4g/e/v wireless personal-area network (WPAN) communications. These routers supply enterprise-class RF mesh connectivity to IPv4, IPv6 and RS-232 serial devices. Cisco IR510 provides higher throughput to support IoT use cases in distributed intelligence and supervisory control and data acquisition (SCADA).

Key IR510 features:

- World class IPv6 Networking
- Highly Secure and Scalable
- IEEE 802.15.4, g/e/v, IETF 6LoWPAN
- IETF Routing Protocol for Low Power and Lossy Networks (RPL)
- IETF Constrained Application Protocol (CoAP)
- IETF Mapping of Address and Port - Translation (MAP-T)
CCI CR-Mesh Access Network Solution

- Wi-SUN 1.0 PHY Certified
- DC Power input 9.6-60VDC, 7 watts of power consumption
- 10/100 Fast Ethernet port
- RS-232/RS-485 serial port
- Digital alarm input
- Raw socket support on serial ports
- SCADA Support
- Dying gasp
- Network and Transport Layer: IPv4, IPv6, RPL, NAT44, MAP-T, Leaf node, Static NAT

Data Center Services

Network Time Protocol (NTP) Server

NTP delivers time accuracies of 10 to 100 milliseconds over the CCI network, depending on the characteristics of the synchronization source and network paths in the WAN.

AAA and Directory Services

RADIUS provides authorization and authentication services for CR-Mesh.

RSA Certification Authority

During the pre-staging process, RSA CA-signed RSA certificates are provisioned in FAR. The RSA CA-signed certificates are also provisioned in HER. In order to verify RSA CA signed certificates, the RSA CA public key is loaded at FAR and HER. Thus, HER and FAR can verify authenticity of each other’s certificate.

ECC Certification Authority

ECC CA security keys are authenticated by AAA during CGE onboarding.
Cisco CR-Mesh network solution operations comprise of six major topics:

- Frequency Hopping Spread Spectrum Types
- Radio frequency area setup SSID, NAN and PAN
- CR-Mesh authentication and data flow
- Interoperability of FSK and OFDM endpoints
- Scale and Redundancy
- Ongoing operations

**Frequency Hopping Spread Spectrum Types**

CR-Mesh implements Frequency Hopping Spread Spectrum (FHSS) using two methods in the 902 to 928 MHz ISM band:

- Two Frequency Shift Keying (2FSK): 64 channels, 400-kHz spacing
- Orthogonal frequency Division Multiplexing (OFDM): 31 channels, 800kHz channel spacing

The frequency-hopping protocol used by CR-Mesh maximizes the use of the available spectrum by allowing multiple sender-receiver pairs to communicate simultaneously on different channels. The frequency hopping protocol also mitigates the negative effects of narrowband interferers.

CR-Mesh allow each communication module to follow its own channel-hopping schedule for unicast communication and synchronize with neighboring nodes to periodically listen to the same channel for broadcast communication. This enables all nodes within a CGE PAN to use different parts of the spectrum simultaneously for unicast communication when nodes are not listening for a broadcast message.
Wi-SUN 1.0 and CR-Mesh support 2FSK narrowband modulation schemes. While 2FSK is effective for applications like smart metering, they can encounter group delay and narrowband interference in complex or highly contested environments. In addition to 2FSK, CR-Mesh supports OFDM radio management technology. OFDM employs frequency-division multiplexing and advanced channel coding techniques enabling reliable transmission and improved data rates in more complex and contested environments. Future releases of Wi-SUN will support OFDM, Cisco will also release a future OFDM reference design. Current Cisco OFDM CR-Mesh devices (IR510 and OFDM WPAN module) are backwards compatible supporting both OFDM and 2FSK devices, but not CR-Mesh and Wi-SUN 1.0 simultaneously. Wi-SUN 1.0 has a different MAC frame format and flow control preventing interoperability between Wi-SUN and CR-Mesh.

This guide and the supporting implementation guide will explore combining both FSK and OFDM devices on a neighborhood area network (NAN).

Frequency Shift Keying (FSK)

FSK is a digital modulation technique in which the frequency of the carrier signal varies according to the digital signal changes. The output of the an FSK modulation high frequency wave represents a high (binary 1) input value and a low frequency wave represents a low (binary 0).

The following image is the representation of the FSK modulated waveform along with its binary representation.

![Figure 54 FSK Modulation Wave](image)

Orthogonal Frequency Division Multiplexing (OFDM)

OFDM is a digital modulation technique where data is transmitted over different subcarriers. OFDM modulation contains overlapping spectra, but the signals are orthogonal and have in interaction with each other.

The following image represents data being transmitted over various subcarriers.
FSK and OFDM comparisons

While networks may have to operate with both FSK and OFDM for some time, network operators may be able to bypass FSK networks to OFDM networks based on endpoint selection. They may also want to ensure that the key network equipment supports both FSK and OFDM. The obvious advantages of OFDM limit the feasibility of installing only an FSK network. Interoperability between FSK and OFDM are discussed later in this document.

- FSK uses a single carrier while OFDM makes efficient use of the spectrum by allowing carrier overlap
- OFDM divides the channel into narrowband flat fading subchannels, making it more resistant to frequency selective fading that exist in single channel systems (FSK)
- OFDM has adequate channel coding and interleaving to recover data (symbols) lost due to frequency selectivity of the channel
- FSK is more sensitive to sample timing offsets than OFDM
- OFDM allows more decoding techniques and complexity in deployment options
- OFDM provides better protection against co-channel interference and impulsive parasitic noise
- OFDM supports higher data rates and wider channel spacing
- OFDM has better channel resiliency
Table 19 Frequency Hopping Spread Spectrum (FHSS) RF Modulation and PHY Data Rates

<table>
<thead>
<tr>
<th>Frequency band (MHz)</th>
<th>Modulation</th>
<th>Data rate (kbs)</th>
<th>Channel spacing (kHz)</th>
<th>Number of channels</th>
</tr>
</thead>
<tbody>
<tr>
<td>863–870 EMEA</td>
<td>2FSK mode 1</td>
<td>50</td>
<td>100</td>
<td>69</td>
</tr>
<tr>
<td></td>
<td>2FSK mode 2 &amp; 3</td>
<td>100</td>
<td>200</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>OFDM option 4</td>
<td>150</td>
<td>200</td>
<td>35</td>
</tr>
<tr>
<td>865–867 India</td>
<td>2FSK mode 1</td>
<td>50</td>
<td>100</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>2FSK mode 2, 3</td>
<td>100, 150</td>
<td>200</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>OFDM option 4</td>
<td></td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>902–907.5 &amp; 915–928</td>
<td>2FSK mode 1, 2, 3</td>
<td>50, 100, 150</td>
<td>200</td>
<td>91</td>
</tr>
<tr>
<td>North America and Brazil</td>
<td>2FSK mode 4, 5</td>
<td>200, 300</td>
<td>400</td>
<td>45</td>
</tr>
<tr>
<td></td>
<td>OFDM option 4</td>
<td>200</td>
<td></td>
<td>91</td>
</tr>
<tr>
<td></td>
<td>OFDM option 3</td>
<td></td>
<td>400</td>
<td>45</td>
</tr>
<tr>
<td></td>
<td>OFDM option 2</td>
<td>800</td>
<td></td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>OFDM option 1</td>
<td>1200</td>
<td></td>
<td>13</td>
</tr>
</tbody>
</table>

Feature CGM-WPAN-FSK-NA and WPAN-OFDM-FCC (Combined) Consult each individual datasheet for specific module functionality and feature support

PHY/MAC
- IEEE 802.15.4 g/e/v
- IETF 6LoWPAN (RFC 6282)
- Wi-SUN 1.0 Certified

Frequency range support
- 902–928 MHz (and subsets of it to comply with country regulations)
  - North America: ISM:902–928 Mhz
  - Australia: 915–912 Mhz
  - Brazil: 902–907.5, 915–912 Mhz

Frequency hopping spread spectrum
- Frequency hopping
- OFDM: 31 channels, 800 kHz channel spacing
- 2FSK: 64 channels, 400 kHz channel spacing

Output conducted transmit power (average)
- OFDM: up to 28 dBm
- FSK: 30 dBm

Link budget
- OFDM: Up to 143 dB, depending upon antenna gain and data rate
- FSK: up to 154 dB, depending upon antenna gain and data rate

Receiver sensitivity
- OFDM: down to -105 dBm
- FSK: down to -114 dBm
- FSK & OQPSK: down to -114 dBm
A CR-Mesh network is a secure end to end network meaning, the CGE devices contain certificates that identify them as part of the network they are joining. The endpoints are either configured at that factory or restaged onsite with the networks Service Set Identifier (SSID) and security certificates that are required and generated from the host network. Without the proper SSID the device will not find the proper host network and without certificates from the host network the endpoint will be refused an IP address when they request to join the network over the configure SSID.

The CR-Mesh SSID is advertised through IEEE 802.15.4e enhanced beacons which can also pass additional vendor information. Enhanced Beacon (EB) messages allow communication modules to discover PANs that they can join. The EB message is the only message sent in the clear that can provide useful information to joining nodes. CGRs drive the dissemination process for all PAN-wide information.

Joining devices also use the RSSI value of the received EB message to determine if a neighbor is likely to provide a good link. The transceiver hardware provides the RSSI value. Neighbors that have an RSSI value below the minimum threshold during the course of receiving EB messages are not considered for PAN access requests.

RFC 768 User Datagram Protocol (UDP) is the recommended transport layer over 6LoWPAN. Table 21 summarizes the protocols applied at each layer of the NAN.

### Table 21 Summary of Network Protocols in the NAN

<table>
<thead>
<tr>
<th>Networking Layers</th>
<th>Networking Protocols and Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport</td>
<td>UDP</td>
</tr>
<tr>
<td>Network</td>
<td>6LoWPAN, IPv6 addressing, RPL, Neighbor Discovery for IPv6, DHCPv6</td>
</tr>
<tr>
<td>MAC</td>
<td>IEEE 802.15.4e</td>
</tr>
<tr>
<td>Physical</td>
<td>RF sub-GHz, FHSS, FSK, OFDM, IEEE 802.15.4g</td>
</tr>
</tbody>
</table>
The CR-Mesh network defines a SSID, which identifies the owner of the resilient mesh. The SSID is programmed on the CGE, and that same SSID must also be configured on the Cisco Connected Grid Router (CGR) WPAN interface during deployment.

A CR-Mesh NAN is subdivided into one or more Personal Area Networks (PAN). Each PAN has a unique PAN-ID. A PAN-ID is assigned to a single WPAN module installed within an FAR. All CGEs within a PAN form a single CR-Mesh network.

**Figure 56  PAN, NAN and SSID locations in the network**

---

**CR-Mesh Authentication and Data Flow**

There are several requirements for the CCI infrastructure to support a CR-Mesh installation. Layer 3 interfaces on the FAR, such as Ethernet/fiber or cellular, must be enabled and properly addressed. Route entries must be added on the head-end router. The FAR is connected to the HER using secure IPSEC FlexVPN tunnels. Loopback interfaces must be enabled for network management, local applications, and tunnel or routing configuration must be completed.

**ZTD in depth:**

Zero Touch

- Stage the FAR with bootstrap configuration to callhome to the headend network
- FAR is powered up and acquires Certificates from PKI infrastructure in Headend for HTTPS communication
- FAR initiates communication with the tunnel provisioning proxy which forwards request to FND behind firewall
- FND configures Flex/IPsec tunnels on the FAR and ASR
- FAR now registers with the FND through the Tunnel
- CR mesh related configuration should be prestaged in the FND and pushed via the FND once the FAR registers

CGE onboarding to the CR-Mesh network:
CCI CR-Mesh Access Network Solution

- CGE are field configured with EUI64 (MAC), SSID, regional compliance factors, CGE identity CA certificate, or NMS certificate.
- Once the FAR registers the FND pushes down WPAN configuration to start onboarding crmesh devices
- CR mesh authenticate with AAA servers in headend and acquire x.509 certificates and Join the FAR WPAN link neighbor table and start process of acquiring DHCPv6 address
- Once DHCP address is acquired the CRMesh RPL protocol allows the mesh to join the PAN and send a registration request to the FND
- CGE become manageable via CoAP Simple Management Protocol (CSMP) once they are registered with FND

Proper time synchronization is required to support the use of certificates on network equipment and CGE devices. The network management services (FND) is configured and ready to accept clients. Certificates are generated from a public key infrastructure on the CCI network and the network can support IPv6 traffic natively or through the use of GRE tunnels.

If the network has been prepared to accommodate all of the above requirements, the endpoints are staged with the network SSID and unique PKI certificate for each device.

As endpoints are powered on, each device attempts to connect to their programmed SSID. The FAR hosting the SSID should hear the request if the endpoint is within range. A proper site survey should have been completed prior to deploying the CGE in their final locations to guarantee communication and RF coverage with redundancy/fail-over planning.

The FAR will than begin to authenticate the endpoint. First the FAR will validated the endpoints certification key using RADIUS services. After the device is validated, the device will be assigned an IP address from the data center DHCP server.

After successful authentication and ip assignment the endpoint will be able to communicate across the CCI network if proper DMZ traffic policies are enabled. The endpoint should be able to communicate with the management systems (FND) for operational status and device management including firmware updates, mesh formation, and device status.

In some cases, the device will also need access to public cloud services. Additional security policies may need to be created to ensure the communication to these services are available. Also, since these endpoints are communicating as IPv6 endpoints additional consideration may be needed to encapsulate traffic from these devices across the network to the public cloud–based services. The public cloud services may be running native IPv6 to communicate to the endpoint essentially requiring an end-to-end IPv6 communications path from the endpoint to the public cloud services.

Figure 57 depicts the CR-Mesh access network solution across the CCI network, system components at each layer, and the end-to-end communication path.
After endpoints are onboarded to the network and the network is in an operational state, CR-Mesh performs routing at the network layer using the Routing Protocol for Low-Power and Lossy Networks (RPL). The CGEs act as RPL Directed Acrylic Graph (DAG) node, whereas the FAR serves as the RPL DAG root. The FAR runs RPL protocol to build mesh network and serves as the RPL root.

When a routable IPv6 address is assigned to its CG-Mesh interface, the CGE sends Destination Advertisement Object (DAO) messages informing the DAG root (FAR) of its IPv6 address and the IPv6 addresses of its parents. Using the information in the DAO messages, the FAR builds the downstream RPL route to CGE. A Destination Oriented Directed Acrylic Graph (DODAG) is formed, which is rooted at a single point, namely the FAR. The FAR constructs a routing tree of the CGEs. When an external device such as FND try to reach the CGE, the FAR routes the packets with source routing. The RPL tree rooted at the FAR can be viewed at the FAR. In the RPL tree, a CGE can be a part of a single PAN at a time. Cisco FND monitors and manages the CGEs with CSMP protocol.

Interoperability of FSK and OFDM endpoints and devices

CR-Mesh endpoints can support various phy modes under the adaptive modulation feature which allows both FSK and OFDM modulation schemes to coexist. The Link can operate in both modes, eg the forwarder can use phy mode 66 (2FSK 150KBps) and reverse path can use phy mode 166 (OFDM 800KBps). The entire PAN can use various modes based on channel conditions.

When Resilient Mesh nodes supports several IEEE 802.15.4g PHY modes, adaptive modulation enables Resilient Mesh nodes changing their data rate on a packet-by-packet basis to increase the reliability of the link.

Two methods are used to enable a Resilient Mesh node to switch data rate:

- OFDM modulation switch - RF driver can decode frames with different data rates according to PHY header MCS values
MR-FSK modulation switch – based on MR-FSK mode switch header. When MR-FSK mode switch header is received, Resilient Mesh Endpoints, supporting mode switching, change their PHY mode to the new PHY mode defined in the MR-FSK mode switch header, in order to receive the following packets.

To ensure compatibility the WPAN module should support both FSK and OFDM. Cisco OFDM WPAN modules are backwards compatible to FSK. Using an OFDM WPAN module allows endpoints to be either FSK or OFDM. Mixing endpoint types allows for easy migration between technologies.

Scale and Redundancy

In the figure below if the FAR that is hosting PAN1 where to fail and the devices on PAN1 would be orphaned. If a CGE was in range of either the PAN2 WPAN interface in the second FAR the devices and theoretically all the other devices would fail over to PAN2.

Optionally, a second WPAN could be configured as a standby to PAN1 in close proximity to the existing FAN router. Failover is dependent on the ability for the CGEs to hear other CGE or WPAN interfaces in the same SSID.

Figure 58 CR-Mesh Access Network Architecture with a Smart Street Lighting Solution in RPoP

Ongoing Operation

CGE Firmware Upgrade Procedure

The CR-Mesh CGE firmware can be installed by CLI or from Cisco FND using the CSMP protocol and multicast over IPv6.
For more information on upgrading the firmware, see the latest Release Notes for the Cisco 1000 Series Connected Grid Routers for Cisco IOS Release at the following URL:

- [www.cisco.com/go/cgr1000-docs](http://www.cisco.com/go/cgr1000-docs)

**Compromised CGE or Network Device Eviction**

A compromised endpoint is one where the CGE can no longer be trusted by the network and/or operators. Nodes within an IEEE 802.15.4 PAN must possess the currently valid Group Temporal Key (GTK) to send and receive link-layer messages. The GTK is shared among all devices within the PAN and is refreshed periodically or on-demand. By communicating new GTKs to only trusted devices, compromised nodes may be evicted from the network and the corresponding entry is removed from the AAA/NPS server, preventing the device from rejoining the network without a new valid certificate. Additional devices that could be evicted from the network include any infrastructure components that have been joined using a PKI certificate.

**Power Outage Notification**

CR-Mesh supports timely and efficient reporting of power outages and restorations. In the event of a power outage, CR-Mesh endpoints enter power-outage notification mode and the CGE stops listening for traffic to conserve energy. The CGE network stack and included SDK triggers functions to conserve energy by notifying the communication module and neighboring nodes of the outage. The outage notification is sent using Cisco Connected Grid Router (CGR) battery backup with the same security settings as any other UDP/IPv6 datagram transmission to Cisco FND. This is documented as the "last gasp" feature of the CGR FAR.

In the event of a power restoration, a CR-Mesh endpoint sends a restoration notification using the same communication method as the outage notification. The communication modules unaffected by the power outage event deliver the restoration notification.

**CR-Mesh Access Network Solution IP Addressing**

For most CR-Mesh deployments, address planning will be required. The IPv4 addressing plan must be derived from the existing enterprise scheme while the IPv6 addressing plan will most likely be new. In all cases, the network needs to be dual-stack (IPv4, IPv6) capable.

Table 22 shows CR-Mesh devices with their IPv4 and IPv6 capabilities.

<table>
<thead>
<tr>
<th>Device/Application</th>
<th>IPv4 Capable</th>
<th>IPv6 Capable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Field Network Director</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>HER</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CGE application manager (Cimcon LightingGale light manager)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CGE Endpoints (eg Cimcon Street Light Controller)</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>CGR 1000 series</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

The following communication flows occur over IPv6:

- CGE to FND
- CGE to CGE application server

All other communications can occur over IPv4.
IPv4 address to all devices in the network are statically configured, IPv6 address to CGE are allocated by CPNR. CGE also receives FND IPv6 address and application server IPv6 address during DHCP allocation. As CCI currently does not support IPv6 endpoints, at the access network, this traffic is encapsulated in FlexVPN over IPv4.

CCI DSRC Access Network Solution

This chapter, which discusses design of the CCI DSRC Access Network for endpoint connectivity, includes the following major topics:

- DSRC Access Network, page 120
- DSRC Vertical Solution, page 124

DSRC Access Network

Dedicated Short Range Communications (DSRC) is a two-way short-to-medium-range wireless communication technology designed for low latency, high performance data transmission for critical communications for safety applications.

A regulatory effort by the Federal Communications Commission (FCC) in the U.S. consisted of the allocation of 75 MHz of spectrum in the 5.9 GHz band for use by the Intelligent Transportation System (ITS).

Similarly, the European Telecommunications Standards Institute (ETSI) allocated 30 MHz of spectrum in the 5.9 GHz band for ITS, under a similar standard called ITS-G5 (ETSI EN 302 663).

Figure 59 depicts the spectrum allocation and channel plan.

Figure 59  DSRC and ITS-G5 Spectrum Allocation and Channel Plan (Source: IEEE 802.11-13/0282r2.doc)

Standardization efforts have been carried out by various organizations to standardize a set of protocols and messages to facilitate communications between Vehicle to Infrastructure (V2I), Vehicle to Vehicle (V2V), and Vehicle to Pedestrian (V2P) under the defined spectrum. Collectively these capabilities are commonly referred to as Vehicle to Everything (V2X).

In the U.S., the main standardization bodies are IEEE and SAE, where the main standard components for DSRC, such as IEEE 802.11p, IEEE 1609, and SAE J2735, are standardized.
In Europe, the main standard bodies are ETSI and CEN, which have produced a set of C-ITS standards. ETSI has focused on specifications for the communication system and vehicle-to-vehicle applications; CEN has mainly produced standards for vehicle-to-infrastructure applications. A mandate was issued by the European Commission to ensure the standards are consistent and approved by EU members and associated states.

It is expected that the deployment of C-ITS in Europe will be driven by automobile manufacturers and supported by local governments. In the U.S., it was proposed by the Department of Transportation in 2016 to mandate DSRC in all new vehicles, but no legislature process is in place. In December 2018, an RFC from U.S. Department of Transportation was sent out to request comments on current and future communication technologies for V2X, including DSRC and cellular (C-V2X).

While much industry and standards body debate continue, DSRC is by now a well-established and proven technology, though not yet widely deployed. As such this release of CCI has adopted DSRC as its first V2X access technology and has specifically tested with the Cohda DSRC Roadside Unit (RSU). The CCI architecture is fully capable of supporting other V2X radio access technologies and Cisco will continue to assess the market developments in this area and may in the future test and validate other V2X technologies.

**DSRC Protocol Stack**

Figure 60 shows the standardized layer of protocols for DSRC. The scope of the CCI CVD includes DSRC implementation only and is based on the SAE J2735 2016 revision.

![DSRC Protocol Stack](image)

- IEEE 802.11p defines extensions to the Wi-Fi standard for vehicular communications.
  - 1609.2: Security
  - 1609.3: Network and Transport Layer:
    - The WAVE Short Message Protocol (WSMP)
    - IPv6 along with various transport layer (i.e., TCP and UDP)
- SAE J2735 defines the format and structure of DSRC messages, including data frames and data elements for exchanging data between vehicles (V2V) and between vehicles and infrastructure (V2I). For example:
Basic Safety Message (BSM)—Every DSRC-equipped vehicle broadcasts its core state information in a BSM message at rate of 10 messages/second. A BSM message is a broadcast message sent from On-Board Unit (reside in vehicle) to Roadside Unit (at roadside, connected to backhaul) using 802.11p protocol. A BSM message indicates the vehicle its position, direction, speed, and other parameters.

Table 23 includes a full list of SAE DSRC messages:

<table>
<thead>
<tr>
<th>Message Name</th>
<th>Acronym</th>
<th>From</th>
<th>Method</th>
<th>To</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Safety Message</td>
<td>BSM</td>
<td>Vehicle</td>
<td>Broadcast</td>
<td>Surrounding vehicles and RSU</td>
<td>Exchange safety data regarding vehicle state.</td>
</tr>
<tr>
<td>Common Safety Request</td>
<td>CSR</td>
<td>Vehicle participating in BSM</td>
<td>Unicast</td>
<td>Vehicle</td>
<td>Request additional information to be added to BSM.</td>
</tr>
<tr>
<td>Emergency Vehicle Alert</td>
<td>EVA</td>
<td></td>
<td>Broadcast</td>
<td>Surrounding vehicles</td>
<td>Send warning that an emergency vehicle is operating, and additional caution is required</td>
</tr>
<tr>
<td>Intersection Collision Avoidance</td>
<td>ICA</td>
<td>Equipped vehicle or infrastructure</td>
<td>Broadcast</td>
<td>Other DSRC devices</td>
<td>Warning of a potential collision with a vehicle entering an intersection without right of way</td>
</tr>
<tr>
<td>Map Data</td>
<td>MAP</td>
<td>RSU</td>
<td>Broadcast</td>
<td>Surrounding vehicles</td>
<td>Provide intersection and roadway lane geometry data for one or more locations.</td>
</tr>
<tr>
<td>NMEA corrections</td>
<td>NMEA</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>Wrap NMEA 183 differential corrections to be transported in DSRC media</td>
</tr>
<tr>
<td>Personal Safety Message</td>
<td>PSM</td>
<td>VRU device</td>
<td>Broadcast</td>
<td>Surrounding vehicles</td>
<td>Send safety data regarding kinematic state of Vulnerable Road Users (VRU)</td>
</tr>
<tr>
<td>Probe Data Management</td>
<td>PDM</td>
<td>RSU</td>
<td>Broadcast</td>
<td>Surrounding vehicles</td>
<td>Control type of data collected and sent by OBUs to RSU. Instruct vehicles to adjust data.</td>
</tr>
<tr>
<td>Probe Vehicle Data</td>
<td>PVD</td>
<td>Vehicle</td>
<td>Unicast</td>
<td>RSU</td>
<td>Exchange collections of information about typical vehicle traveling behaviors along a segment of the road</td>
</tr>
<tr>
<td>Road Side Alert</td>
<td>RSA</td>
<td>--</td>
<td>Broadcast</td>
<td></td>
<td>Send alerts for nearby hazards to travelers</td>
</tr>
<tr>
<td>RTCM corrections</td>
<td>RTCM</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>Wrap RTCM differential corrections to be transported in DSRC media</td>
</tr>
<tr>
<td>Signal Phase and Timing Message</td>
<td>SPAT</td>
<td>RSU in signalized intersection</td>
<td>Broadcast</td>
<td>Surrounding vehicles</td>
<td>Convey current status of one or more signalized intersections</td>
</tr>
</tbody>
</table>
Most work on DSRC is focused on active safety for collision avoidance by providing driver alerts based on sophisticated sensing and vehicle communications. ITS pilot deployment use case examples include the following:

- **Emergency Electronic Brake Lights (EEBL)**—An application where the driver is alerted to hard braking in the traffic stream ahead. This provides the driver with additional time to look for and assess situations developing ahead.

- **Forward Collision Warning (FCW)**—An application where alerts are presented to the driver in order to help avoid or mitigate the severity of crashes into the rear end of other vehicles on the road. Forward crash warning responds to a direct and imminent threat ahead of the host vehicle.

- **Intersection Movement Assist (IMA)**—An application that warns the driver when it is not safe to enter an intersection—for example, when something is blocking the driver’s view of opposing or crossing traffic. This application only functions when the involved vehicles are each V2V-equipped.

- **Left Turn Assist (LTA)/Right Turn Assist (RTA)**—An application where alerts are given to the driver as they attempt an unprotected left turn across traffic, to help them avoid crashes with opposite direction traffic.

- **Blind Spot/Lane Change Warning (BSW/LCW)**—An application where alerts are displayed to the driver that indicate the presence of same-direction traffic in an adjacent lane (Blind Spot Warning), or alerts given to drivers during host vehicle lane changes (Lane Change Warning) to help the driver avoid crashes associated with potentially unsafe lane changes.

- **Do Not Pass Warning (DNPW)**—An application where alerts are given to drivers to help avoid a head-on crash resulting from passing maneuvers.

- **Vehicle Turning Right in Front of Bus Warning**—An application that warns transit bus operators of the presence of vehicles attempting to go around the bus to make a right turn as the bus departs from a bus stop.

Other DSRC use case examples include:

- **Transit Signal Priority**—An application where the public transit vehicles communicate with roadside infrastructure to time the traffic signal to allow priority for public transit vehicles.
Routing Management for Emergency Services—An application using DSRC to improve upon emergency response efforts in the event that traffic accidents occur.

Automatic Toll Collection—An application to collect tolls automatically, such as ETS (European Teletoll Services) and Telepass.

DSRC Vertical Solution

DSRC Solution over CCI

The CCI network architecture includes the DSRC access technology that is depicted in Figure 61:

The network components for DSRC communication include:

- On-board Unit (OBU):
  - DSRC device on vehicle to send and receive DSRC messages.
  - The DSRC OBU, which is provided by car manufacturers, and typically is an OEM product from the RSU manufacturers.

- Roadside Unit (RSU):
  - DSRC device on the roadside that is connected to the backhaul network.
  - The DSRC RSU tested with CCI is the Cohda RSU MK5. It is manufactured and available through Cohda Wireless at the following URL:
    - https://cohdawireless.com/sectors/v2x
  - The Cohda RSU MK5 is an IP67-rated outdoor device. Cohda wireless also manufactures DSRC OBU, which has the same features as DSRC RSU, but without the ruggedized enclosure. The MK5 unit supports DSRC radio and comes with an Ethernet port, GNSS antenna, and microSD for firmware storage.
This device can be powered using Power Over Ethernet (POE).

Traffic Monitoring Center (TMC)/DSRC Applications:

- Traffic monitoring and DSRC applications typically reside in the Data Center.
- The monitoring tool processes DSRC messages and sends out alternate messages and/or interworking with other network elements based on the analytics results.

Many DSRC use cases require very low latency in order to avoid accidents. The Cisco CCI solution recommends edge compute network components be located at the roadside to facilitate fast responses at the access layer:

Edge Compute Node:

- A platform for DSRC application (i.e., DSRC DSLink and Broker) where DSRC messages from multiple DSRC RSUs are aggregated. Additional input beside DSRC messages, such as LiDAR at street crossing and weather monitoring sensor input, are possible based on the type of application run on the edge compute platform.
- The recommended Edge Compute platform in the CCI solution is the Cisco IC3000 Industrial Compute Gateway. Other Cisco platforms offer memory and compute with container technology such as Cisco IE 4000, Cisco Connected Grid Router (CGR) 1000, and Cisco IR829 Integrated Services Router.
- Recommendation for RSU roadside placement is one RSU per quarter mile and one IC3000 node per mile, therefore with one IC3000 consuming data from four RSUs. This is based on the factors of radio coverage, latency, and number of vehicles.
- The specific DSRC application running on the Edge Compute node is out of scope for the CCI solution. However, the Cisco Customer Experience (Advanced Services) organization have broad experience and defined offers to assist with these types of DSRC applications and use cases.

Regional Hub:

- Aggregation for multiple roadway intersections for regional services.
- Typical equipment for aggregation and services needed include the Catalyst 9000 and UCS platform for service software.

The RSU and equipment in the roadside cabinet are connected to a CCI PoP access ring at the CCI network access layer. Typically, equipment residing in the roadside cabinet at intersections includes:

Traffic Light Controller:

- A control system to control traffic lights and coordinate vehicles, cyclists, and pedestrians move across intersections as efficient and safe as possible.
- For traffic light controllers, Cisco has previous experience working with Econolite Group, Inc. (https://www.econolite.com) but CCI is capable of supporting a broad range of such traffic systems and vendors.

Traffic Detection System:

- Smart cities and roadway agencies want to have a complete view of intersection usage in order to provide safety protection for future roadway improvement. The detection system includes components such as cameras, LiDAR, and Radar to detect vehicles, bicycles, and pedestrian with advance software performing analytics to provide information desired by agencies.
- For traffic detection systems, Cisco has previous experience working with Iteris, Inc. (https://www.iteris.com) and has completed basic connectivity validation with the Iteris Vantage Next® video detection platform using CCI. However it should also be noted that CCI is capable of supporting a broad range of such systems and vendors.
Uninterrupted Power Supply (UPS):
- If a power failure occurs with vital equipment such as the traffic light controller, a UPS device provides power so that traffic can still move smoothly.
- For UPS systems, CCI tested with Schneider Electric (APC) UPS systems (http://www.schneider-electric.com). It should be noted that CCI is capable of supporting a broad range of UPS systems and vendors.

DSRC applications can either be standalone or interworking with the roadside equipment together to provide safety and smooth traffic for the travelers on the roadways.

FND release 4.6 and newer allows for the deployment of a small form factor Linux based device agent for secure lifecycle management of endpoint devices. The IoT device agent (IDA) uses multiple techniques for device management, configuration, and health monitoring. Cisco IDA facilitates secure life cycle management of Cisco products including the IC3000 as well as third-party devices including the Cohda RSU and OBU devices.

For information about management for Cohda DSRC RSU, please refer to the following URL:


FND is the management tool for managing the Cisco IC3000 gateway. The FND image should be installed and provisioned with an IP address, and all IC3000 devices that will be managed by the FND need to be provisioned. The DHCP server for IP address assignment should be configured with option 43.

FND should also prepare the firmware image and application to be installed on IC3000 (for example, IoX applications) so image upgrades can be performed once the IC3000 is on-boarded.

The management tasks performed between FND and IC3000 include the following:

- **On-boarding the IC3000**—When IC3000 is connected to the network, it obtains an IP address from the DHCP server. In the DHCP offering message, it contains Option 43, which provides the IP address of FND for the IC3000. IC3000 starts the registration process once it learns the FND IP address; the registration events will show up on the FND console and indicate that the IC3000 device has been on-boarded once registration completed.

- **Firmware Upgrade**—FND first uploads the firmware to the IC3000, and then updates the firmware on IC3000.

- **Application Installation**—FND (FD in case of Oracle Database) first uploads the application to the IC3000, installs the application onto the IC3000, and then starts the application.

Cisco IC3000 also has a built-in Local Manager that allows a user to access the management software by plugging in a laptop to the dedicated management port. The Local Manager is a web-based user interface to manage, administer, monitor, and troubleshoot the application on the IC3000.

For complete details, please refer to the “Adding the IC3000 Gateway(s) to FND” section of the Cisco IC3000 Industrial Compute Gateway Deployment Guide at the following URL:


DSRC Communication Types

The three categories of DSRC communications are described below. The use cases discussed earlier can be further categorized based on the design:

- **Vehicle to Vehicle (V2V)**—DSRC information to alert or assist drivers in avoiding dangerous situation using vehicle-to-vehicle communication:
  - Emergency Electronic Braking Lights (EEBL)
  - Intersection Movement Assist (IMA)
  - Forward Collision Warning (FCW)
  - Blind Spot/Lane Change Warning (BSW/LCW)
CCI DSRC Access Network Solution

- Left Turn Assist (LTA)

- Vehicle to Infrastructure (V2I)—DSRC information to alert or assist drivers in avoiding dangerous situation using vehicle-to-infrastructure communication:
  - Red Light Violation Warning (RLVW)
  - Curve Speed Warning (CSW)
  - Reduce Speed/Work Zone Warning (RSZW)

- Vehicle to Pedestrian (V2P)—DSRC information to alert drivers and/or pedestrians about avoiding dangerous situation using vehicle-to-pedestrian communication:
  - Pedestrian Crossing Assist (PCA)

The V2I use cases are the focus area for CCI where DSRC messages initiated from the vehicles are received by DSRC RSU at the roadway that is connected to the CCI Infrastructure, and vice versa. The DSRC messages from DSRC RSU are forwarded to the Edge Compute Node to be processed, and a copy of the DSRC message will be forwarded to the Regional Hub and/or the Data Center for further processing.

Data Flow

As shown in Figure 62, the Cisco IC3000 Industrial Compute Gateway (Edge Compute Node) has three Ethernet interfaces: one is dedicated for management traffic and the other two are designed for input and output interfaces. All management-related traffic should be designated to the management port. DSRC messages from DSRC RSU will be received on the Input interface of IC3K and will be transmitted to Regional Hub/Data Center on the Output interface.

Figure 62  DSRC Message Flow
CCI LoRaWAN Access Network Solution

This chapter, which discusses design of the CCI LoRaWAN Access Network for endpoint connectivity.

LoRaWAN Access Network

LoRa (Long Range) is a radio modulation technology for wireless communication. It is proprietary and owned by Semtech, which drives the technology via the LoRa Alliance where the open LoRaWAN protocol and ecosystem is developed.

The LoRa technology achieves its long-range connectivity (up to 10km+) by operating in a lower radio frequency that trades off data rate. Because its data rates are below 50kbps and because LoRa is limited by duty cycles and other restrictions, it is suitable in practice for non-real time applications for which one can tolerate delays.

LoRaWAN operates in an unlicensed (ISM band) radio spectrum. Each country/region allocates radio spectrum for LoRaWAN usage with regional parameters to plan out the regional frequency plan and channel usage.

In Europe, LoRaWAN operates in the 863-870 MHz frequency band, while in the US, LoRaWAN operates in the 902-928 MHz frequency band. The diagram below shows spectrum allocations for different countries/regions.

LoRaWAN is a Media Access Control (MAC) layer protocol running on top of the LoRa radio as the physical layer. It is designed to allow low-power devices to communicate with applications over long-range wireless connections.

Some of the key benefits of the LoRaWAN access technology include:

- Long range (up to 15km)
- Low cost radio, enabling low cost devices
- Low power given the opportunity for small battery powered sensors with 5-10 years+ battery life
- End-to-end encryption and Over the Air Activation (OTAA) for devices
- Strong industry forum via the LoRa Alliance with more than 500 members (including Cisco); for more information, please refer to:
  - https://lora-alliance.org/
- Very large ecosystem of sensors and vendors with excellent interoperability
An End-to-End LoRaWAN architecture is illustrated in Figure 64.

CCI can support a broad set of use cases using LoRaWAN technology. Key Smart City use cases include:

- Parking:
  - Parking occupancy and availability
  - Utilization reports and analytics
- Waste management:
  - Waste Bin Level Detection
  - Waste Bin Temp (inside)
Waste Bin sensor battery level

Environmental monitoring:
- Sensor-based air quality
- Software modeling of air quality

Water monitoring:
- Water metering
- Water levels and flood sensing/detection
- Water quality monitoring

Note: For more use case details refer to the use case section of this document.

The architecture components include LoRaWAN devices, LoRaWAN Gateways, Network Server, and Application Servers. The LoRaWAN devices to Network Server and Application Servers are secured by keys, which are exchanged between devices and servers during device over-the-air on-boarding process. In a CCI deployment, LoRaWAN gateways are managed with Cisco FND, the Cisco network management system for gateways. More detail of each solution components is described below.

LoRaWAN Devices

- LoRaWAN devices categorized into three classes: Class A, B, and C. All LoRaWAN devices must implement Class A, whereas Class B and Class C are extensions to the specific Class A devices.
  - Class A devices—Support bi-directional communication between a device and a gateway. Uplink messages can be sent at any time from the device, typically as a triggered event or a scheduled interval. Then the device can receive messages at two receive windows at specified times after the uplink transmission. If no message is received, the device can only receive messages after the next uplink transmission.
  - Class B devices—Support scheduled receive windows for downlink messages. Devices can receive messages in the scheduled receive windows; this is not limited to receiving messages only after being sent.
  - Class C devices—Support receive windows open unless they are transmitting to allow low-latency communication. However, Class C devices consume much more energy compared to Class A devices.

- LoRaWAN devices are certified by LoRa Alliance to ensure interoperability.

- LoRaWAN device activation can be completed in two ways:
  - OTAA: Over the air activation
  - ABP: Activation by personalization

Earlier release of CCI added LoRaWAN devices via the ABP process. When using ABP, unique hardcoded DevAddr and security keys are manually entered at the time a device joins and remain the same until physically changed.

OTAA is more secure and the recommended method for onboarding LoRaWAN devices. Dynamic DevAddr are assigned and security keys are negotiated with the device as part of the join-procedure. OTAA also makes it possible for devices to join other networks.

LoRaWAN Gateways

- LoRaWAN Gateways receive messages from devices across the LoRaWAN network, encapsulate the message into IP, and forward the message to the Network Server over IP Backhaul.
Conversely, LoRaWAN messages from the application or the network server will be sent through the best available gateway, determined by the network server, to reach the device.

The Cisco Wireless Gateway for LoRaWAN is the solution component chosen in the CCI infrastructure. It has the following functionality:

- Cisco Wireless Gateway for LoRaWAN can be a standalone gateway (Ethernet backhaul) or an IOS interface (Integrated Interface) on Cisco IR809, IR829 router. A LoRaWAN gateway can be part of a wired CCI network located in a PoP or connected over a cellular network from a RPoP.
- Cisco Wireless Gateway for LoRaWAN adopts Semtech Next Gen gateway reference design (known as v2 gateway).

The Linux container (LXC) in the Cisco Wireless Gateway for LoRaWAN runs Actility long range router (LRR) packet forwarder image, which interworks with Actility Network Server long range controller (LRC) functionality for radio management

- Carrier and industrial grade: IP67 rating, PoE+ power, GPS, main and diversity antennas.
- Fully complies with LoRaWAN specifications 1.0x and 1.1.
- Two hardware SKUs: IXM-LPWA-800-16-K9 (868 MHz) and IXM-LPWA-900-16-K9 (915 MHz).
- Supports LoRaWAN regional RF parameters profiles through the LoRaWAN network server solution.
- Supports LoRaWAN devices class A, B, and C.
- Enables flexible topologies: standalone for Ethernet backhaul, one to multiple Cisco LoRaWAN Interface modules on Cisco IR809/IR829 routers.
- Managed by Cisco IoT FND; refer to the following URL:

Network Server

LoRaWAN messages sent by a device are broadcast and can be received by multiple LoRaWAN gateways within the range. The Network Server de-duplicates multiple copies of the same message for further process.

The messages received are LoRaWAN MAC layer messages. See Table 24 for message types.

<table>
<thead>
<tr>
<th>MAC Message Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>Join Request</td>
</tr>
<tr>
<td>001</td>
<td>Join Accept</td>
</tr>
<tr>
<td>010</td>
<td>Unconfirmed Data Up (acknowledge not required)</td>
</tr>
<tr>
<td>011</td>
<td>Unconfirmed Data Down (acknowledge not required)</td>
</tr>
<tr>
<td>100</td>
<td>Confirmed Data Up (acknowledge required)</td>
</tr>
<tr>
<td>101</td>
<td>Confirmed Data Down (acknowledge required)</td>
</tr>
<tr>
<td>110</td>
<td>RFU (Reserved for Future Usage)</td>
</tr>
<tr>
<td>111</td>
<td>Proprietary</td>
</tr>
</tbody>
</table>

The Network Server performs the following functions based on the message type it received:
Over-the-air activation (OTAA)—Each LoRaWAN device is equipped with a 64-bit DevEUI, a 64-bit AppEUI, and a 128-bit AppKey. The DevEUI is a globally unique identifier for the device that has a 64-bit address comparable with the MAC address for a TCP/IP device. The AppKey is the root key of the device. All three values are then made available to the Network Server to which the device is supposed to connect. The device sends the Join Request message, composed of its AppEUI and DevEUI. It additionally sends a DevNonce, which is a unique, randomly generated, two-byte value used for preventing replay attacks.

These three values are signed with a 4-byte Message Integrity Code (MIC) using the device AppKey. The server accepts Join Requests once it validates these keys and the MIC value and responds the Join Accept message.

The Join Accept message is encrypted by APPKey with information about NetID, DevAddr, and additional local parameters.

This completes the device activation process to allow device to communicate with the application server to send and receive information in encrypted format only can be decoded by the server with the appropriated keys.

**Figure 65** lists the key information details:

**Figure 65 Information Elements for MAC Messages**

<table>
<thead>
<tr>
<th>IE</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>DevEUI</td>
<td>A globally unique device ID in EU!64 format.</td>
<td>Built-in at Manufacture</td>
</tr>
<tr>
<td>DevAddr</td>
<td>A device ID of 32 bits that identifies the end device. Dev is composed of NetworkID and NetworkAddr.</td>
<td>Received after OTAA</td>
</tr>
<tr>
<td>AppEUI</td>
<td>A globally unique application ID in EU!64 format that uniquely identifies the application provider (i.e., owner) of the end device.</td>
<td>Built-in at Manufacture</td>
</tr>
<tr>
<td>NwkSKey</td>
<td>A device-specific network session key used by both the network server and the end device to calculate and verify the Message Integrity Check (MIC) of all data messages to ensure data integrity. It is further used to encrypt and decrypt the payload field of MAC-only data messages.</td>
<td>Derived after OTAA</td>
</tr>
<tr>
<td>AppKey</td>
<td>AES-128 root key specific to the end-device. Provisioned at manufacturing. AppKey is used to derive the AppSKey session key.</td>
<td>Built-in at Manufacture</td>
</tr>
<tr>
<td>AppSKey</td>
<td>A device-specific application session key used by both the network/app server and the end device to encrypt and decrypt the payload field of application-specific data messages. It may also be used to calculate and verify an application-level MIC to be optionally included in the payload.</td>
<td>Derived after OTAA</td>
</tr>
</tbody>
</table>

**Figure 66** depicts the call flow of OTAA procedures:
Data messages: The messages can be uplink or downlink messages, with or without acknowledgment by the receivers. The Network Server uses NwkSKey to validate the message integrity and prepare the payload of the data messages (message type of 010, 011, 100, 101) to the corresponding application server by publishing the message to a data connector used by the applications.

- Network Server dynamically selects the best gateway for optimized sensor data traffic routing.
- Implements Adaptive Data Rate (ADR) scheme to optimize the individual data rates and RF output of each connected device to allow more end devices to communicate.
- Network Server supports reporting and administration functions.
- Actility Network Server ThingPark Enterprise (TPE) (available on the Cisco Global Price List) is the network server validated in the CCI infrastructure.

**Application Server**

- An application is a collection of devices with the same purpose, of the same type.
- An Application Server typically resides in the cloud or on-premise and collects information from devices of the same purpose and of the same type.
- The Application Server uses AppSKey to de-encrypt the message to ensure data security.
- An Application Server may offer web interface for users to manage/view devices as well as data collected from the devices.
- An Application Server may also offer an API such as RESTFUL for integration with external services.
- The CCI infrastructure supports Application Servers as long as it is able to connect with Actility Network Server using a supported connector such as HTTPS, WebSocket, etc. For a complete list of connectors supported by Actility, refer to the following URL:
  
Management of LoRaWAN solution components listed above are achieved in two steps. First, bring up Cisco Wireless Gateway for LoRaWAN manually and then use the Actility Management tool as described below:

1. On Cisco Wireless Gateway for LoRaWAN gateway:
   a. Load the desired IOS image to Cisco Wireless Gateway for LoRaWAN manually.
   b. Load the LRR image to Cisco Wireless Gateway for LoRaWAN to IXM container manually.
   c. Set up proper configuration of Cisco Wireless Gateway for LoRaWAN.
      Refer to the *Cisco Wireless Gateway for LoRaWAN Software Configuration Guide* for more details.

2. On ThingPark Enterprise (TPE) server:
   a. Add Cisco Wireless Gateway for LoRaWAN information into the Base Station list.
   b. Then add the sensor information and application information to the TPE management tool as described in Actility ThingPark Enterprise Management Portal, page 134.

**Actility ThingPark Enterprise Management Portal**

- Actility has several GUI management tools on TPE server:
  - Device Manager—It manages device list creation to allow devices to join the network. Once a device is created, it provides device status information along with associated device parameters such as DevEUI, DevAddr, RSSI, SNR, battery status, application associated with the device, and time stamp for last uplink/downlink activities.
  - Base Station Manager—It manages the Base Station connected to the TPE server and displays the Base Station status, its unique ID, LRR ID, software version, and time stamp for last activity.
  - Application Manager—It manages applications connected to the TPE server, its URL, application ID, and number of devices using the application.

Figure 67 depicts LoRaWAN integration in the CCI infrastructure. The communication data flows generated from the PoPs and RPoPs are described in detail below.
Data Flow from Internal PoPs (Flow A)

- Cisco Wireless Gateway for LoRaWAN is connected to Cisco Industrial Ethernet (IE) switches in a REP ring at PoPs.
- The TPE server resides in the Data Center.
- A Cisco Wireless Gateway for LoRaWAN receives sensor data from LoRaWAN devices, then forwards to the TPE server at the Data Center through the transit network in the SD-Access fabric.
- If the message has application payload, TPE prepares the message and puts it into the connector appropriate for the Application Server in the cloud.

Data Flow from Remote PoPs (Flow B)

- Cisco Wireless Gateway for LoRaWAN gateways are connected with Cisco IR809/IR829/IR1101 for cellular backhaul in standalone mode in an R-PoP (i.e., the gateway works in standalone or integrated mode to leverage IR809/IR829/IR1101 router for cellular backhaul).
- The Cisco IR809/IR829/IR11101 establishes a VPN tunnel with the HE router residing in the DMZ.
- The Actility TPE server resides in the Data Center.
- A Cisco Wireless Gateway for LoRaWAN receives sensor data from LoRaWAN devices. It sends data to the data center through the cellular backhaul encapsulated within the secure VPN tunnel.
The headend router de-encapsulates the message from the VPN tunnel and forwards it to the destination IP, under the condition the firewall allows the traffic to go through.

LoRaWAN device addition via Actility management portal

Adding a new device to Actility:

Step 1: Open the Actility management interface and select Device:Create – LoRaWAN Generic

Step 2: Add device information
- Model
- Name
- DevEUI
- Activation Mode
- JoinEUI (AppEUI)
- AppKey
- Associate your sensor to the appropriate application for data streaming

Step 3: Device add confirmation

Step 4: Device add validation

Step 5: Verify device join process

Step 6: Device status shows active

LoRaWAN deployment guidance

Wireless signals can be impacted by interference in the spectrum as well as obstacles that exist in the real world. In this regard, LoRaWAN is no different than other wireless technologies. A proper site survey should be completed prior to the installation, verification should be done after installation, and ongoing periodic checks of the wireless health of the area should be continued for the life of the installation.

Cisco has created the following document to provide basic guidance for outdoor LoRaWAN installations: https://salesconnect.cisco.com/open.html?c=27f90a9a-f7c7-4c6d-9020-8fd5b9cd0025

CCI Rail Trackside Access Network Solution

Many of the Rail onboard applications nowadays depend on reliable train-to-ground communications for safety and security of the trains. Furthermore, there are applications that require high bandwidth and low latency to provide a quality passenger experience. Some examples of these applications are train maintenance and monitoring applications, CCTV, and passenger Wi-Fi services.

The train-to-ground communication includes three major components:

- Onboard communication component:
  This is the communication system on the train. It typically uses wireless and/or cellular technology to communicate between the train and ground network.
  
  The onboard network, which includes network and safety equipment within the train, is out of scope for this guide.

- Trackside communication component:
This is the ground-based network to provide cellular and/or wireless coverage alongside the train track to communicate with the train.

- For cellular communication, it relies on cellular coverage along the train track.
- For a dedicated wireless trackside communication network, wireless radios are set up along the trackside to communicate with the wireless components on the train.

These trackside radios connect to the CCI network at an extended node or policy extended node within an Edge PoP.

A cellular based train to trackside solution is out of scope for this guide.

Network Backhaul and Datacenter component:

Each Edge PoP is connected to the datacenter/HQ PoP through an IP or SDA transit. In the datacenter resides the equipment and services required to complete the end to end communication for the train services.

This guide will discuss the design for enabling communication to the train, but not the services within the train.

To overcome the challenges of providing high bandwidth, low latency communication to a moving train at speed, Fluidmesh radios and technology will be used. They are well suited to the rail environment, providing up to 500Mbps at up to 225 MPH. The design and integration of the Fluidmesh technology within the CCI network will be the focus of this guide.

**Rail Solution System Level Overview**

The diagram below depicts a high-level system view of the Rail Solution under the CCI infrastructure.
Connected Trains

The train infrastructure consists of an onboard network and a train to trackside radio network. The train to trackside radio network connects the services supported on the train with systems and services in the centralized infrastructure.

For the dedicated train to trackside wireless communication, there is a Fluidmesh radio on the train which communicates with the Fluidmesh trackside radio. It supports high speed seamless roaming between trackside radios while providing high throughput and low latency.

Trackside Network

The CCI network spreads across a large geographical area, logically divided into several Points-of-Presence (PoPs). Each Edge PoP has one or more Access Rings comprised of extended or policy extended node IE switches (Maximum 30) in a Resilient Ethernet Protocol (REP) ring. The IE switch models include IE3300, IE3400, IE 4000, and IE 5000. Refer to “Point of Presence (PoP)” section for more detail.

The Fluidmesh trackside devices connect to the IE switches in the PoPs within a trackside virtual network (VN). A group of trackside radios in the same IP subnet forms a Trackside Radio Group (TRG). These trackside radio groups can span one or more Access Rings in the Edge PoP.

Station Network

A station network design needs to provide various passenger services as well as to maintain safety and security of the train station and its passengers. The network also needs to scale to meet the demand of the number of passengers at the station during peak hours.

The station network can be an Edge PoP or connected to an Edge PoP in the CCI environment and provides connectivity to devices such as train schedule bulletin boards, ticketing kiosks, surveillance cameras, and passenger devices/mobiles via wired or wireless connections. These devices are either directly connected to the IE switches in the Access Ring or, more generally, connected to the Wireless Access Points using Wi-Fi technology. Refer to Table 11 “APs tested and supported in CCI” for a complete list of Access Points supported in CCI to make Access Point selection choices in the Station Network.
A Centralized Wireless LAN Controller (WLC) deployment model is recommended for Station Network. The Centralized WLC deployment model is to have a pair of WLC reside in the Shared Services to serve wireless Access Points across all PoPs.

This way, the system is able to scale more efficiently to support the aggregated number of passengers during peak hours. Passengers typically enter the train station, travel from one station to another, then exit the train station. The WLC choice is dependent on the number of wireless users expected during peak travel times which is typically the morning and evening rush hours.

The Central WLC support is available in CCI infrastructure. Refer to “CCI Wi-Fi Access Network Solution” section in this document. The specific solution option for Station Network is documented in the “Centralized WLC deployment” section.

Backhaul

The CCI infrastructure supports two types of backhaul:

- transparent backhaul where traffic resides entirely within the SDA fabric using an SDA Transit (e.g. routed over a private or dark fiber)
- opaque backhaul where traffic exits the SDA fabric domain to an IP transit network (e.g. a Service Provider or private MPLS network) and returns to the SDA fabric at the other side of the transit network

Refer to the section “Backhaul for Points of Presence” for more information. Both types of backhaul are applicable for rail environment.

Centralized Infrastructure

This is the area encompassing the CCI data center or headquarters PoP and the shared services. The servers and services supporting the trackside end to end solution reside here. This includes the Fluidmesh gateway devices necessary to support the seamless roaming from train to trackside.

Overview of Fluidmesh Technology

This section discusses the Cisco Fluidmesh technology relevant to the CCI Trackside Network.

Fluidmesh Fluidity is the technology that enables seamless roaming between a train radio and the trackside radio network. In this context, seamless roaming occurs when there is no disruption in the communication path as the train radio associates and disassociates with trackside radios. Fluidity makes use of a customized MPLS implementation as the mechanism to ensure this unbroken communication path which overcomes the limits of standard wireless protocols. This implementation acts as an overlay on the CCI network. It enables data throughput of up to 500Mbps at up to 225 Mph (360 Kmh) with optimal wireless conditions.

Fluidity operates over a flat Layer 2 network or a routed Layer 3 network. In Layer 2 Fluidity, all Fluidmesh devices and therefore, all trackside roaming, occurs within a single subnet or broadcast domain. Layer 3 Fluidity supports roaming between L3 domains. As an Edge PoP is based on a Layer 3 network, it is required to deploy Layer 3 Fluidity to enable roaming when the train moves from one TRG (IP subnet) to another.

MPLS relies on label identifiers, rather than the network destination address as in traditional IP routing, to determine the sequence of nodes to be traversed to reach the end of the path.

An MPLS-enabled device is also called a Label Switched Router (LSR). A sequence of LSR nodes configured to deliver packets from the ingress to the egress using label switching is denoted as a Label Switched Path (LSP), or “tunnel”.

LSRs situated on the border of an MPLS-enabled network and / or other traditional IP-based devices are also called a Label Edge Router (LER).

Below is a brief description of Fluidmesh Terminologies frequently referred to in the context of this document:
Train radio – The physical radio onboard the train that connects the Onboard Network (OBN) within the train to the trackside infrastructure. This is the demarcation point between the Fluidmesh wireless network and the train network. The radio will impose an MPLS label on packets coming in from the train network or remove the label when packets are moving to the train network. A single train will typically have one or more train radios to communicate with the trackside infrastructure, for example at the front and at the back of the train.

Trackside radio – The physical radio installed along the trackside that communicates with the train radio and other trackside Fluidmesh devices. It can operate as a Mesh Point, a Mesh Point Wireless Relay, or a Mesh End.

Mesh Point – A Mesh Point primarily serves to swap MPLS labels as traffic ingresses and egresses. This means all Mesh Points function as an LSR and act as a relay between the train radio and a Mesh End. When a Mesh Point is connected to the wired network, it is operating in infrastructure mode. A Mesh Point can also operate in wireless only mode to act as a wireless relay.

Mesh End – Based on which version of Fluidity (L2 or L3) is being used, the Mesh End serves different purposes. In both versions, the Mesh End is the logical demarcation between the Train Radio Group (which communicates by swapping MPLS labels) and the L3 IP network. In a Layer 3 Fluidity network a Mesh End also serves to terminate L2TP tunnels connected to a Mesh End gateway in the datacenter. The traffic from Mesh Points enters the Mesh End and is then forwarded to the datacenter Mesh End through these L2TP tunnels. When traffic is received from the datacenter Mesh End, it is removed from the L2TP tunnels and forwarded to the train through the Mesh Points. Using the MPLS terminology described before, all Mesh Ends function as LSRs and LERs. A Mesh End must have a wired connection and it must be in the same broadcast domain as the Mesh Points.

Global Gateway – A global gateway is a special type of Mesh End that enables seamless roaming between different Layer 3 domains. It resides in the datacenter as described above. A global gateway serves to anchor numerous Mesh Ends in different broadcast domains and provide seamless roaming across them. This is achieved by building L2TP tunnels between the Global Gateway and all Mesh End devices. This fast MPLS label swapping between the above nodes along with L2TP tunnels between the Mesh Ends and Global Gateway enable seamless roaming at high speed and high throughput.

Plug-ins – Fluidmesh features are dependent on software licenses called Plug-ins. There are plug-ins for maximum throughput, security, and other network features. The high availability feature, called TITAN and explained later in this document, also requires the appropriate plug-in.

The diagram below depicts a Layer 3 Fluidity network to summarize the nodes and their placement in the network.
Solution Components

The following components are used in the CCI Rail trackside solution, in addition to the components which are already part of the main CCI infrastructure.
Fluidmesh Mesh Point and Mesh End

In a TRG, there are Mesh Points and Mesh Ends and they must be in the same broadcast domain.

The trackside radios are deployed along the rail track. For maximum performance, it is recommended to connect the mesh points wired to the IE switches in the Edge PoP access ring. Given the proper IE switch configuration, the mesh points can be powered through PoE.

When traffic enters the train radio, it will impose an MPLS label for that radio. As the train moves along the train track, the train radio associates and disassociates with the trackside radios (Mesh Point) along the track based on the radio coverage. As the train radio roams, it will change the MPLS label based on which trackside radio it is associated with. When the trackside Mesh Point receives this traffic, it will perform the function of a Label Switch Router (LSR) and do a lookup in its MPLS label table for the Mesh End and swap the labels. It will then send the packet onto the network with a destination address of the Mesh End.

The Mesh End unit functions as a Label Edge Router (LER) as well as an L2TP tunnel endpoint. When a packet arrives from a mesh point, the mesh end will add an L2TP header pointing to the Global Gateway in the datacenter PoP. It will then forward this packet to the Global Gateway. When L2TP traffic is received from the Global Gateway, it will remove the L2TP header and forward to the correct Mesh Point in the LSP. The FM 3500 radio can perform the role of a Mesh End or Mesh Point. When operating as a Mesh End, it can also process wireless traffic from the train radios.

A FM 3500 is suitable to serve as a Mesh End if the expected aggregated traffic does not exceed 500 Mbps. The FM 1000 is the recommended Mesh End unit when the aggregate traffic will not exceed 1 Gbps.

Fluidmesh Global Gateway

The Global Gateway enables seamless roaming when a train radio roams between different Train Radio Groups. This is necessary because the LSP from a mesh point terminates at the mesh end and does not go beyond. The Global Gateway overcomes this by using L2TP tunnels to every Mesh End in the Edge PoPs. The MPLS labeled packets from the Mesh Ends are encapsulated in these L2TP tunnels and the Global Gateway performs its role as a Mesh End by removing these headers and labels before forwarding these packets onto the CCI network. In the CCI network, the Global Gateway resides in the data center PoP in a Virtual Network for train and trackside communication. Because the Global Gateway...
is the head end for the Fluidmesh network, all return traffic destined for the train must use the Global Gateway as the next hop. This traffic is then encapsulated with an MPLS label and L2TP header which is then forwarded to the appropriate Mesh End.

Both the FM 1000 and FM 10000 can perform as a Global Gateway. The selection criteria for choosing between them is based on the bandwidth requirements. The FM 1000 can process aggregate throughput of up to 1Gbps while the FM 10000 handles up to 10 Gbps.

**High Availability (Fluidmesh TITAN)**

TITAN is a Fluidmesh software feature for fail-over technology that constantly tracks link status and network performance of a pair of Mesh Ends or Global Gateways configured in an active-standby role. In case of any failure of the primary unit, traffic is rerouted to the redundant secondary unit. The pair is configured with a single virtual IP address to appear as one unit.

Under the TITAN configuration, the pair of devices will fall into a primary or secondary role (based on the unit’s Mesh ID) and issue keepalives between them in a pre-configured interval (typically between 50 ms and 200 ms). The secondary unit becomes the new primary when it has not received a keep-alive message within the pre-defined interval. Simultaneously, the new primary issues commands to all other Fluidmesh devices in the domain to inform them of the change while updating its own tables and sending gratuitous ARPs out its ethernet port to ensure new traffic will be forwarded properly to the new primary. This feature allows failure detection and recovery in 500ms.

When TITAN is configured on the Mesh Ends and Global Gateways, each device must be configured with two L2TP tunnels. Each Mesh End unit (Primary and Secondary) establishes a L2TP tunnel to each Global Gateway (Primary Global Gateway and Secondary Global Gateway with TITAN).

This is the expected result after configuring all the tunnels. Only one tunnel is in connected state and the other 3 are in idle state:

- L2TP tunnel between primary Global Gateway and primary Mesh End: **CONN**
- L2TP tunnel between primary Global Gateway and secondary Mesh End: **IDLE**
- L2TP tunnel between secondary Global Gateway and primary Mesh End: **IDLE**
- L2TP tunnel between secondary Global Gateway and secondary Mesh End: **IDLE**

If the primary Global Gateway fails, the L2TP tunnels between the primary Global Gateway and primary Mesh End become IDLE. The secondary Global Gateway will become the new elected primary and the L2TP tunnel between secondary Global Gateway to the primary Mesh End will become CONN.

Similarly, at the trackside network level, if the primary Mesh End fails, the L2TP tunnels between it and the primary Global Gateway will become **IDLE**. The L2TP tunnels between the secondary Mesh End (which will be elected the new primary) and the primary Global Gateway will become **CONN**.

It is recommended to use TITAN on all Mesh End pairs and Global Gateway pairs.

**Quality of Service Support**

Fluidmesh forwarding engine supports DiffServ like end-to-end QoS treatment to user traffic. The implementation leverages MPLS technology to bring traffic-engineering features to wireless mesh networks.

The Fluidmesh QoS implementation supports 8 priority levels (0 to 7 with 0 being the lowest priority and 7 being the highest) as below.

Refer to RFC 791 and RFC 2474 for more detail.
When an IP packet first enters the mesh network at an ingress Fluidmesh unit, the TOS field of the IP header is inspected and a priority class using the Class Selector is assigned in the MPLS EXP bits. The class number is the first 3 most significant bits (bit 5 – 7) of the TOS field.

The priority class is then preserved through the end-to-end path to the egress Fluidmesh unit.

For packets being transmitted over the wireless, the 8 priority levels are further mapped into four classes, each corresponding to a specific set of MAC transmission parameters.

Table 26 Mapping between Packet Priority and Access Category

<table>
<thead>
<tr>
<th>Priority</th>
<th>Access Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Best Effort</td>
</tr>
<tr>
<td>1</td>
<td>Background</td>
</tr>
<tr>
<td>2</td>
<td>Background</td>
</tr>
<tr>
<td>3</td>
<td>Best Effort</td>
</tr>
<tr>
<td>4</td>
<td>Video</td>
</tr>
<tr>
<td>5</td>
<td>Video</td>
</tr>
<tr>
<td>6</td>
<td>Voice</td>
</tr>
<tr>
<td>7</td>
<td>Voice</td>
</tr>
</tbody>
</table>

As the labels are swapped between Mesh Points, the EXP bits are copied to each label. When the MPLS packet reaches the Mesh End, the TOS bits are copied into the L2TP IP Header as a Class Selector value. At the Global Gateway, the L2TP header and MPLS label are removed and the packet original DSCP/TOS value is retained.

Refer to 802.1e for Access Category and QoS information.

Network Provisioning and Monitoring

Configuration Tools (Configurator and RACER)

The Configurator is a web-based configuration software that resides on the Fluidmesh device locally. A user can connect to the device L3 IP address configured from the Virtual Network IP Pool to view this interface.
RACER is a cloud-based configuration portal that can be accessed through the Internet. Using the RACER portal, a Fluidmesh device reachable from the RACER portal can be configured remotely. The RACER portal also supports different permissions based on the user role. An administrator would be able to edit a device config or assign devices to other users and a viewer would only be able to view a device’s configuration. The Fluidmesh devices must also be entered into the RACER portal before the device can have a successful connection. These features ensure that rogue devices and rogue users cannot make changes to the Fluidmesh devices.

A Fluidmesh device has to be configured with some basic settings before it can be part of the wireless network. If a new unit is being configured for the first time or has been reset to factory default configuration for any reason, the unit will enter Provisioning Mode. This mode allows setting of the unit’s initial configuration.

If the unit is in Provisioning Mode, it will try to connect to the internet using Dynamic Host Configuration Protocol (DHCP):

- The device will try and connect to partners.fluidmesh.com on port 443
- If the unit successfully connects to the internet, the unit can be configured by using RACER or by using the local Configurator tool.
- If the unit fails to connect to the internet, the unit must be configured using the local Configurator interface.

If the unit is not able to connect to the internet, it will revert back to a Fallback state and its setting will become the factory default setting with IP address to 192.168.0.10/255.255.255.0.

In this state, RACER can still be used in an offline mode. All the devices are entered into the RACER portal and the configuration built for each one. The configurations for all the devices can then be exported as a single file.

Using the Configurator page on the Fluidmesh device, the RACER section gives the option to upload a RACER configuration file. The device will choose the correct config from the file and apply the configuration.

Because these configurations can be done ahead of time in the RACER portal, this is the recommended option if Internet access to the device is undesirable. The devices can be pre-staged before deployment or a user with a laptop can upload the config to the Fluidmesh device at the deployment site. After the device is fully configured and has reachability within the VN, further config changes can be made using RACER offline, but from a centralized location.

Fluidmesh MONITOR

Fluidmesh MONITOR is a centralized radio network diagnostic and monitoring tool.

It is used to:

- Monitor the real-time condition of Fluidmesh-based networks.
- Generate statistics from network history.
- Verify that device configuration settings are optimal for current network conditions.
- Receive event loggings for diagnostic and repair purposes and generate alerts if network-related faults arise.
- Analyze network data with the goal of increasing system uptime and maintaining optimum network performance.
- Generate and back up network statistics databases for future reference.
Fluidmesh and CCI Network Integration and Considerations

Cisco DNAC

Virtual Network and Segmentation

When integrating Fluidmesh into the CCI Network, it is recommended to set it up as a separate service in a Virtual Network dedicated to train to trackside communication. Alternatively, a virtual network with other shared train or station related services (such as signage, ticketing, etc.) can be used. Within the virtual network, micro-segmentation can then be used to prevent Fluidmesh devices from communicating with these station devices. Note that in an Edge PoP, only Policy Extended Nodes support micro-segmentation.

Refer to CCI's Cisco Software-Defined Access Fabric, page 14 section for macro and micro segmentation information.

IP Pool

The Fluidmesh devices will only use a DHCP address if they are able to reach the RACER portal through the Internet. Otherwise they must be statically addressed. Additionally, when a Mesh End is configured for L2TP and TITAN it requires more addresses. There will be one IP address for the interface, one IP address for the L2TP tunnel, and then a virtual IP address that is also configured on the secondary Mesh End. All of these addresses come out of the IP scope allocated
to the Train Radio Group. If the Virtual Network is dedicated to the Fluidmesh devices and RACER will not be used in Online mode, DHCP should be disabled for that Train Radio Group. Otherwise, the DHCP scope should be configured to exclude the number of addresses needed.

When using Layer 3 Fluidity, the IP addressing for the train radios and devices behind those radios is not related to or part of the IP addressing used for the trackside communication VN. It is recommended to create IP Pools for the trackside radios and gateway devices aboard the train as an administrative task.

Host Onboarding

The Fluidmesh devices do not support 802.1X, therefore MAB authentication is the only other option for secure onboarding. Once authenticated through MAB, the device can operate on the CCI network.

Refer to the section in this guide, Onboarding Endpoints, page 70, for more information.

Datacenter PoP

As mentioned in the section on IP Pools, the IP addressing for the train radios and gateway devices is not part of the trackside communication VN. This means there must be an explicit route added for these networks with the Global Gateway as the next hop. This will ensure that all return traffic destined for the train will enter the Global Gateway and be tunneled to the appropriate Mesh End.

Edge PoP

As discussed previously, Layer 3 Fluidity supports multiple Train Radio Groups, where each group is in a different IP subnet. There are multiple considerations and recommendations when planning this deployment.

- Each Mesh Point should be connected to a PoE capable IE switch in an access ring
- If the number of Fluidmesh devices in the Train Radio Group exceeds the maximum number of nodes in an access ring, they can span across multiple access rings as long as that subnet is present in those rings. This should be balanced with the expected throughput in that Train Radio Group.
- The Redundant Mesh Ends should be connected to the Fabric in a box switch stack on different members to eliminate single points of failure. If the Mesh Ends are FM 3500s, they should be connected to different access ring switches.

See Figure 72 for an example of a PoP with a pair of FM 1000s covering the entire PoP.
Figure 72  FM 1000 as Mesh End for a Single Ring in the Entire PoP

See Figure 74 for an example of a pair of FM 1000s covering two access rings within a PoP.
See Figure 73 for an example of a pair of FM 1000s covering separate access rings. The standby links are not shown to improve clarity.
The below diagram shows the sequence of MPLS tag handling and L2TP encapsulation events after the Fluidmesh devices have been integrated into the CCI network.
The summary of the sequence of events:

1. IP devices on the train send packets to their destinations
2. The packets are switched to the Train Radio (FM 4500) on the train.
3. The Train Radio adds MPLS tags to the packets, selects the best trackside radio and sends the packets over the wireless network to R5 on the trackside.
4. R5 on the trackside receives the packets. Since it is a Mesh Point, it will send the data toward the Mesh End. It looks up the destination in the label lookup table, swaps the label for the next Mesh End, and sends it out.
5. The packets are forwarded to the next IE switch
6. The IE switch continues forwarding the packets to the Mesh End
7. The FM 1000, which is the Primary Mesh End, encapsulates the packets into an L2TP tunnel connected to the Global Gateway and forwards to the Edge PoP Fabric-in-a-box
8. The packets are forwarded from the Edge Pop Fabric-in-a-box to the Transit network
9. The Transit network forwards the packets to the Datacenter PoP
10. The packets arrive at the Datacenter PoP to be placed in the Trackside VN
11. The packets are forwarded to the Primary Global Gateway
12. The Global Gateway removes the L2TP and MPLS headers and forwards the original data packets to their destination
End-to-End QoS Integration

As described in the Fluidmesh QoS section, when Mesh Points exchange packets with other Mesh Points and the Mesh End, they have an MPLS label where the EXP bits are set based on the inner payload DSCP. The IE switches are unable to match on the MPLS EXP bits and therefore within the access ring, a different QoS strategy is required. Using Day N templates, a MAC ACL configured on each switchport connected to the Fluidmesh devices allows it to match on the device MAC address. This MAC address is created by concatenating 00:F1:CA with the last six octets of the burned in MAC address of the device which is found in the Configurator tool. For example, if the burned in MAC address is 40:36:5A:12:34:56, the MAC address used for the MAC ACL will be 00:F1:CA:12:34:56.

With this information, QoS can be performed based on those ACLs. Note that this does not allow differentiated service for the different types of traffic coming from the train, but rather all train traffic can be marked with a configurable level of service within the Edge PoP access ring.

When the packets reach the Mesh End, a L2TP header is attached with the DSCP value based on the inner payload. The Fabric in a box will then process the data according to the QoS policies.

Refer to the CCI Network QoS Design, page 48 for more details of QoS handling in CCI.

Trackside Network Design and Considerations

Required trackside radio spacing is based on achieving the RSSI radio coverage for the targeted data rates. Typical distance is around 800 meters (0.5 mile) apart. Whenever possible, deploy radios along both sides of tracks in a zig-zag fashion for best coverage.

The radio placement can be a single radio or dual radios per pole as shown in below diagram. The signal for single radio per pole will be split between two MIMO antennas, which results in a shorter trackside radio placement interval due to the RF power reduction. A typical splitter RF loss is -3 dB, resulting in half power. However, with a single radio per pole the handoff does not occur as the train passes the pole (unlike the two radios per pole option). While this is a cost saving measure, depending on the site survey, throughput requirements, and pole placement, a single radio per pole may not provide enough coverage.

The dual radios per pole configuration increases the allowable distance between poles for the same coverage requirement as shown in the below diagram.

The dual radios per pole configuration enables multi-frequency support that allows multiple channels to be used to improve aggregate network throughput.

A dual radio deployment is recommended for better coverage over longer distances with more options in selecting frequencies.
As the typical distance between radios is around 800 meters (0.5 mile), an Access Ring with 30 IE switches covers around 15 miles in a linear setup along trackside. To cover the desired area, one can expand the nodes in a TRG group into multiple Access Rings. Each TRG must be able to support the aggregate throughput desired for the train.

Fluidmesh Product Compliance and Physical Deployment

Products designed to support the Rail industry are routinely exposed to harsh conditions. When deploying a rail solution within the CCI context, care must be taken when choosing where to locate devices. The table below summarizes the location options given the temperature and mounting options.

Table 27  Product Installation Summary

<table>
<thead>
<tr>
<th>Product</th>
<th>Installation Location Options</th>
<th>Temperature Rating</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>FM 3500</td>
<td>Trackside</td>
<td>-40C to 75C</td>
<td>No M12 conn</td>
</tr>
<tr>
<td>FM 4500</td>
<td>Train</td>
<td>-40C to 80C</td>
<td>M12 conn or Fiber</td>
</tr>
<tr>
<td>FM 1000</td>
<td>Datacenter or Field Center</td>
<td>-20C to 55C</td>
<td>Rack/VESA/DIN Rail/Wall mount</td>
</tr>
<tr>
<td>FM 10000</td>
<td>Datacenter</td>
<td>0C to 40C</td>
<td>Rack mount</td>
</tr>
</tbody>
</table>

Below is the Fluidmesh products compliance matrix for more detailed information.

Figure 77  Fluidmesh Product Compliance Matrix

| EN50155   | ☑ | ☑ | ☑ | ☑ |
| EN45545   | ☑ | ☑ | ☑ | ☑ |
| EN50121-4 | ☑ | ☑ | ☑ | ☑ |
| EN61373   | ☑ | ☑ | ☑ | ☑ |
| EN55011   | ☑ | ☑ | ☑ | ☑ |
| EN55022   | ☑ | ☑ | ☑ | ☑ |
| EN55024   | ☑ | ☑ | ☑ | ☑ |
| EN55032   | ☑ | ☑ | ☑ | ☑ |
| EN61000-3-2 | ☑ | ☑ | ☑ | ☑ |
| EN61000-3-3 | ☑ | ☑ | ☑ | ☑ |
| EN61000-6-2 | ☑ | ☑ | ☑ | ☑ |
| EN61000-6-4 | ☑ | ☑ | ☑ | ☑ |
CCI Remote Point-of-Presence Design

This chapter covers CCI Remote Point-of-Presence (RPoP) design considerations to extend CCI macro segmentation and multiservice network capabilities to remote sites along with RPoP network, management and services high availability. RPoP in CCI can be managed using Cisco IoT FND application installed as an on-premise application in CCI shared services at HQ/DC site and/or IoT Operation Center in the Cisco Cloud; for guidance on cloud-managed gateways please see the Cisco Remote and Mobile Assets (RaMA) solution Cisco.com/go/rama.

This chapter includes the following major topics:

- Remote Point-of-Presence Gateways, page 154
- Remote Point-of-Presence Design Considerations, page 155
- RPoP High Availability Design, page 158
- RPoP Gateways Management, page 162

Remote Point-of-Presence Gateways

An RPoP is a Connected Grid Router (CGR) or Cisco Industrial Router (IR) and is typically connected to the Public Internet via a cellular connection, although any suitable connection can be used (such as xDSL or Ethernet), over which FlexVPN secure tunnels are established to the CCI HE in the DMZ.

This section covers the CCI Remote PoP gateway(s) that aggregates CCI services at RPoP(s) and extends the CCI multiservice network to RPoP endpoints. The RPoP router may provide enough local LAN connectivity, or an additional Cisco Industrial Ethernet (IE) switch may be required.

Cisco IR1101 as RPoP Gateway

Cisco IR1101 Integrated Services Router is a modular and ruggedized platform designed for remote asset management across multiple industrial vertical markets. As part of the CCI solution, the IR1101 can play the role of a CCI RPoP gateway aggregating remote site (RPoP) endpoints/assets and services and extending the CCI multiservice network to the RPoP along with network macro-segmentation.

For more details, refer to the IR1101 Industrial Integrated Services Router Hardware Installation Guide at the following URL:


As shown in Figure 78, IR1101 is designed as a modular platform for supporting expansion modules with edge compute. IR1101 supports a variety of communication interfaces such as four FE ports, one combo WAN port, RS232 Serial port, and LTE modules. The cellular module is pluggable and a dual SIM card and IPv6 LTE data connection are supported. SCADA Raw sockets and protocol translation features are available.

The IR1101 provides investment protection. The base module of IR1101 provides a modular pluggable slot for inserting the pluggable LTE module (or) storage module. The expansion module, on the other hand, also comes with a modular pluggable slot for inserting the pluggable LTE module. Overall, two pluggable LTE modules could be inserted on IR1101 (with an expansion module), thus enabling cellular backhaul redundancy with Dual LTE deployments.

Using the expansion module, an additional fiber (SFP) port, an additional LTE port and an SSD local storage for applications could be added to the capability of IR1101.

For more details on IR1101 base and expansion modules, refer the following URL:

Cisco CGR1240 as RPoP Gateway

The CGR 1000 Series Routers are ruggedized, modular platforms on which utilities and other industrial customers can build a highly secure, reliable, and scalable communication infrastructure. They support a variety of communications interfaces, such as Ethernet, serial, cellular, Radio-Frequency (RF) mesh, and Power Line Communications (PLC). In CCI, CGR1240 router can be used as Field Area Router and RPoP gateway with cellular backhaul for providing CR-Mesh access network in CCI PoP and RPoPs.

Refer to the section CR-Mesh Network Overview, page 104 for more details on CGR1240 in CCI and refer the “Table 9 CCI Remote PoP and IoT Gateways Portfolio Comparison” for more details on other IRs as RPoP gateways.

Remote Point-of-Presence Design Considerations

This section covers Cisco IR1101 as Remote PoP gateway design considerations in CCI. It discusses different services that RPoP offers with the capabilities of IR1101 and how the CCI multiservice network with macro-segmentation is extended to RPoP endpoints/assets via the CCI headend (HE) network in the DMZ.

RPoP Multiservice design in IR1101

As shown in Figure 30, the IR1101 base module supports four FE (LAN) ports and a RS232 Serial port which helps connect various CCI vertical endpoints. Multi-VRF, VLAN, and VPN features support on IR1101 helps segment the network and services in the CCI RPoP by configuring and maintaining more than one routing and forwarding tables.

Figure 78 shows an IR1101 in the CCI RPoP with the support for the following services:

- Ethernet Connectivity: Separate LAN network Connectivity for CCTV Camera, IXM Gateway (LoRaWAN access network at RPoP), Wi-Fi Access Points (Wi-Fi access network at RPoP) and Traffic Signal Controller in Roadways & Intersection use cases
- SCADA: DNP3 Serial-to-DNP3/IP protocol translation for SCADA Serial RTU devices connectivity at RPoP
- Edge Computing: Analyses the most time-sensitive data at the network edge, close to where it is generated, and enables local actions, independent of backhaul or cloud connectivity. A highly secure, extensible environment for hosting applications ensures authenticity of applications.

A separate LAN network is created on the IR1101 for each of the services in separate Virtual Route Forwarding (VRF) routes. Each LAN’s network traffic is backhauled via a secure FlexVPN tunnel to the CCI headend network over a Cellular or DSL based public backhaul networks. Figure 31 shows an example multiservice RPoP in CCI.
RPoP Macro-Segmentation Design in IR1101

Network segmentation divides a larger network into smaller sub-networks that are isolated from each other for improved security and better access control and monitoring. CCI provides network macro-segmentation using SD-Access which is discussed in the section Security Segmentation Design, page 38. CCI RPoP offering multiservice requires each service to be isolated from the other for network security and also provide a CCI RPoP connectivity to rest of CCI network i.e CCI PoP sites and Application Servers in HQ/DC site.

This section discusses the design considerations for macro-segmenting the RPoP network and extend CCI services to RPoPs (IR1101s) connected via public Cellular network (or other backhaul) to the CCI headend (HE) in the DMZ.

Since CCI RPoP traffic can traverse any kind of public WAN, data should be encrypted with standards-based IPSec. This approach is advisable even if the WAN backhaul is a private network. An IPSec VPN can be built between the RPoP Gateway (IR1101) and the HER in the CCI HE. The CCI solution implements a sophisticated key generation and exchange mechanism for both link-layer and network-layer encryption. This significantly simplifies cryptographic key management and ensures that the hub-and-spoke encryption domain not only scales across thousands of field area routers, but also across thousands of RPoP gateways.

IP tunnels are a key capability for all RPoP use cases forwarding various traffic types over the backhaul WAN infrastructure. Various tunneling techniques may be used, but it is important to evaluate the individual technique OS support, performance, and scalability for the RPoP gateway (IR1101) and HER platforms.

The following is tunneling design guidance:

- **FlexVPN Tunnel**— FlexVPN is a flexible and scalable VPN solution based on IPSec and IKEv2. To secure CCI data communication with the headend across the WAN, FlexVPN is used. IKEv2 prefix injection is used to share tunnel source loopbacks.
Communication with IR1101 in a RPoP is macro-segmented and securely transported as an overlay traffic through multipoint Generic Routing Encapsulation (mGRE) Tunnels. Next-hop resolution protocol (NHRP) is used to uniquely identify the macro-segments (VNs). It is recommended to combine mGRE, for segmentation, with a FlexVPN tunnel for secure backhaul to the HER.

Routing for overlay traffic is done via iBGP (VRF Lite) between the RPoP routers and the HER, inside the mGRE; similarly between the HER and FR is done inside p2p GRE.

Figure 79 depicts how CCI services are macro-segmented and extended to RPoPs via the CCI headend (HER) using Point-to-Point FlexVPN (between each IR1101 RPoP and the HER), and Multipoint GRE tunnels (from each IR1101 RPoP over the FlexVPN tunnel to the HER and from there to the Fusion Router).

Figure 79 IR1101 as RPoP with Macro-Segmentation Design

In Figure 80:

- CCI HQ/DC Site with Application Servers hosted in each VN for each CCI vertical service. CCI vertical services like Safety and Security (SnS_VN), LoRaWAN access based FlashNet street Lighting (LoRaWAN_VN), CR-Mesh access based Water SCADA (SCADA_VN or CR-Mesh_VN) etc., is macro-segmented in CCI SD-Access fabric with separate routing and forwarding (VRF) tables for each of the services.
- CCI Common Infrastructure or Shared Services consists of Cisco ISE, IoT FND, DHCP & Active Directory (AD) servers and WLC.
- CCI Fusion Routers (FR) connected to HQ/DC site via IP-Transit extends SD-Access fabric overlay VNs/VRFs created in fabric using Cisco DNA Center. FR provides access to non-fabric and shared services in CCI.
- The DMZ network portion of CCI communication headend, which includes:
  - A Cluster of ASR1000 Series or CSR1000v routers as Headend Routers (aka Hub Router for IP Tunnels)
  - Security FirePower/Firewalls in routed mode
  - DMZ Network Switch (L2)
CCI Remote Point-of-Presence Design

- IR1101s as Spoke routers in RPoP1 and RPoP2 connected to CCI headend via public cellular (LTE) WAN backhaul network.

Design Considerations

Cisco IR1101 routers in CCI RPoP supports multi-VRF, VLAN, and GRE to achieve network segmentation. To build on top of that, access lists and firewall features can be configured on CCI firewalls in the headend to control access to CCI from RPoP gateways/networks.

Tunneling provides a mechanism to transport packets of one protocol within another protocol. Generic Routing Encapsulation (GRE) is a tunneling protocol that provides a simple generic approach to transport packets of one protocol over another protocol by means of encapsulation.

As shown in Figure 80:

- Point-to-Point GRE tunnels are created over L3 (routed) network between Fusion Routers (FR) and HERs for each of the VNs/VRFs in CCI (specifically those needed at an RPoP, although all VNs will be present on the FR). An IP routing protocol peering between FR and HER must be established to exchange CCI SD-Access fabric overlay subnets and routing tables between HER and FR. While any routing protocol may be chosen to exchange IP routing, it is recommended to use BGP to simplify and ease the IP routing configurations in each VRF.

- IP routes among HER cluster nodes are advertised using a routing protocol redistributing static and Virtual Access Interface (VAI) routes among themselves.

- Each RPoP with IR1101 as a spoke router establishes a FlexVPN tunnel with a HER in CCI headend. This secured FlexVPN tunnel to each RPoP spoke can be established using IoT FND with certificated based authentication similar to CGR1240 FlexVPN tunnel to CCI headend.

- IR1101 with dual LTE modules and dual SIMs could establish two FlexVPN tunnels (one from base module Cellular interface and the other from expansion module cellular interface) to HER Cluster in Active-Active deployment with load-balancing (per-destination based).

- A multipoint GRE (mGRE) overlay tunnel is established for each CCI VN/VRF which needs to be extended to the RPoP. VRF forwarding is enabled on the mGRE tunnel interface on the HER (Hub) and IR1101 (Spoke) in a Hub-and-Spoke deployment. The mGRE overlay tunnel per VRF segments the network for each service in the FlexVPN. Next Hop Resolution Protocol (NHRP) with Next Hop Server (NHS) are configured on each spoke (IR1101) and Hub (HER) with a unique network-id for each VN/VRF.

- An IP routing protocol must be configured between RPoP IR1101 and HER to exchange routing tables between CCI headend and IR1101 in RPoP. BGP is recommended to simplify and ease the IP routing table advertisements in each VRF.

- LAN subnets or VLANs in RPoP VRFs can be redistributed or advertised to HER and then to FR via the routing protocol.

- Once routing information is exchanged between the RPoP and CCI HE, assets/endpoints in the RPoP can communicate with CCI Application Servers or endpoints in CCI PoPs via their respective VN/VRFs and shared services.

Detailed RPoP implementation steps are covered in the Implementation Guide of this CCI CVD.

RPoP High Availability Design

High Availability is achieved by designing redundancy at multiple levels of the CCI solution. This section discusses RPoP high availability design as listed below:

- CCI HER Redundancy
- WAN Backhaul Redundancy
- Combined Redundancy
CCI HER Redundancy

Design considerations discussed in this section primary addresses potential failure of the aggregation HER in the CCI headend.

- R1101 acting as FlexVPN spokes and deployed with a single or dual backhaul interface, connect to ASR 1000/CSR1000v aggregation routers in a multi-hub scenario.
- The backhaul interface may be any supported Cisco IOS interface’s type: cellular and/or Ethernet.
- Two ASR 1000s or more (multi hub) in the same Layer 2 domain can terminate the FlexVPN tunnel setup with a spoke.
- A single FlexVPN tunnel is configured to reach one of the ASR 1000s/CSR1000v routers
- Routing over the FlexVPN tunnel can be IKEv2 prefix injection through IPv4 ACL or dynamic routing, such as BGP (preferred).

![CCI Headend Router Redundancy](image)

As shown in Figure 80, HER redundancy is achieved using the IKEv2 load balancer feature. The IKEv2 Load Balancer support feature on HERs provides a Cluster Load Balancing (CLB) solution by redirecting requests from remote access clients to the Least Loaded Gateway (LLG) in the Hot Standby Router Protocol (HSRP) group or cluster. An HSRP cluster
is a group of gateways or FlexVPN servers in a LAN. The CLB solution works with the Internet Key Exchange Version 2 (IKEv2) redirect mechanism defined in RFC 5685 by redirecting requests to the LLG in the HSRP cluster. Failover between HERs will be automatically managed by the IKEv2 load balancer feature.

For more details on IKEv2 Load Balancer feature for FlexVPN, refer to the following URL:


ASR 1000s or CSR1000v act as a FlexVPN server. Remote spokes (IR1100) act as FlexVPN clients. The FlexVPN server redirects the requests from the remote spokes to the Least Loaded Gateway (LLG) in the HSRP cluster. An HSRP cluster is a group of FlexVPN servers in a Layer 3 domain. The CLB solution works with the Internet Key Exchange Version 2 (IKEv2) redirect mechanism defined in RFC 5685 by redirecting requests to the LLG in the HSRP cluster.

For the HER configuration, the HSRP and FlexVPN server (IKEv2 profile) must be configured. For the spoke configuration, the FlexVPN client must be configured. The IoT FND NMS should configure HSRP on the HER in addition to the FlexVPN server feature set. In case of any HER failure, tunnels are redirected to other active HER. If the primary fails, one of the subordinates resumes the role of primary.

The Cisco Cloud Services Router 1000V (CSR 1000V) is a router in virtual form factor. It contains features of Cisco IOS XE Software and can run on Cisco Unified Computing System (UCS) servers. The CSR 1000V is intended for deployment across different points in the network where edge routing services are required. Built on the same proven Cisco IOS Software platform that is inside the Cisco Integrated Services Router (ISR) and Aggregation Services Router (ASR) product families, the CSR 1000V also offers router based IPSec VPNs (FlexVPN) features. The CSR1000V software feature set is enabled through licenses and technology pack. Hence, it is suitable for a small HER Cluster deployment where number of IPsec (FlexVPN) tunnels required at the HER cluster is less (1000 tunnels).

In a medium or large deployment, the HER terminates multiple FlexVPN tunnels from multiple RPoP gateways and CGR1240s connected to the CCI Ethernet access rings or RPoPs. Hence, selecting a router platform that supports a large number of IP tunnels is vital to the headend design. It is recommended to use the Cisco ASR 1000 series routers as the HERs considering the potential FlexVPN tunnels scale in CCI.

Refer to the following URL for ASR 1000 HER scaling guidance:


**Note:** A HER Cluster may consist of >=2 number of routers depending on the FlexVPN tunnels scaling and load-sharing requirements in a deployment. It is recommended to have a minimum of two HERs in a cluster for high availability and load-sharing of RPoP backhaul traffic to the CCI headend.

**WAN Backhaul Redundancy**

RPoP gateways deployed over a single LTE network are a single point of failure, in the absence of a backup network like a secondary cellular radio interface. IR1101 acting as a RPoP gateway comes with the flexibility to host two LTE network interfaces, enabling WAN Cellular Backhaul redundancy to be achieved.

Active/Active load-sharing WAN backhaul redundancy design uses Dual LTEs (or other supported WAN interfaces) on IR1101 with two-tunnel approach, as shown in Figure 81.
- Two tunnels from the RPoP gateways terminates on two different HER clusters at the headend. In normal operational scenarios, both the tunnels would be UP and would be performing load-sharing of traffic across primary and secondary LTE modules. Load balancing is per-destination based.

- Should any of the WAN links (primary/secondary), only the corresponding Tunnel goes down. The other LTE module (and its corresponding Tunnel) would still be UP and keeps forwarding the traffic. For example, if the Cellular interface on the expansion module goes down, only Tunnel1 goes down. Hence, Tunnel0 can still forward the traffic.

In Figure 81, if the primary radio on base module fails, it could be a failure related to the radio or service provider. An Embedded Event Manager (EEM) script detects the radio interface failure (or) connectivity failure (read as service provider failure) over the primary radio. Failure of one of the radios detected by EEM script, leaving only one active radio and its corresponding tunnel for traffic forwarding.

Refer to the following URL for RPoP IR1101 WAN redundancy design considerations for Dual LTEs with Active-Active and Active-Standby tunnels from RPoP gateways to headend.


Combined Redundancy

It is possible to combine both HER and Backhaul redundancy. HER redundancy will allow a single HER cluster to be resilient, to load-balance RPoP routers across the cluster and also to serve RPoPs at the HE in the case of one or more HER failures. WAN Backhaul redundancy allows a given RPoP to have two WAN links, and for them to operate in an
active-active model, where both links are active and passing traffic, and in the event of a failure of one of these links all the traffic is sent via the remaining link; however to do this those two WAN links must terminate on different HER clusters. These HER clusters could be at the same physical location, or different locations.

RPoP Gateways Management

The Network Management System (NMS) for managing the RPoP gateways, its edge applications and serviceability functions can be achieved using following management application:

- Cisco Field Network Director (FND) – An on-premise management application that resides as part of the CCI common infrastructure (aka Shared Services). FND is a software platform that manages the multi-service network and security infrastructure for IoT applications in this CCI solution.

RPoP management using FND

The Cisco FND is a software platform that can monitor and manage several solutions including IR8x9/1101 & CGR1000 Series routers in RPoP. Refer the section Field Network Director (FND), page 31 in this document for more details on FND.

RPoP Network Management Serviceability

Once the RPoP gateway is zero touch deployed and registered with Cisco IoT FND, some of the important serviceability actions of FND must be considered. The following are the key IoT gateway serviceability actions that can be performed from FND:

- RPoP gateway monitoring – Remote monitoring of RPoP gateways from Cisco IoT FND in CCI Shared Services
- Gateway management – Remote management actions such as upgrading gateway firmware, remotely reconfiguring and provisioning of backhaul and enabling/disabling of secondary backhaul on gateways etc.,
- Edge Compute Application life cycle management – An IR1101 operating as a CCI RPoP supports Edge Compute (EC) capabilities. CCI customers could leverage this Edge Compute infrastructure to host custom applications to serve their custom requirements. Custom applications can be written and installed onto RPoP Gateway’s Edge Compute infrastructure remotely using the IoT FND. FND takes care of the lifecycle management of edge compute applications on the Gateway’s Edge Compute platform.
- RPoP gateway troubleshooting – A set of troubleshooting tools that can be used remotely such as Ping, Refresh Metrics, Reboot of gateways

Refer to the following URL for more details on Cisco IoT gateways network management and serviceability:

Validated Use Case Solutions

This chapter includes the following major topics:

- Smart Street Lighting CR-Mesh Solution with CCI Network, page 163
- Public Wi-Fi services with CCI Wi-Fi, page 167
- Safety and Security Solution with CCI, page 169
- Supervisory Control and Data Acquisition (SCADA) Networking over CCI, page 169
- FlashNet Lighting LoRaWAN solution over CCI, page 175
- Water Monitoring Sensor Technologies, page 175
- Axis Camera Onboarding and Integration over CCI, page 176

Note: Cisco Solution Support includes troubleshooting to the edge of the network (FAR). Please contact your service provider or manufacture for issues that may be discovered beyond the edge of the network.

Smart Street Lighting CR-Mesh Solution with CCI Network

Cisco FND and CIMCON LightingGale (LG) are the management platforms that provide end-to-end management for the CIMCON smart street lighting solution. Individual street lights (luminaires) are fitted with a CIMCON Street Light Control (SLC), which communicates over the CCI CR-Mesh network and allows control over the individual street lights, thus making them "smart."

Public Cloud

As tested in CCI, applications such as Cisco Kinetic for Cities and CIMCON LG are hosted in the public cloud. A secure FlexVPN tunnel is established from the cloud where CIMCON LG is hosted to the HER hosted in the CCI. In that way, the communication from CIMCON LG and the CCI network is secured. The communication between the CIMCON LG and Cisco CKC is secured by https. Refer to Figure 82 below for the architecture of the Smart Street Lighting Solution over CCI and its connectivity to applications in the public cloud.

CIMCON LightingGale

CIMCON LG is an example of a public cloud application. It is a Web-based system primarily used to configure, monitor, and acquire various types of data relevant to street lighting. Acquisition data includes parameters such as the voltage, current, frequency, power, power factor, energy, and various status states of the streetlight (on, off, dim level), along with various fault conditions such as lamp oscillating, ballast fail, lamp fail, and photocell fail. In the LG UI, individual street lights can be viewed; by clicking on any Street Light Controller (SLC) icon, the details of the street light can be viewed. Control data includes setting the lamp states manually or automatically through various scheduling methods. Control commands such as Read Data, Switch Off/On, Dim, Set Mode, and Get Mode can be sent to SLC.

Only authorized users of LightingGale can view the current Status, generate Reports, View Trends (graphical representation of various parameters), customize Dashboards for and monitor Alarms (intimation of Normal, Low or Critical conditions) of any site from any remote locations.

Refer to the CCI Implementation Guide for CIMCON LG operation details.


This section describes the system architecture and design specification for the CIMCON street light solution to achieve the functionality required for the CIMCON smart street lighting use cases.
The Cisco Connected Grid Router (CGR1240) is used as the FAR. The CSR1000v router is used as the HER. The network between the HER and the NOC, as well as between the HER and the Cloud CSR at the CIMCON LG, needs to be native IPv6 or IPv6 aware in order to support CR-Mesh communication. Communication between the FAR and HER is secured with an FlexVPN IPSec tunnel, which can pass through a private or public network. If needed, an IPv4 GRE tunnel is established on top of the FlexVPN IPSec tunnel to transport IPv6 packets to and from CIMCON streetlight controllers.

Communications between the HER and the CSR1000v router co-located with the CIMCON LG are protected by the FlexVPN IPSec site-to-site VPN.

During the pre-staging process, the RSA CA-signed RSA Certificates are provisioned in the FAR along with the FlexVPN config and FND address. Similarly, the SLCs are provisioned with ECC CA-signed certificates along with RF configuration information which includes the PAN ID, SSID, and Phy mode.

Software Upgrade

The software upgrade of the CIMCON-supplied SLC application stack is managed by the CIMCON LG application. Bulk upgrades can be performed and upgrade status can be monitored.

Software upgrade of the Cisco-supplied SLC communication stack is managed by the Cisco FND.

Beginning with release 4.6 of FND, over the air (OTA) updates of both the network stack and CIMCON application stack can be performed from the FDN interface. CIMCON firmware 2.0.17 with 3.0.37 application firmware is required on the SLC. The upgrade is pushed from FND and recognized by the SLC. The SLC performs a series of reboots that install the code at the proper times.

Refer to the CCI Implementation Guide for CIMCON LG operation details.

Template Management

CR-Mesh RF templates can be used to upload RF-related parameters to the Cisco Connected Grid Router (CGR) WPAN module and to the SLC communication stack. These templates are configured and distributed by the Cisco FND.

Smart Street Light Controller (SLC)

CIMCON Street Light Controllers (SLC) are CR-Mesh CGEs that control the lighting ballast. An SLC is a hardware device located on or in the luminaires to which data is transmitted and received. CIMCON SLC contains an CR-Mesh RF Module, which communicates with the CR-Mesh access network. SLCs are IP-enabled devices. They contain an IEEE 802.15.4g/e/v interface that consist of the communications module hardware and software. Every SLC is capable of forming and participating in an RF mesh.

CR-Mesh Access Network for CIMCON

Peak communication traffic requirement of CIMCON streetlight controllers and density of lighting nodes should be considered in the design of the access network. Cisco Connected Grid routers should be place in elevated areas that are either well connected or have access to a cellular network for backhaul and can provide the best coverage for the mesh network. Proper positioning is typically determined through an RF site survey. Multiple connected grid routers should be deployed in a region to maintain a high level of redundancy for the mesh backhaul. When combining streetlight communication traffic with other mesh services in the region (i.e. advanced metering) mesh traffic and out comes should be assessed. A typical street light deployment will have peak traffic time during sunrise and sunset or while performing firmware upgrades and management events.

SLCs act as forwarding nodes for 802.15.4 packets. Therefore, their default mode should be RPL non-storing mode.
CIMCON Smart Street Light over CCI CR-Mesh Access Network PoP

Figure 82 CCI Solution with CR-Mesh Access Network
CIMCON System Scale

The street lighting solution with CIMCON smart lighting has the following scaling parameters:

- Maximum number of concurrent tunnels with single CSR1000v: 1,000
- Maximum number of CR-Mesh endpoints with single CGR: 1000 non-redundant / 500 redundant
- Required bandwidth per SLC: 250bps, Required bandwidth per CGR: 125Kbps
- CGR has two one GigE uplinks Ethernet. In case of LTE uplink bandwidth up to 100Mbps downstream, 50Mbps upstream (depending on cellular carrier)

Cisco Kinetic for Cities (CKC)

CKC Smart Lighting operations include viewing the current status of lamps, controlling the switch on/switch off of the light, and dimming the light and is pre-integrated with the CIMCON Smart Street Lighting solution documented here.
Public Wi-Fi services with CCI Wi-Fi

Public Wi-Fi is where an outdoor Wi-Fi service can be provided public users, often at zero cost to the user, and potentially without registration. In the case of CCI this Wi-Fi service will be available outdoors across some or all of the metropolitan area that the CCI deployment covers; e.g. there may be many areas of Wi-Fi coverage, but perhaps just the ones in public parks, plazas and main shopping streets might be enabled for this public Wi-Fi service.

Municipality-wide SSID

A major advantage of a centrally managed Wi-Fi service with CCI, is that a consistent SSID can be beaconed through the municipality, so as a user of the public Wi-Fi service it is always the same Wi-Fi name I see on my device, e.g. “Townsville_FREE_Wi-Fi”. Other SSIDs could also be present (for example, one for municipality employees, one for Wi-Fi-connected sensors, etc.) but these are unlikely to be broadcast.

Captive Portal

A captive portal is used to manage user access to the public Wi-Fi service. A captive portal is an opportunity to:

- Get user acceptance of Terms & Conditions
- Prompt user for credentials
- Allow user registration
- Advertising to user
- All of the above

There are various options on the market for captive portals, however in the CCI CVD we recommend and have specifically tested DNA Spaces; see https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/DNA-Spaces/cisco-dna-spaces-config/dnaSpaces-configuration-guide/Working-with-Captive-Portal-App.html for more details about DNA Spaces’ captive portal capabilities.

In parallel to a captive portal, Open Roaming can be used to provide a more seamless Public Wi-Fi experience for the users; see https://blogs.cisco.com/networking/stay-connected-in-digital-spaces-with-openroaming for more details.

Traffic separated from rest of network

It is highly recommended that traffic associated with the Public Wi-Fi service is separated (segmented) from the rest of the CCI network. There is no need to have citizen/tourist etc. browsing traffic interact with other CCI network traffic, and indeed separating them greatly reduces the security exposure of having potentially a large number of untrusted and unknown devices and users on your network.

Public Wi-Fi traffic is typically given a lower priority than other traffic types (manifested as 802.11e WMM settings on the Wi-Fi infrastructure itself, upstream general IP QoS settings etc.) such that bandwidth will be limited on a per-client and overall service basis; e.g. 1Mbps is sufficient for general browsing and VoIP calls, but may be insufficient for consuming streaming video services and making video calls.

Traffic is tunneled over CAPWAP directly from the AP to the WLC, and from there typically on to a firewall towards the Public Internet.
Client Roaming

Because traffic is tunneled in CAPWAP, and anchored on one or more WLCs, and because a centralized captive portal is used for session management, the client roaming experience can be made as seamless as possible. Public Wi-Fi clients do L2 roams between APs, and their L3 IP address typically does not change throughout their session; whether the APs are within one PoP, or across PoPs.

Analytics and Insights

WLCs themselves, and DNA Center via its integration to and management of WLCs (in the case of SDA Wireless), or Prime Infrastructure (in the case of CUWN Mesh Wireless), can give a detailed picture of wireless networking health, traffic etc., over the short and longer-term. However DNA Spaces provides a richer and more detailed set of analytics and insights, plus (with the DNA Spaces Act licensing) specific APIs and SDKs allowing system integration.

Outdoor Wi-Fi as a sensor, with CCI Wi-Fi

Building on the Public Wi-Fi services above, per the Analytics and Insights, DNA Spaces can be used to turn an outdoor Wi-Fi deployment into a sensor.

Density and approximate location of Wi-Fi devices (be they associated or unassociated) can be inferred from the Wi-Fi infrastructure, and represented as a heat map, and/or exported via APIs and integrations.

This relies on accurate latitude and longitude information for the APs themselves, and in general the more APs the better in terms of painting an accurate picture.

Outdoor IP Camera with CCI Wi-Fi

The classic CCTV/Security camera is an important device for smart cities and roadways. With onboard or centralized video analytics capabilities, the video camera can become the ultimate sensor; typical use cases are:

<table>
<thead>
<tr>
<th>Deployment area</th>
<th>Use cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cities</td>
<td>General surveillance for public safety</td>
</tr>
<tr>
<td></td>
<td>People counting</td>
</tr>
<tr>
<td></td>
<td>Police and Security Body Cameras (with Wi-Fi connectivity and real-time uploading)</td>
</tr>
<tr>
<td>Roadways</td>
<td>General surveillance for traffic monitoring and public safety</td>
</tr>
<tr>
<td></td>
<td>Wrong-way driving detection</td>
</tr>
<tr>
<td></td>
<td>License-plate Recognition (LPR)</td>
</tr>
<tr>
<td></td>
<td>Vehicle counting and classification</td>
</tr>
</tbody>
</table>

Modern cameras are almost all natively IP-connected, and the camera typically exposes a web management interface, sockets for APIs and outbound it will send one or more video streams, as unicast or multicast; depending on the use case the streams may be low (1fps) to high (60fps) frame rate, and low (CIF) to high (4K) resolution (please see the Safety and Security Solution with CCI, page 169 section for more details), and this will create network demands ranging from 10s of kbps, up to 10Mbps.

CCI helps provide power for these cameras, and secure connectivity (incl. macro-segmentation), and scaling to thousands of cameras across a deployment.
The preferred method of providing CCTV camera connectivity is via a wired Ethernet and PoE connection to an IE switch in the CCI PoP. However where wired connectivity is not easily available, the CCI Wi-Fi infrastructure can be used to bridge high-bandwidth cost-free wireless connectivity to the CCTV camera via a WiFi AP virtual wired LAN extension.

Power

IP cameras can typically be powered via PoE, and outdoor cameras tend to need the higher end of the PoE capabilities, to get >30W in order to support heater elements in the cameras that allow them to operate outdoors even in cold environments. Some cameras (typically larger cameras, with comprehensive PTZ capabilities) require >=60W of power, or even >=110V AC power. For up to 30W PoE, the PoE capability of a Cisco Wi-Fi AP is a good option, because data and power is down a single cable, and it becomes easier to wire-up and commission such a camera; for >30W a separate power source will be required for the camera.

Connectivity

IP cameras will be Ethernet-connected, or Wi-Fi connected. CCI Wi-Fi can either provide connectivity for the cameras via a virtual wired LAN extension, or regular Wi-Fi client access if the camera is natively WiFi enabled.

Segmentation

This virtual LAN or SSID should then be mapped into the upstream network in a way that both segments the traffic in terms of separation and in terms of QoS. Depending on the use-case it may be more or less important that the video streams be kept isolated from other traffic in a CCI deployment, but in general the recommendation is that a separate VN be created for this purpose; similarly it is recommended to leverage CCI automated QoS capabilities to give the video streams the correct treatment. Note: not all IP traffic for the cameras needs to be treated equally; the video streams might get one QoS treatment, but the HTTPS administration traffic might get another.

Safety and Security Solution with CCI

Cisco’s Safety and Security real-time Video Analytics solution for empty and crowded scenes accelerates the response time to incidents and helps gain a better understanding of the traffic situation in a City. This addresses several use-cases including object and intrusion detection, perimeter protection and face recognition. Similar to the lighting solution described earlier, Safety and Security is a use case solution that can be supported on the CCI Network.

For a detailed design and implementation of the Cisco Safety and Security solution, please refer to the *Cisco Safety and Security Design and Implementation Guide* from the Cisco Industry Solution Design Zone.

Supervisory Control and Data Acquisition (SCADA) Networking over CCI

SCADA is a category of software application programs for process control and the gathering of data in real time or near real time from remote locations in order to control equipment and report conditions.

SCADA equipment is used in power plants, utilities, oil and gas, manufacturing, transportation, and water and waste control.

SCADA software repeatedly polls Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs) for data values of attached sensors, motors, and valves.

SCADA systems can help detect faults and provide alarm notification to operators for identifying and preventing defects at an early stage. Rising energy requirements have generated opportunities for greenfield expansions, while brownfield projects such as modernizing infrastructure offer lucrative opportunities for the SCADA market to grow. The use of fourth-generation technologies provides various benefits, such as faster navigation, improved alarm notification, and an increase in usability.
SCADA systems are transitioning to IoT systems (4th Generation SCADA System)

Modern SCADA systems are evolving from monolithic or isolated control points to highly networked communications systems with integrated distributed data services (DDS).

- **First Generation**: Monolithic or Isolated SCADA systems
  - Typically, in developing countries
  - Some percentage in developed countries (~30%)

- **Second Generation**: Distributed SCADA systems, Single Site (LAN)

- **Third Generation**: Networked SCADA systems, Multi Site (WAN)

- **Fourth Generation**: Internet of Things (IoT) technology SCADA systems

The Figure 84 below represents the evolution of SCADA systems over time.

### Figure 84  Evolution of SCADA System

**SCADA Components**

SCADA systems are made up of several components represented below.

- Primary Control System - Reports, Control DB, Real time or near real time data
- Communications Server - Gateway function, polls, controls, timeouts, recovery
- Remote terminal units (RTU) - Connected to the physical equipment and convert collected data to digital information
- Programmable logic controllers (PLC) - Connected to the physical equipment and convert collected data to digital information
- Human to machine interface (HMI) - Gives process data to the human operator
Validated Use Case Solutions

- Intelligent Electronic Device (IED)
- Supervisory computers – Communicates with PLCs, RTUs and presents to the HMI
- Communication infrastructure - Analog (T202, POTS) or digital (RS485, TCP/IP)

Depending on the generation or level of the deployment it may not include all of these items. As an example, the environment may be evolving from RTUs to PLCs or may exclusively have either RTUs or PLCs. An RTU/PLC may operate or perform a function in a remote location and not require a communications server or remote supervisory computers.

For the purpose of this document, it will cover the requirements and outcomes of an environment requiring a modern communication infrastructure but may maintain legacy components.

Primary SCADA functions

SCADA systems are designed to monitor and perform to prescribed outcomes. In many situations, if the SCADA system does not perform as expected it can cause severe system damage or in extreme cases loss of life.

Common SCADA functions are listed below:

- Alarm handling
- PLC (Plant) / RTU (Field) programming
- Timeouts / Polling Intervals
- Control
- Data Acquisition and Presentation
- Network Data Communication
- Recovery

Modern SCADA communication system

SCADA systems do not control the process in real time. They usually coordinate the process in real time. A common SCADA implementation communicates process status as alarm or normal operation along with process metrics. As communication systems supporting generation 3 and 4 SCADA systems become more reliable and redundant, poll rates are changing from what could be up to 15 minutes to sub-second.

SCADA systems can be deployed using a multitude of protocols. This document will cover three access methods, three deployment models across those three access methods and several protocols.

Following the CCI guidance above, SCADA devices could be connected at the access layer using Ethernet/Fiber, cellular, or across CR-Mesh. It is recommended that each access layer be deployed in accordance to CCI guidelines and appropriate redundancy models are in place. In this document we will not cover recovery time of the network in accomplishing our outcomes.

In each of the access methods above we support three communication types Native IP, Gateway encapsulation, and RAW Socket SCADA traffic.

- Native IP – Traffic that SCADA equipment itself sends as an IP packet. Sent from a SCADA device that has Ethernet interface on the device. Protocol conversion is completed inside the SCADA device prior to it being sent on the network.
- Gateway encapsulation – Traffic that is received at a mediary endpoint (Gateway) in its native protocol (DNP or Modbus) and converted or encapsulated at the gateway to an IP packet prior to be sent on the network to other SCADA systems.
- RAW Socket – transport streams of characters from one serial interface to another over an IP network.
The following protocols are supported over the access methods described above to set a base line of the capabilities of the CCI network when performing the communications network operations of a SCADA network.

- **Modbus RTU RS232 using Raw Socket** – Makes the use of a compact, binary representation of the data for protocol communication. RTU messages are transmitted continuously without inter-character hesitation. Application layer protocol.

- **Modbus TCP** - Variant of Modbus where the checksum is completed at lower layers


- **DNP3/IP** – DNP3 over a TCP/IP network

- **DNP3 RTU (Serial) to DNP3 IP using protocol translation**

The supported deployment models are displayed below:
Over all these configurations we provide guidance on how to maintain less than 150 millisecond response time for alarm messages and a less than 50 millisecond response time for control messages on the SCADA system.

The biggest impact to latency is the type of backhaul used to transmit the SCADA traffic regardless of its protocol or encapsulation type. The closer you can get to an end to end Ethernet deployment the better your flexibility in getting to real-time results.

Using wireless technologies are less deterministic. In our testing, we considered CR-Mesh and Cellular backhaul. This is further defined in the Distributed Automation Design and Implementation guides.


CR-Mesh Backhaul Design Considerations

Cisco’s IR510 Industrial Router can perform the mapping of address and port using translation (MAP-T) between IPv4 and IPv6. In a design where IPv4 endpoints are remotely connected using an IPv6 mesh network the IR510 Industrial Router would perform the MAP-T network translation required for end to end communication.

This section covers common design considerations, followed by capacity planning of the CR mesh for deployment of SCADA use cases. It also includes design guidance including considerations that impact the number of gateways that could be positioned in the CR mesh for these use cases, along with few mesh topology combinations.

It becomes vital to dissect and understand the application requirement and its exhibited traffic characteristics, to then figure out if CR mesh could cater to it. The first step is to understand the traffic profile of the application that is being considered for deployment on CR mesh. Additional guidance is available in the Distributed Automation Design Guide.
Validated Use Case Solutions

Listed below are common design considerations that should be considered when planning a SCADA deployment, in general, but become even more critical to understand in depth on a sub-gigahertz network (CR-Mesh):

- Understanding the packet profile of the application traffic, for example, SCADA application traffic profile.
- What subset of the packet profile are periodic? These would be exchanged even without any SCADA event.
- What subset of the packet profile are event driven that would be exchanged only when there is a SCADA event. Within CCI 2.0 that includes basic set and get functions across CR-Mesh.
- What is the latency requirement of the application? For CCI 2.0 we used Set times not to exceed 50 milliseconds from device to device (not including application latency) and 150 milliseconds to perform Get functions to read device settings.
- How many devices participated in the SCADA traffic profile that is under analysis?
- Are the devices connected via a hub and spoke or are they extended over a daisychain or tree topology? Depth of the daisychain and/or tree can impact the operation of set and get procedures and may limit the depth of topology deployments. In CCI 2.0, the tested limit depth of the CR-Mesh topology is four hops.
- Number of packets of varying size that are being transmitted (very small, small, medium, large packet sizes)
- Classification of the packets being transmitted (some may be periodic, some are event-driven).
- Frequency of packets being transmitted (Is it bandwidth intensive?).
- Area and the distance that needs to be aggregated (Urban vs Rural) by the CGR and CR mesh.
- Transport layer used for Application traffic (Choice of UDP vs TCP), with recommendation being UDP.
- DNP3 security if used, would increase the payload size.
- Average number of SCADA events per day.

Cellular Backhaul Design Considerations

This section covers common design considerations, followed by capacity planning of the cellular for deployment of SCADA use cases. It also includes design guidance including considerations that impact SCADA systems deployed with cellular backhaul to Cisco gateways supporting SCADA.

Listed below are common design considerations that should be considered when planning a SCADA deployment using Cellular backhaul:

- Bandwidth is generally shared between many users (such as smartphones, smart meters, and M2M) when attached to the same base station. This makes it difficult to design a network with guaranteed bandwidth, latency, and QoS parameters for meeting any performance-based criteria.
- Bandwidth is asymmetric since the services are designed to offer greater download speed to smartphone users. Conversely, SCADA traffic profiles have either symmetrical or greater upstream speed requirements, which requires evaluating the traffic load when designing the network. This means using a network protocol to understand the link capacity and potential costs (dependent on service subscription tariffs).
- Coverage and network availability must be evaluated for rural zones with isolated devices.
- Cellular deployments only offer native IPv4 services and if IPv6 connectivity is required, IPv6 traffic must be tunneled over GRE/IPv4.
FlashNet Lighting LoRaWAN solution over CCI

FlashNet, an Engie company, is a fast-paced tech company that integrates the latest IT, energy and telecommunications technologies into hardware and software solutions. FlashNet’s inteliLIGHT smart street lighting control system communication was tested from the street light controller to the FlashNet application server as part of ongoing LoRaWAN sensor testing within CCI. CCI 2.0 validated the data stream from the sensor to the FlashNet application layer using the established CCI LoRaWAN access network with Actiliiy network server for sensor onboarding and management.

CCI validated device onboarding and management over the LoRaWAN network as well as On/Off control of the street light controller from the applications server.

Figure 87  FlashNet inteliLight Light Management System

Water Monitoring Sensor Technologies

GreenStream LoRaWAN water level monitoring solution over CCI

GreenStream is an environmental technology firm. GreenStream flood sensors and water level sensors were tested as part of ongoing LoRaWAN sensor testing within CCI. CCI 2.0 validated the data stream from the sensor to the GreenStream application layer using the established CCI LoRaWAN access network with Actiliiy network server for sensor onboarding and management.

CCI validated device onboarding and management over the LoRaWAN network as well as data collection on water depth, battery power, and signal strength.

Below is a sample screen shot of data from a GreenStream sensor.
Danalto LoRaWAN water level monitoring solution over CCI

Danalto delivers flexible, scalable IoT solutions and technologies which release the potential of low power sensing. GullySpy helps water operators manage their flood risk. GullySpy has been specifically designed to provide insight and early warning indications of flood risks. It monitors when the water level of a drain system exceeds capacity. Through analytics combining rain levels and sensor data to determine the length of time it takes for water levels to return to normal level. This insight allows operators to prioritize field engineer time to clear slow draining water ways or in making future investments. GullySpy has been validated over the CCI architecture on the LoRaWAN access network.

https://www.danalto.com/flood-gullyspy/

Axis Camera Onboarding and Integration over CCI

Axis Communications offers a wide portfolio of IP-based products for security and video surveillance. Axis network cameras integrates easily and securely with CCI to build a complete security, video surveillance and video analytics based use case solution in CCI.

This section covers Axis network cameras secure onboarding and integration use case in CCI using open industry standards (Eg., IEEE 802.1X) in CCI PoP and RPoP sites. Field engineers need to install and maintain infrastructure along the City streets or roadways. The camera has to be installed and maintained by field technicians in a quick and efficient manner. It is important to apply policy for segmentation and security consistently across the network while ensure seamless endpoint’s connectivity and availability in CCI. The aim of section is provide the best-practice to enable simplified deployment of Axis cameras on the CCI network, while automatically ensuring the best possible security posture with network segmentation and zero-trust, authenticated-only access to the CCI network.

Axis Components in CCI

The following Axis components are added to the CCI network for initial field deployment (Day 0 provisioning) and ongoing management of the cameras (Day N management) in a CCI Safety and Security Virtual Network to send video streams to a Video Management Server (VMS).
Validated Use Case Solutions

- **Axis Device Manager (ADM)** - an on-premise tool that delivers an easy, cost-effective and secure way to perform device management. It offers security installers and system administrators a highly effective tool to manage all major installation, security and maintenance tasks. It is compatible with the majority of Axis network cameras, access control and audio devices.

- **Axis Network Cameras** - robust outdoor cameras that provide excellent High-Definition (HD) image quality regardless of lighting conditions and the size and characteristics of the monitored areas.

Refer to the following URLs for more details on Axis Device Manager and Network Cameras:


**Axis Camera Onboarding in CCI**

Axis network cameras that provide video surveillance and analytics connect to CCI Ethernet Access ring (IE switches) in a PoP site or a remote gateway (IR1101) in RPoP. Secure onboarding, profiling and applying network policies for the cameras in CCI requires that the cameras to be staged for initial discovery in the network, followed by provisioning industry standard X.509 certificates (using PKI) on the cameras. The aim of the capability described here is to enable the ‘staging’ for initial discovery to be done automatically, in the field by the field technician, using a standard unconfigured or new Axis camera (i.e. no off-line / off-network staging required)

The camera onboarding or staging process is divided into the following two steps, both of which can be completed in the field (i.e. at the final camera location) by the field technician:

- **Axis cameras discovery and device profiling in the network.**
- **Provisioning cameras with X.509 certificates and enabling IEEE 802.1X authentication and authorization in the network.**

**Axis Camera discovery and profiling**

Endpoints or hosts that connect to IE switches access ports or RPoP gateway (IR1101) in CCI are authenticated and authorized for network access by Cisco ISE in the shared services network. Endpoints or hosts that are initially connecting to CCI are quarantined in the network (as untrusted devices) using a VLAN or subnet in a CCI fabric overlay, the Quarantine VN. The endpoints or hosts that support 802.1X become trusted devices in the network after their successful 802.1X authentication with ISE by presenting its device identities like user/password or X.509 certificates.

The cameras in the quarantine network in the CCI PoP or RPoP are discovered using ADM. In order to discover the cameras from ADM, the cameras and ADM require IP reachability in the quarantine network. Axis cameras that connect to IE switch port or IR1101 FE port (on non-PoE port and the camera powered through PoE injector) are initially authenticated using the MAC Authentication Bypass (MAB) method and the switch port is assigned a quarantine network VLAN by ISE. The cameras are profiled by ISE using a built-in Cisco provided “Axis-Device” profile available in ISE.

The following pre-requisite configurations are required in CCI for Axis cameras onboarding and initial discovery in the network:

- Install and Configure ADM application in CCI Shared Services network (for Day 0 provisioning and Day N management of cameras) in a separate VLAN or subnet with access to quarantine network.
- Ensure a separate Quarantine VN is created for untrusted hosts in the CCI network and subnets in Quarantine VN are created for cameras in each PoP.
- Ensure a centralized DHCP server is configured in quarantine network for providing IP addresses to cameras in the quarantine network. This is required for initial discovery of cameras in ADM.
- Ensure ADM is network access permitted to access quarantine network for Day 0 provisioning of the cameras.
Cisco ISE is configured with appropriate 802.1X and MAB authentication and authorization policies for the cameras in different sites.

Note: The ADM application can also be connected to an IE switch port in the PoP access ring where cameras are connected for initial discovery and provisioning of cameras (Day 0 provisioning) in a PoP site. In this case, another ADM application could be configured in either Shared Services network or Camera VN network (Eg., SnS_VN) for Day N management of the Axis cameras in CCI.

Figure 89 illustrates the Day 0 provisioning of Axis Cameras for initial discovery and onboarding steps in CCI.

In Figure 89:

1. Axis Camera in a CCI PoP or a RPoP plugged in to 802.1X and MAB enabled Ethernet access port of an IE switch in the access ring or FE port in RPoP IR1101 gateway.

2. IE switch or IR1101 receives MAC address of the camera from the initial packets sent by the camera to the switch (MAC learning process) and initiates MAB authentication with Cisco ISE as AAA or RADIUS authentication server.

3. Cisco ISE verifies the device profile and authenticates the camera using MAB method. The device profile “Axis-Device” is built-in the Cisco ISE application.

Note: Axis camera connected to RPoP IR1101 FE port requires a power recycle to initiate MAB during initial onboarding since the camera is connected to a non PoE port and powered through an external power injector.

4. After successful MAB authentication of the camera, ISE assigns a VLAN in quarantine network to the Ethernet port using an authorization profile. This is sent to switch as RADIUS protocol Attribute and Value Pair (AVP) message. The authorization profile in ISE matches a specific authentication condition and assigns a result profile configured in ISE.

5. Axis Camera sends DHCP messages to request for a new IP address in quarantine VLAN.

Note: There is limited access between the quarantine VLAN and the rest of the network.
6. DHCP server in quarantine network allocates IP address to the camera and the camera receives the IP address for its request.

7. Once IP address is assigned to the camera, ADM can discover the camera in the network using Universal Plug-and-Play (UPnP) protocol. UPnP protocol is by default enabled on Axis cameras for network discovery by ADM. UPnP in turn uses Simple Service Discovery Protocol (SSDP) to discover the cameras in the network. ADM searches for the camera(s) using a specific IP address or a subnet or a range of IP addresses in a subnet.

Figure 90 depicts a sequence of messages flow for Axis Camera onboarding in a CCI PoP.

Figure 90  Axis Cameras Onboarding Messages Flow Diagram

Note: In case of an Axis camera connected to RPoP IR1101, the IR1101 will act as an authenticator sending RADIUS authentication requests to Cisco ISE in the above flow instead of an IE switch in a CCI PoP.

Provisioning cameras with X.509 certificates and enabling IEEE 802.1X

Axis cameras support IEEE 802.1X open standard based device authentication with a RADIUS and policy server. Axis Cameras support X.509 certificates for device identity. An X.509 is a digital certificate that uses a widely accepted X.509 Public Key Infrastructure (PKI) standard to verify that a public key belongs to a user, host (computer) or endpoint identity within the certificate.

Once a camera is successfully onboarded in the CCI network, the next step is to authenticate and authorize the camera for the correct VN access. Cameras in CCI are required to have access to a vertical service VN (Eg., Safety and Security VN or simply SnS_VN) to stream live video feeds to a VMS system in the VN for video surveillance and other video analytics–based use cases in CCI. This is achieved using 802.1X authentication and followed by authorization of cameras using Cisco ISE.
Axis cameras use IEEE 802.1X Extensible Authentication Protocol over LAN (EAPoL) as an authentication method to authenticate with Cisco ISE as a RADIUS authentication and Network Policy Server (NPS). There are many EAP methods available to gain access to a network. The protocol used by Axis is EAP-TLS (EAP-Transport Layer Security) for wired and wireless 802.1X authentication.

Using EAP-TLS, to gain access to a network, the Axis device must have a Certificate Authority (CA) certificate, a client certificate and a client private key. They should be created by servers and uploaded via ADM to all the Axis cameras in the network. When the Axis device is connected to the network switch, the device will present its certificate to the switch. If the certificate is approved, the switch allows the device access to the trusted SnS VN.

ADM can also be used as a Root-CA server to provide certificates. In order to successfully authenticate Axis cameras in CCI using 802.1X, the following pre-requisite PKI configuration is required to provide necessary certificates needed for the authentication.

- Configure ADM in quarantine network as Root-CA server to provide client certificates to Axis Cameras and Cisco ISE as the RADIUS server in CCI.
- Install ADM Root CA certificate chain in Cisco ISE trusted certificate store.
- Configure ISE certificate as authentication server certificate in ADM.
- Centralized DHCP server in Shared Services network is configured with DHCP scope options in a respective vertical service VN (Eg., SnS_VN) for the cameras.

Refer to the following URL for more details on IEEE 802.1X in Axis products:


**Figure 91** shows the Axis Cameras 802.1X authentication steps in a CCI PoP or RPoP.
Figure 91  Axis Cameras 802.1X Authentication in CCI

In Figure 91:

1. Once ADM discovers all the cameras in the quarantine network, the ADM install Root-CA, client and authentication server certificates configured in ADM on all the cameras. Note that, ADM generates unique client certificate for each of the cameras in the network which are installed on the camera during the certificate installation step in ADM. ADM enables 802.1X on all the cameras and restarts the cameras.

2. The cameras (802.1X supplicants) initiate the 802.1X process by sending EAPoL start message to IE switch (in CCI PoP) or IR1101 (in RPoP).

3. IE switch or IR1101 (authenticators) sends RADIUS protocol access request message to ISE and also request the device identity from the cameras using EAPoL Request-Identity message.

4. ISE as 802.1X authentication server verifies client and ADM certificates by sending RADIUS messages (a sequence of RADIUS messages explained as a flow diagram in Figure 84). Upon successful verification of certificates, the ISE authorizes the cameras and assigns a VLAN (Eg., a subnet in SnS VN) configured in an authorization profile in ISE.

Note: If the 802.1X authentication fails, the MAB authentication will trigger as fallback authentication method and the camera will be authorized to access only the quarantine network.

5. The cameras send DHCP messages in the VLAN (SnS VN) and a centralized DHCP server in shared services network receives DHCP requests and allocates IP addresses to cameras in the respective VLAN DHCP scope.

6. The cameras receive IP addresses allocated by DHCP server and assigned with IP address in the respective VLAN for network access. Once, cameras are assigned with IP addresses they can communicate with all devices in the respective VN (Eg., SnS VN). This completes the Axis Cameras onboarding use case in CCI.
Note: ADM in shared services network must re-discover all the cameras using new IP address or range of IP addresses of the cameras for the Day N management of the cameras using ADM. Alternatively, the ADM which can also be placed in the respective vertical service VN in CCI (Eg., SnS_VN) along with a VMS system, can discover the cameras for Day N management.

Figure 92 lists a sequence of Axis Cameras 802.1X authentication messages and DHCP messages flow in the CCI network.

Figure 92  Axis Cameras 802.1X Authentication Messages Flow Diagram

Note: In case of an Axis camera connected to RPoP IR1101, the R1101 will act as an authenticator sending RADIUS authentication requests to Cisco ISE in the above flow instead of an IE switch in a CCI PoP.

Conclusions

Digital transformation for cities, communities, and roadways form the basis for future sustainability, economic strength, operational efficiency, improved livability, public safety, and general appeal for new investment and talent. Yet these efforts can be complex and challenging. Cisco Connected Communities Infrastructure is the answer to this objective and is designed with these challenges in mind.

In summary, this Cisco Connected Community Infrastructure (CCI) solution Design Guide provides an end-to-end secured access and backbone for cities, communities, and roadway applications. The design is based on Cisco’s Intent-based Networking platform: the Cisco DNA Center. Multiple access technologies and backbone WAN options are supported by the design. The solution is offered as a secure, modular architecture enabling incremental growth of applications and network size, making the solution cost effective, secure, and scalable. Overall, the design of CCI solution is generic in nature, enabling new applications to be added with ease. Apart from the generic CCI solution design, this document also covers detailed design for the Smart Lighting solution, Safety and Security solution, and frameworks for Public and Outdoor Wi-Fi, LoRaWAN, and DSRC-based solutions.

“Every smart city starts with its network. I want to move away from isolated solutions to a single multi-service architecture approach that supports all the goals and outcomes we want for our city.”

- Gary McCarthy Mayor, City of Schenectady, NY
Acronyms and Initialisms

The following table summarizes all acronyms and initialisms used in the *Cisco Connected Communities Infrastructure Solution Design Guide*:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AB</td>
<td>Anywhere Border</td>
</tr>
<tr>
<td>ADR</td>
<td>Adaptive Data Rate</td>
</tr>
<tr>
<td>AMP</td>
<td>Advanced Malware Protection</td>
</tr>
<tr>
<td>AVC</td>
<td>Application Visibility &amp; Control</td>
</tr>
<tr>
<td>BGP</td>
<td>Border Gateway Protocol</td>
</tr>
<tr>
<td>BN</td>
<td>Border Node</td>
</tr>
<tr>
<td>BSM</td>
<td>Basic Safety Message</td>
</tr>
<tr>
<td>BSW</td>
<td>Blind Spot Warning</td>
</tr>
<tr>
<td>BW</td>
<td>Bandwidth</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
</tr>
<tr>
<td>CCI</td>
<td>Cisco Connected Communities Infrastructure</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed Circuit Television</td>
</tr>
<tr>
<td>CDN</td>
<td>Cisco Developer Network</td>
</tr>
<tr>
<td>CGE</td>
<td>Connected Grid Endpoint</td>
</tr>
<tr>
<td>CGR</td>
<td>Connected Grid Router</td>
</tr>
<tr>
<td>Cisco DNA Center</td>
<td>Cisco Digital Network Architecture Center</td>
</tr>
<tr>
<td>CKC</td>
<td>Cisco Kinetic for Cities</td>
</tr>
<tr>
<td>CLB</td>
<td>Cluster Load Balancing</td>
</tr>
<tr>
<td>CPNR</td>
<td>Cisco Prime Network Registrar</td>
</tr>
<tr>
<td>CR-Mesh</td>
<td>Cisco Resilient Mesh</td>
</tr>
<tr>
<td>CSMP</td>
<td>CoAP Simple Management Protocol</td>
</tr>
<tr>
<td>CSR</td>
<td>Common Safety Request</td>
</tr>
<tr>
<td>CSW</td>
<td>Curve Speed Warning</td>
</tr>
<tr>
<td>CTS</td>
<td>Cisco TrustSec</td>
</tr>
<tr>
<td>CVD</td>
<td>Cisco Validated Design</td>
</tr>
<tr>
<td>DAD</td>
<td>Dual Active Detection</td>
</tr>
<tr>
<td>DAO</td>
<td>Destination Advertisement Object</td>
</tr>
<tr>
<td>DC</td>
<td>Data Center</td>
</tr>
<tr>
<td>DCE</td>
<td>Data Communications Equipment</td>
</tr>
<tr>
<td>DC-EN</td>
<td>Daisy-Chained Extended Node</td>
</tr>
<tr>
<td>DC-PEN</td>
<td>Daisy-Chained Policy Extended Node</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DMZ</td>
<td>De-militarized Zone</td>
</tr>
<tr>
<td>DNPW</td>
<td>Do Not Pass Warning</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>DODAG</td>
<td>Destination Oriented Directed Acrylic Graph</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------</td>
<td>----------------------------------------------------------------</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>DSRC</td>
<td>Dedicated Short-Range Communications</td>
</tr>
<tr>
<td>EB</td>
<td>Enhanced Beacon</td>
</tr>
<tr>
<td>EB</td>
<td>External Border</td>
</tr>
<tr>
<td>ECC</td>
<td>Elliptic Curve Cryptography</td>
</tr>
<tr>
<td>ECMP</td>
<td>Equal-Cost Multi Path</td>
</tr>
<tr>
<td>EEBL</td>
<td>Emergency Electronic Brake Lights</td>
</tr>
<tr>
<td>EID</td>
<td>End Point Identifier</td>
</tr>
<tr>
<td>EIGRP</td>
<td>Enhanced Interior Gateway Routing Protocol</td>
</tr>
<tr>
<td>EN</td>
<td>extended nodes</td>
</tr>
<tr>
<td>EPs</td>
<td>Endpoints</td>
</tr>
<tr>
<td>ETS</td>
<td>European Teletoll Services</td>
</tr>
<tr>
<td>ETSI</td>
<td>European Telecommunications Standards Institute</td>
</tr>
<tr>
<td>EVA</td>
<td>Emergency Vehicle Alert</td>
</tr>
<tr>
<td>FAR</td>
<td>Field Area Routers</td>
</tr>
<tr>
<td>FC</td>
<td>Fiber Channel</td>
</tr>
<tr>
<td>FCAPS</td>
<td>enhanced fault, configuration, accounting, performance, and security</td>
</tr>
<tr>
<td>FCC</td>
<td>Federal Communications Commission</td>
</tr>
<tr>
<td>FCoE</td>
<td>Fiber Channel over Ethernet</td>
</tr>
<tr>
<td>FCW</td>
<td>Forward Collision Warning</td>
</tr>
<tr>
<td>FE</td>
<td>Fabric Edges</td>
</tr>
<tr>
<td>FI</td>
<td>Fabric Interconnects</td>
</tr>
<tr>
<td>FiaB</td>
<td>Fabric in a Box</td>
</tr>
<tr>
<td>FND</td>
<td>Cisco Field Network Director</td>
</tr>
<tr>
<td>FNF</td>
<td>Flexible NetFlow</td>
</tr>
<tr>
<td>FP</td>
<td>FirePower</td>
</tr>
<tr>
<td>FW</td>
<td>Firewall</td>
</tr>
<tr>
<td>HER</td>
<td>headend router</td>
</tr>
<tr>
<td>HSRP</td>
<td>Hot Standby Router Protocol</td>
</tr>
<tr>
<td>HQ</td>
<td>Headquarter</td>
</tr>
<tr>
<td>HTDB</td>
<td>Host Tracking Database</td>
</tr>
<tr>
<td>IB</td>
<td>Internal Border</td>
</tr>
<tr>
<td>ICA</td>
<td>Intersection Collision Avoidance</td>
</tr>
<tr>
<td>IE</td>
<td>Industrial Ethernet</td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange</td>
</tr>
<tr>
<td>IMA</td>
<td>Intersection Movement Assist</td>
</tr>
<tr>
<td>IPAM</td>
<td>IP Address Management</td>
</tr>
<tr>
<td>iSCSI</td>
<td>Internet Small Computer Systems Interface</td>
</tr>
<tr>
<td>ISE</td>
<td>Identity Services Engine</td>
</tr>
<tr>
<td>LER</td>
<td>Label Edge Router</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>L2TP</td>
<td>Layer 2 Tunneling Protocol</td>
</tr>
<tr>
<td>LG</td>
<td>Cimcon LightingGale</td>
</tr>
<tr>
<td>LLG</td>
<td>Least Loaded Gateway</td>
</tr>
<tr>
<td>LoRa</td>
<td>Long Range</td>
</tr>
<tr>
<td>LoRaWAN</td>
<td>Long Range WAN</td>
</tr>
<tr>
<td>LSP</td>
<td>Label Switched Path</td>
</tr>
<tr>
<td>LSR</td>
<td>Label Switched Router</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>MAN</td>
<td>Metropolitan Area Network</td>
</tr>
<tr>
<td>ME</td>
<td>Mesh End</td>
</tr>
<tr>
<td>MIC</td>
<td>Message Integrity Code</td>
</tr>
<tr>
<td>MNT</td>
<td>Monitoring Node</td>
</tr>
<tr>
<td>MP</td>
<td>Mesh Point</td>
</tr>
<tr>
<td>MUD</td>
<td>Manufacture Usage Description</td>
</tr>
<tr>
<td>NAN</td>
<td>Neighborhood Area Network</td>
</tr>
<tr>
<td>NAT</td>
<td>network address translation</td>
</tr>
<tr>
<td>NBAR2</td>
<td>Cisco Next Generation Network-Based Application Recognition</td>
</tr>
<tr>
<td>NGFW</td>
<td>Next General Firewall</td>
</tr>
<tr>
<td>NGIPS</td>
<td>Next-Generation Intrusion Prevention System</td>
</tr>
<tr>
<td>NOC</td>
<td>Network Operation Center</td>
</tr>
<tr>
<td>NSF/SSO</td>
<td>Non-Stop Forwarding with Stateful Switchover</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>OAM</td>
<td>Operations, Administration, and Management</td>
</tr>
<tr>
<td>OBU</td>
<td>On-board Unit</td>
</tr>
<tr>
<td>OSPF</td>
<td>Open Shortest Path First</td>
</tr>
<tr>
<td>OTAA</td>
<td>Over the Air Activation</td>
</tr>
<tr>
<td>PAN</td>
<td>Policy Administration Node; Personal Area Networks</td>
</tr>
<tr>
<td>PAgP</td>
<td>Port Aggregated Protocol</td>
</tr>
<tr>
<td>PCA</td>
<td>Pedestrian Crossing Assist</td>
</tr>
<tr>
<td>PEN</td>
<td>Policy Extended Node</td>
</tr>
<tr>
<td>PEP</td>
<td>Policy Enforcement Point</td>
</tr>
<tr>
<td>PIM-ASM</td>
<td>Protocol Independent Multicast – Any Source Multicast</td>
</tr>
<tr>
<td>PIM-SSM</td>
<td>Protocol Independent Multicast – Source Specific Multicast</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>PLC</td>
<td>Power Line Communication</td>
</tr>
<tr>
<td>PnP</td>
<td>Plug and Play</td>
</tr>
<tr>
<td>PoP</td>
<td>Point of Presence</td>
</tr>
<tr>
<td>PQ</td>
<td>Priority Queuing</td>
</tr>
<tr>
<td>PSM</td>
<td>Personal Safety Message</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------</td>
</tr>
<tr>
<td>PSN</td>
<td>Policy Services Node</td>
</tr>
<tr>
<td>PVD</td>
<td>Probe Vehicle Data</td>
</tr>
<tr>
<td>PVM</td>
<td>Probe Vehicle Management</td>
</tr>
<tr>
<td>PXG</td>
<td>Platform Exchange Grid Node</td>
</tr>
<tr>
<td>pxGrid</td>
<td>Platform eXchange Grid</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial-In User Service</td>
</tr>
<tr>
<td>REP</td>
<td>Resilient Ethernet Protocol</td>
</tr>
<tr>
<td>RLOC</td>
<td>Routing Locator</td>
</tr>
<tr>
<td>RLVW</td>
<td>Red Light Violation Warning</td>
</tr>
<tr>
<td>RPL</td>
<td>Routing Protocol for Low-Power and Lossy Networks</td>
</tr>
<tr>
<td>RPoPs</td>
<td>Remote Points-of-Presence</td>
</tr>
<tr>
<td>RSA</td>
<td>Roadside Alert</td>
</tr>
<tr>
<td>RSU</td>
<td>Roadside Unit</td>
</tr>
<tr>
<td>RSZW</td>
<td>Reduce Speed/Work Zone Warning</td>
</tr>
<tr>
<td>RTA</td>
<td>Right Turn Assist</td>
</tr>
<tr>
<td>SCMS</td>
<td>Security Credential Management System</td>
</tr>
<tr>
<td>SD-Access</td>
<td>Software-defined Access</td>
</tr>
<tr>
<td>SFC</td>
<td>Stealthwatch Flow Collector</td>
</tr>
<tr>
<td>SGTs</td>
<td>Security Group Tags</td>
</tr>
<tr>
<td>SGACL</td>
<td>Security Group-based Access Control List</td>
</tr>
<tr>
<td>SLC</td>
<td>Street Light Controller</td>
</tr>
<tr>
<td>SMC</td>
<td>StealthWatch Management Console</td>
</tr>
<tr>
<td>SPAT</td>
<td>Signal Phase and Timing Message</td>
</tr>
<tr>
<td>SRM</td>
<td>Signal Request Message</td>
</tr>
<tr>
<td>SSID</td>
<td>Service Set Identifier</td>
</tr>
<tr>
<td>SSM</td>
<td>Software Security Module</td>
</tr>
<tr>
<td>SVL</td>
<td>StackWise Virtual Link</td>
</tr>
<tr>
<td>SXP</td>
<td>SGT eXchange Protocol</td>
</tr>
<tr>
<td>TC</td>
<td>Transit Control</td>
</tr>
<tr>
<td>TFTP</td>
<td>Trivial File Transfer Protocol</td>
</tr>
<tr>
<td>TIM</td>
<td>Traveler Information Message</td>
</tr>
<tr>
<td>TMC</td>
<td>Traffic Monitoring Center</td>
</tr>
<tr>
<td>TPE</td>
<td>ThingPark Enterprise</td>
</tr>
<tr>
<td>UCS</td>
<td>Cisco Unified Computing System</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>UPS</td>
<td>Uninterrupted Power Supply</td>
</tr>
<tr>
<td>V2I</td>
<td>Vehicle to Infrastructure</td>
</tr>
<tr>
<td>V2P</td>
<td>Vehicle to Pedestrian</td>
</tr>
<tr>
<td>V2V</td>
<td>Vehicle to Vehicle</td>
</tr>
<tr>
<td>V2X</td>
<td>Vehicle-to-Infrastructure</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>--------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>VN</td>
<td>virtualized network</td>
</tr>
<tr>
<td>VNI</td>
<td>VXLAN Network Identifier</td>
</tr>
<tr>
<td>VoD</td>
<td>Video-on-Demand</td>
</tr>
<tr>
<td>VRF</td>
<td>virtual routing and forwarding</td>
</tr>
<tr>
<td>VSM</td>
<td>Video Surveillance Manager</td>
</tr>
<tr>
<td>VXLAN</td>
<td>Virtual Extensible LAN</td>
</tr>
<tr>
<td>WAVE</td>
<td>Wireless Access in Vehicular Networking</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>Wireless Fidelity</td>
</tr>
<tr>
<td>WLC</td>
<td>Wireless LAN Controller</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
<tr>
<td>WPAN</td>
<td>Wireless Personal Area Network</td>
</tr>
<tr>
<td>WRED</td>
<td>Weighted Random Early Detect</td>
</tr>
<tr>
<td>WSMP</td>
<td>WAVE Short Message Protocol</td>
</tr>
<tr>
<td>ZTD</td>
<td>Zero Touch Deployment</td>
</tr>
<tr>
<td>ZTP</td>
<td>Zero Touch Provisioning</td>
</tr>
</tbody>
</table>