Connected Communities Infrastructure – Cities Solution

Design Guide

November 2021

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Contents

Connected Communities Infrastructure – Cities Solution

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. This Cisco Connected Communities Infrastructure Smart Cities Solution discusses the validated design for various Smart Cities use cases on Connected Communities Infrastructure Solution discussed in a separate design guide. This document should be used with general CCI design guide for the design and deployment of various smart cities use cases discussed in this document.

References

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

- Cisco Connected Communities Infrastructure: https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-industry-solutions/iot-connected-communities-infrastructure.html
- 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.

CCI Validated Use Case Solutions

Cisco Connected Communities Infrastructure (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.

Figure 1 CCI Use Cases

An example is a city/municipality that is deploying a network to cover connected street lighting, smart parking, public Wi-Fi, CCTV cameras and intelligent intersections. All of these have different access, security, and QoS requirements, and may be owned by different departments. CCI can provide a single architecture, based on a common infrastructure, to support these various capabilities.

Validated Cities Use Case Solutions

This chapter discusses the various Smart Cities Use Case Solutions that are validated in CCI.

This chapter includes the following major topics:

Connected Street Lighting

CR-Mesh Connected Street Lighting

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.”

Refer to the following chapters in the CCI General Solution Design Guide for the detailed design on Connected Street Lighting network infrastructure:

- Solution Architecture
- Switched Ethernet Access Networks
- CR-Mesh in Wireless IoT Device Networks
- CCI Remote Sites (RPoPs)C

Public Cloud

As tested in CCI, applications such as 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 is secured by https. Refer to Figure 2 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.

CR-Mesh Access Network Solution Message Flow Architecture

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.

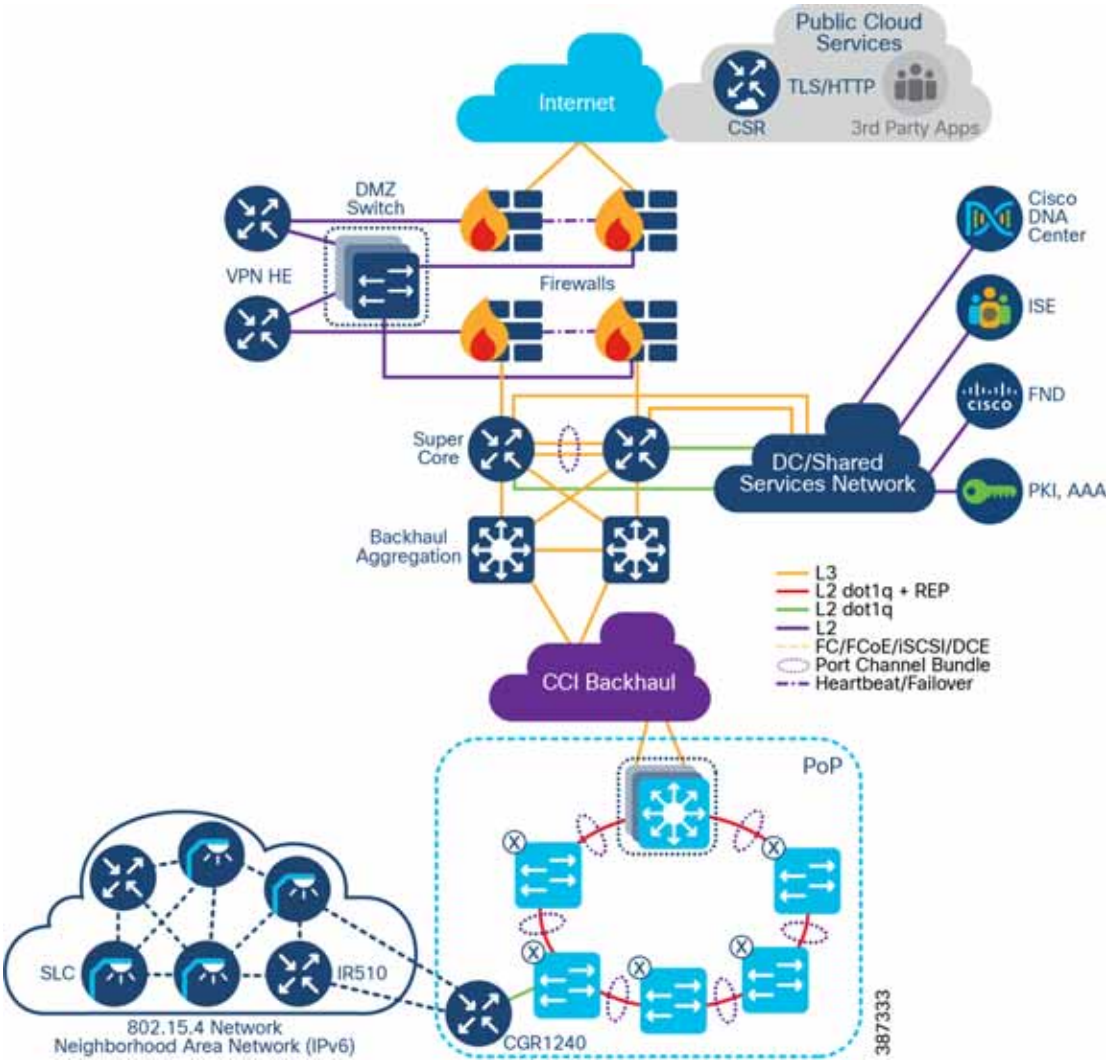
CR-Mesh Access Network for CIMCON

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 placed 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.

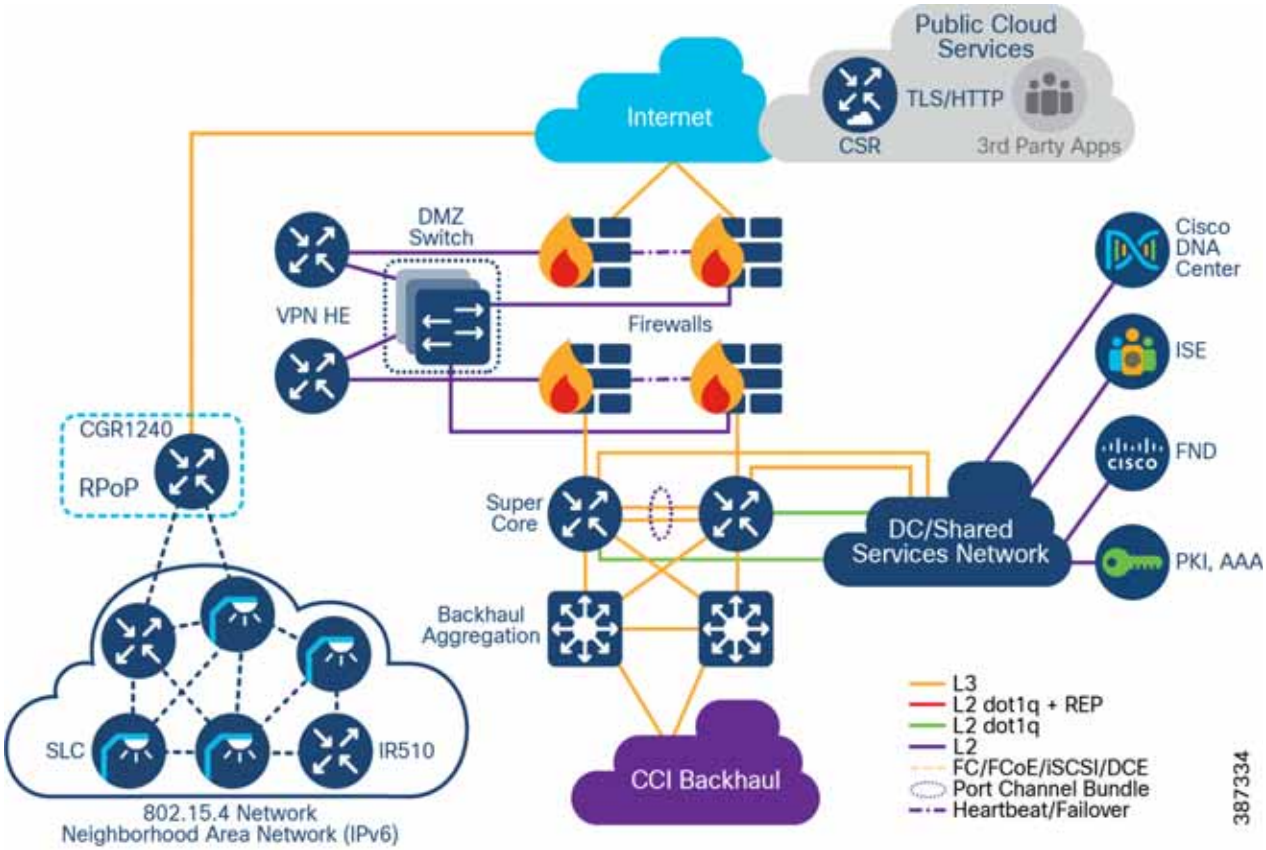
CIMCON Smart Street Light over CCI CR-Mesh Access Network PoP

Figure 2 CCI Solution with CR-Mesh Access Network



CIMCON Smart Street Light over CCI CR-Mesh Access Network RPoP

Figure 3 CCI Solution with CR-Mesh Access Network with RPoP



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 in the WAN/backhaul: 125Kbps
- CGR has two one GigE uplinks Ethernet. In case of LTE uplink bandwidth up to 100Mbps downstream, 50Mbps upstream (depending on cellular carrier)

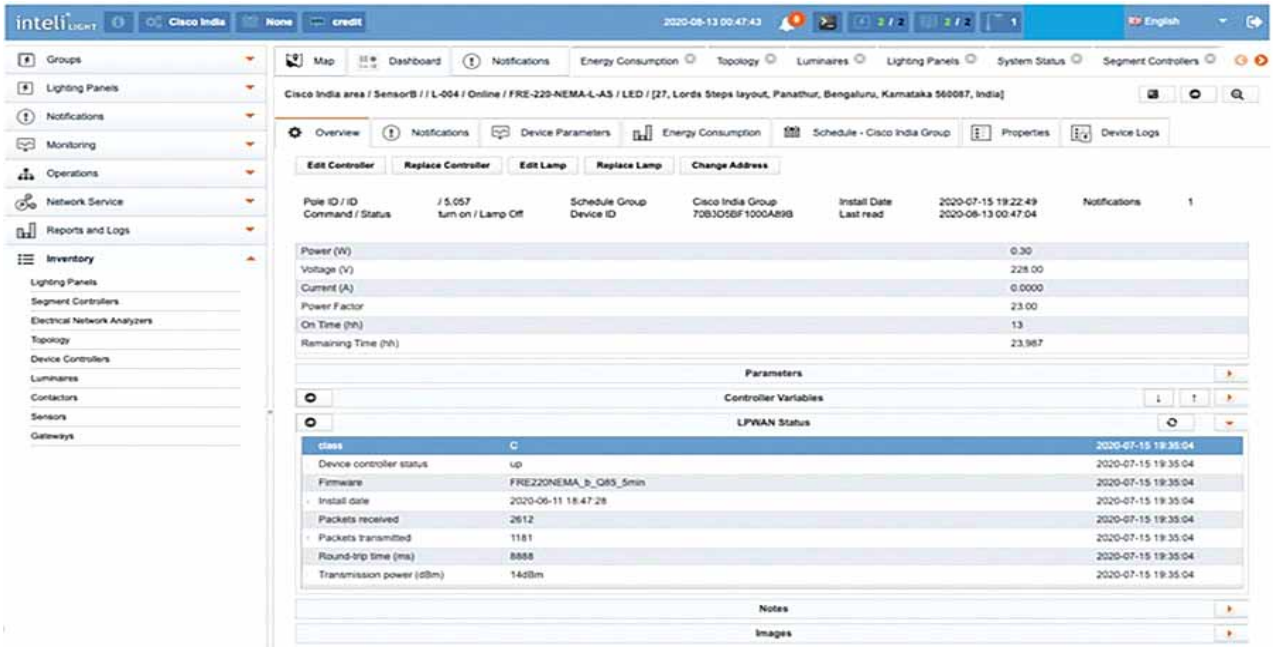
LoRaWAN Connected Street Lighting

FlashNet Lighting LoRaWAN solution over CCI

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 2.1 validated the data stream from the sensor to the FlashNet application layer using the established CCI LoRaWAN access network with Actiliy 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 4 FlashNet inteliLIGHT Light Management System



Connected Safety and Security Solution

Keeping cities and citizens safe is critical. Safe cities attract the investments, businesses, and skilled labor necessary for economic growth and development. Our solution helps protect cities against crime, terrorism, and civil unrest, enabling government agencies to respond to emergencies and safeguard citizens. This section discusses the Cities Video Surveillance CCTV Camera use cases that can be deployed on CCI. Similar to the lighting solution described earlier, Video Surveillance is a use case solution that can be supported on the CCI Network.

Refer to the following chapters in the CCI General design guide for the detailed design on Connected Safety and Security network architecture:

- Solution Architecture
- Switched Ethernet Access Networks
- CCI Remote Sites (RPoPs)

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 (for example, 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 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 streamsto a Video Management Server (VMS).

- 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:

- https://www.axis.com/en-in/products/axis-device-manager/
- https://www.axis.com/en-in/products/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. 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 prerequisite configurations are required in CCI for Axis cameras onboarding and initial discovery in the network:

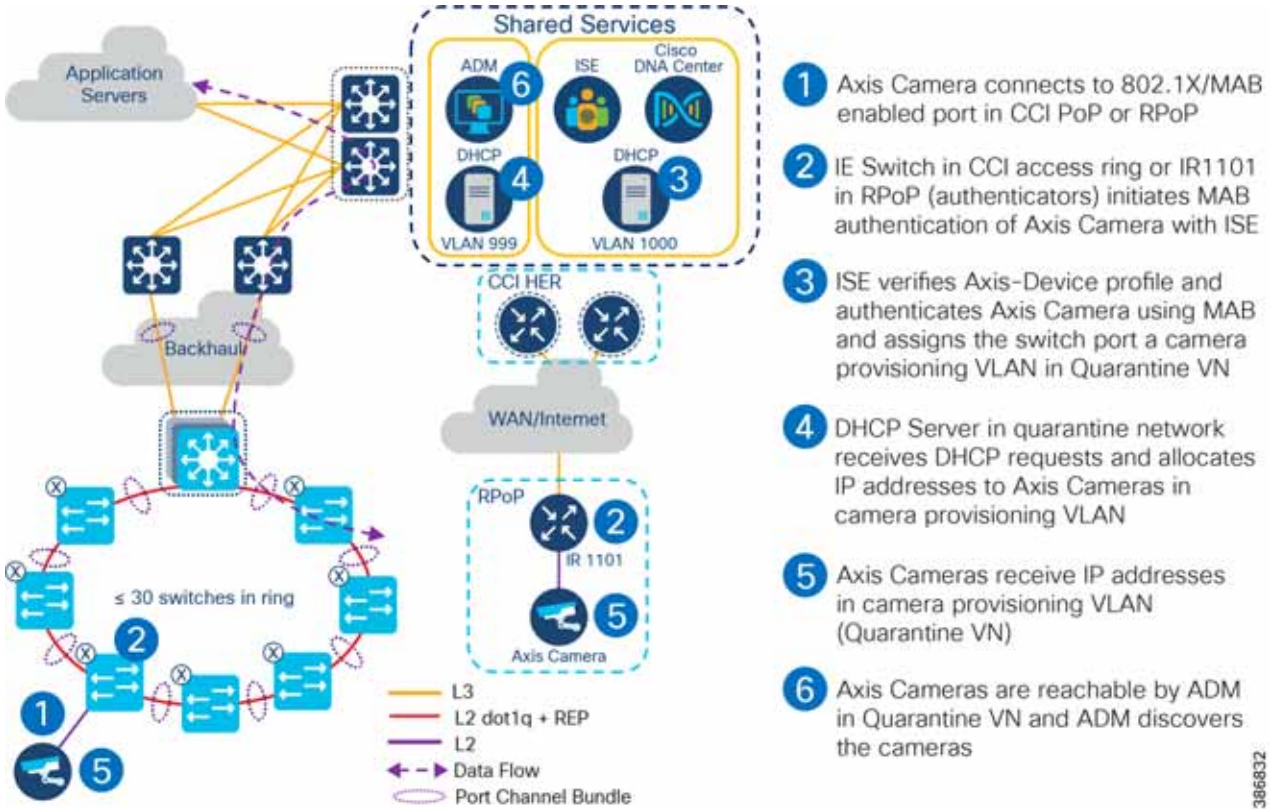
- Install and Configure ADM application in CCI Shared Services network (for Day 0 provisioning and Day N management of cameras) in a separate VLAN or subnet with access to quarantine network.

- 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 5 illustrates the Day 0 provisioning of Axis Cameras for initial discovery and onboarding steps in CCI.

Figure 5 Axis Cameras Day 0 Onboarding



In Figure 5:

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. Axis Camera sends DHCP messages to request for a new IP address in quarantine VLAN.

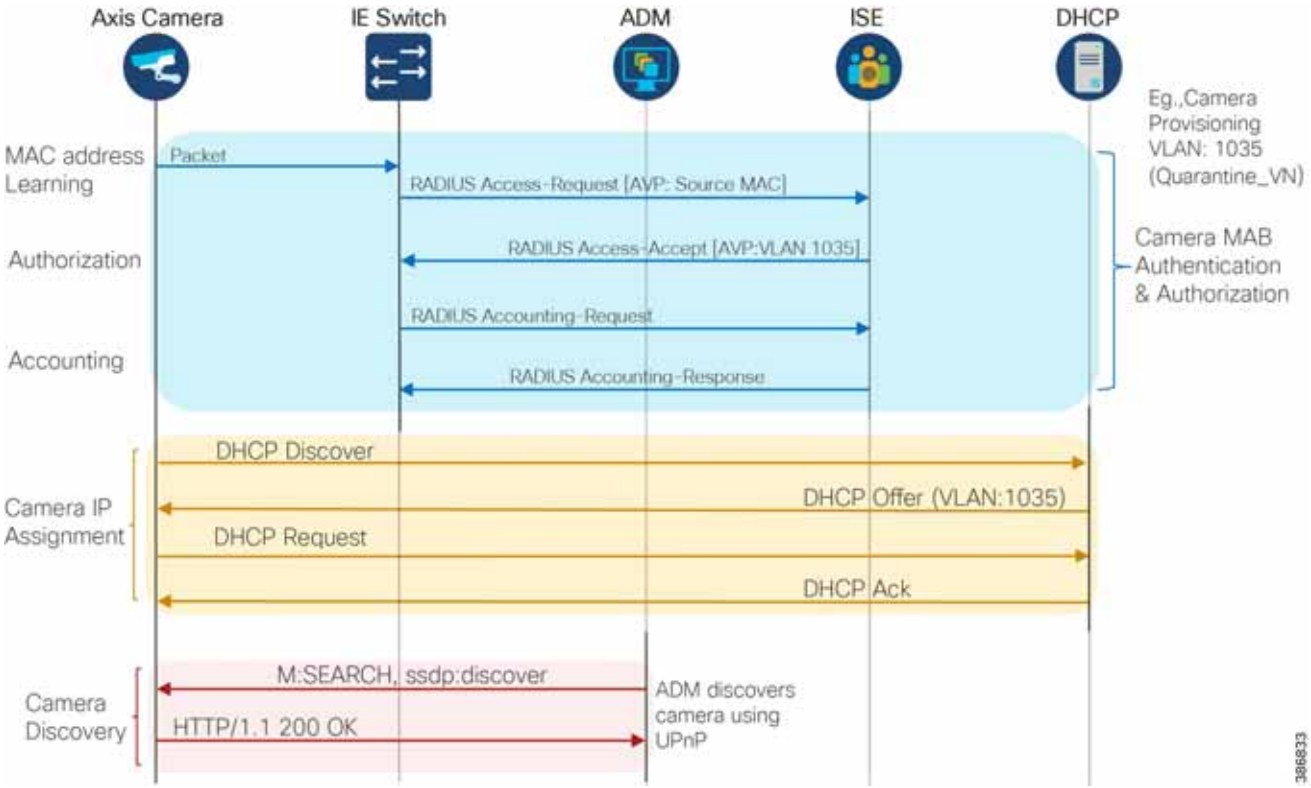
   Note: There is limited access between the quarantine VLAN and the rest of the network.

5. DHCP server in quarantine network allocates IP address to the camera and the camera receives the IP address for its request.

6. After the 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 6 depicts a sequence of messages flow for Axis Camera onboarding in a CCI PoP.

Figure 6 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 Extensibe 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.

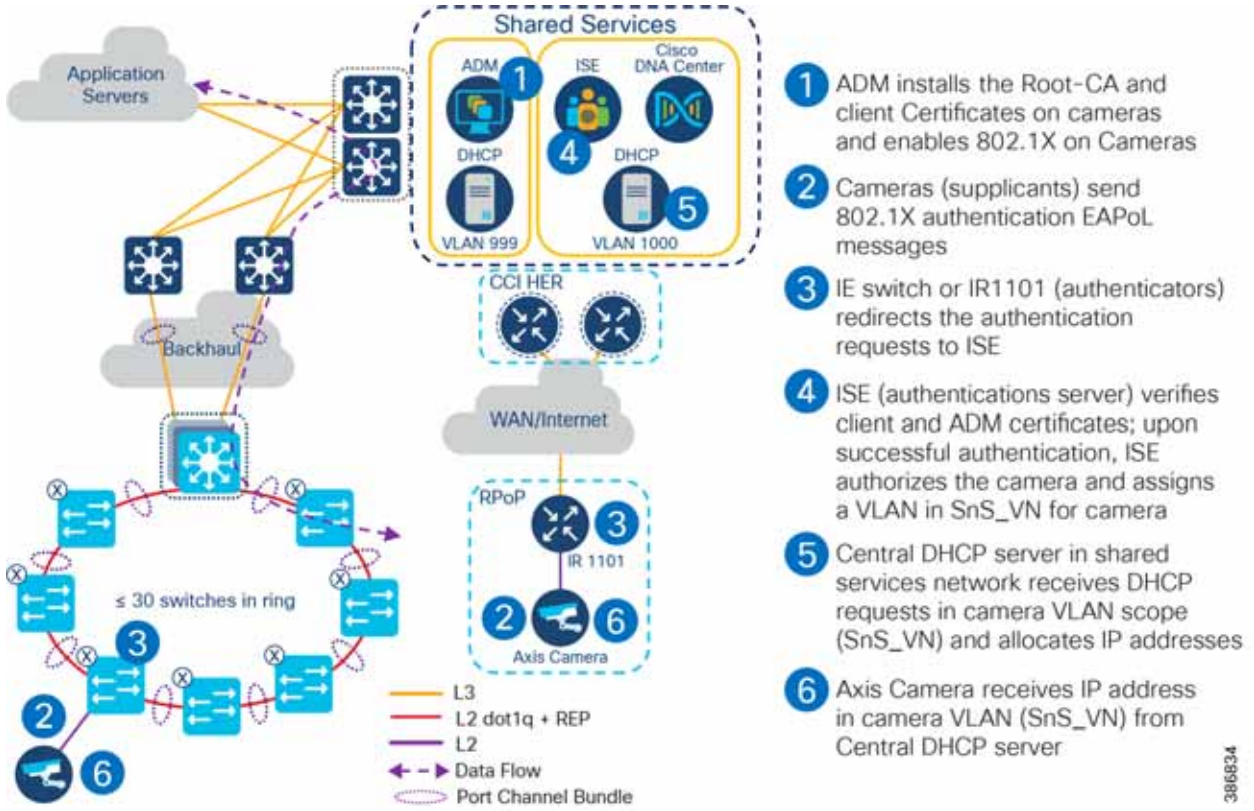
- Configure ADM in quarantine network as Root-CA server to provide client certificates to Axis Cameras and Cisco ISE as the RADIUS server in CCI.
- Install ADM Root CA certificate chain in Cisco ISE trusted certificate store.
- Configure ISE certificate as authentication server certificate in ADM.
- 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:

- https://www.axis.com/files/whitepaper/wp_ieee_8021x_axis_products_en_2003_hi.pdf

Figure 7 shows the Axis Cameras 802.1X authentication steps in a CCI PoP or RPoP.

Figure 7 Axis Cameras 802.1X Authentication in CCI



In Figure 7:

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 as 802.1X 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 switch port in the network 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.

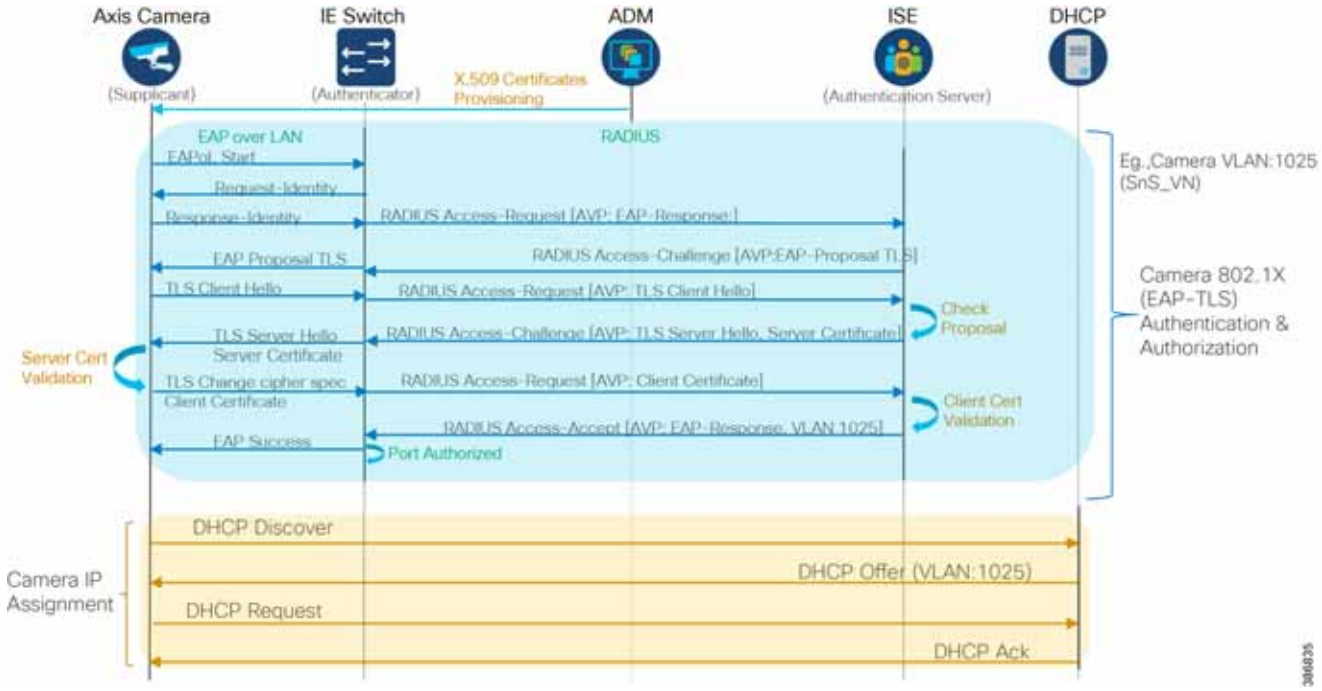
5. The cameras send DHCP messages in the VLAN (SnS_VN) and a centralized DHCP server in shared services network receives DHCP requests and allocates IP addresses to cameras in the respective VLAN DHCP scope.

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 (for example, 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 8 lists a sequence of Axis Cameras 802.1X authentication messages and DHCP messages flow in the CCI network.

Figure 8 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.

Meraki Video Camera

A key element in any network or city planning is security. Whether network or physical security, it must be considered and implemented to some degree. While network security practices are well known, physical security must also be used to prevent or discourage unauthorized access or to monitor sensitive areas. Video security has been an effective means of monitoring activity while acting as a visible crime deterrent. In a city environment this could look like monitoring of city buildings or assets. They could also be used to monitor sensitive or high value installations. In a roadways or intersection scenario, video can be used to monitor intersections with high accident rates for later analysis. It can also be used to monitor who accesses a roadside cabinet. Cisco Meraki video cameras connected to a secured CCI network can provide video security for these scenarios with access, configuration, and monitoring handled by a cloud managed portal. And using the latest 2nd generation cameras provides video analytics enabling object detection whether vehicle or pedestrian.

For more information on the Cisco Meraki MV Smart Camera, see this link: https://documentation.meraki.com/MV.

Meraki and CCI Integration

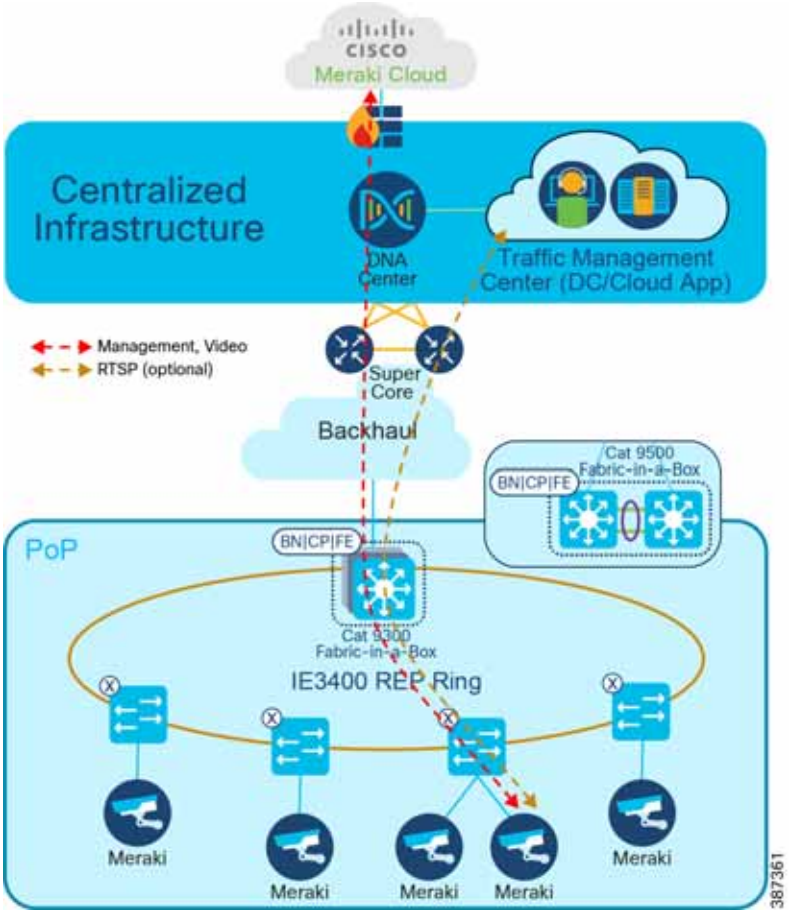
The Meraki management solution is completely cloud based with no on premise option for the video cameras. The only requirement is that the cameras can reach the Meraki dashboard. The specific ports needed are found at this link,

https://documentation.meraki.com/General_Administration/Other_Topics/Upstream_Firewall_Rules_for_Cloud_Connectivity.

To minimize the security risks of a device communicating with the Internet, it is recommended to put the Meraki cameras in a VN that already has Internet access with a separate SGT to prevent any cross communication. This VN must have the necessary TCP/UDP ports open on the firewall to allow the Meraki management and video traffic to reach the dashboard. Because the cameras do not support 802.1x on the wired port, it is also recommended to use MAB to profile the cameras when onboarding them in Cisco DNAC.

To ensure high video quality, Meraki cameras mark the video traffic with DSCP 40. Refer to the CCI QoS section for more details on configuring policies for the various services.

Figure 9 CCI + Meraki Integration



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.

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.

Outdoor and 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 by 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.

Refer to the following chapters in the CCI General design guide for the detailed design on Outdoor and Public Wi-Fi network infrastructure for deploying Wi-Fi use cases in Cities:

- Solution Architecture
- Switched Ethernet Access Networks
- Wireless Access Network
- CCI Remote Sites (RPoPs)

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 betterin 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:

Deployment area	Use cases
Cities	General surveillance for public safety People counting Police and Security Body Cameras (with Wi-Fi connectivity and real-time uploading)
Roadways	General surveillance for traffic monitoring and public safety Wrong-way driving detection License-plate Recognition (LPR) Vehicle counting and classification

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 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 (including 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-out 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 Wi-Fi 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.

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.

Refer to the following chapters in the CCI General Solution Design Guide for the detailed design on SCADA network infrastructure for deploying SCADA use cases in Cities:

- Solution Architecture
- Switched Ethernet Access Networks
- CCI Remote Sites (RPoPs)

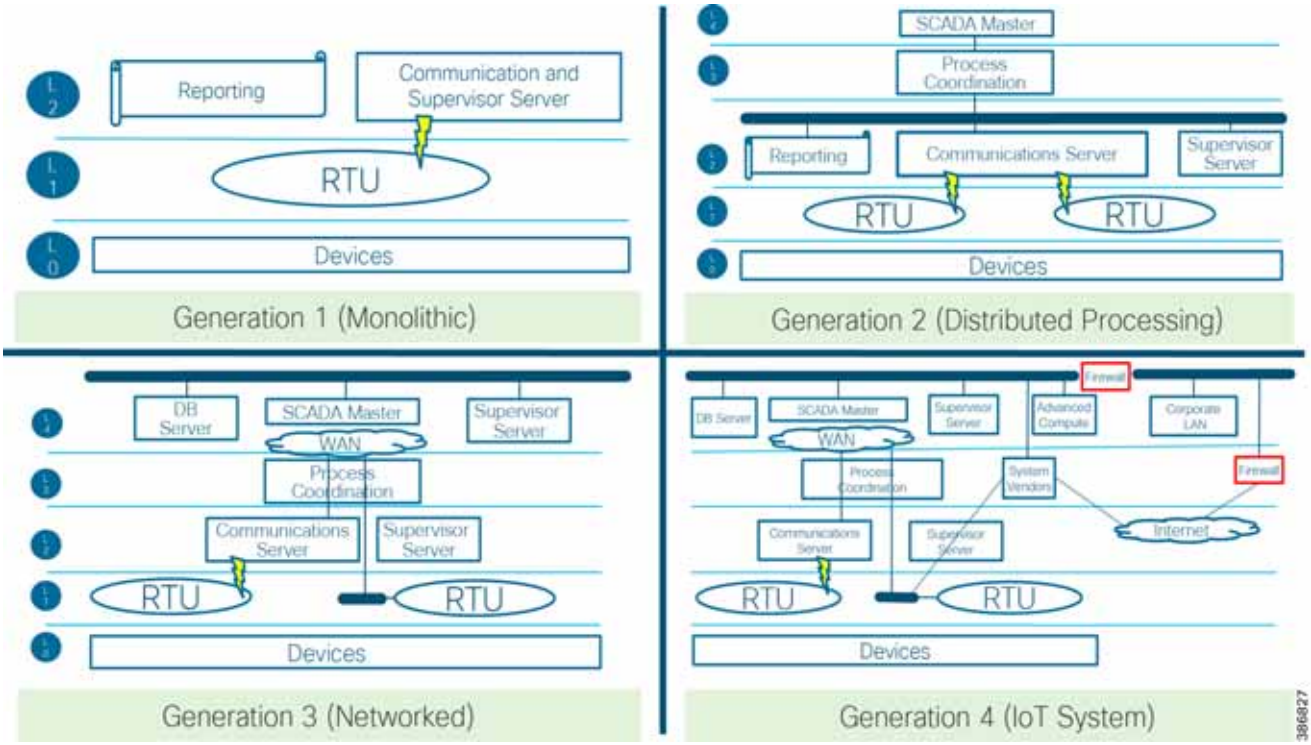
SCADA systems are transitioning to IoT systems (4th Generation SCADA System)

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 10 below represents the evolution of SCADA systems over time.

Figure 10 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
- Intelligent Electronic Device (IED)
- Supervisory computers – Communicates with PLCs, RTUs and presents to the HMI
- Communication infrastructure – Analog (T202, POTS) or digital (RS485, TCPIP)

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.

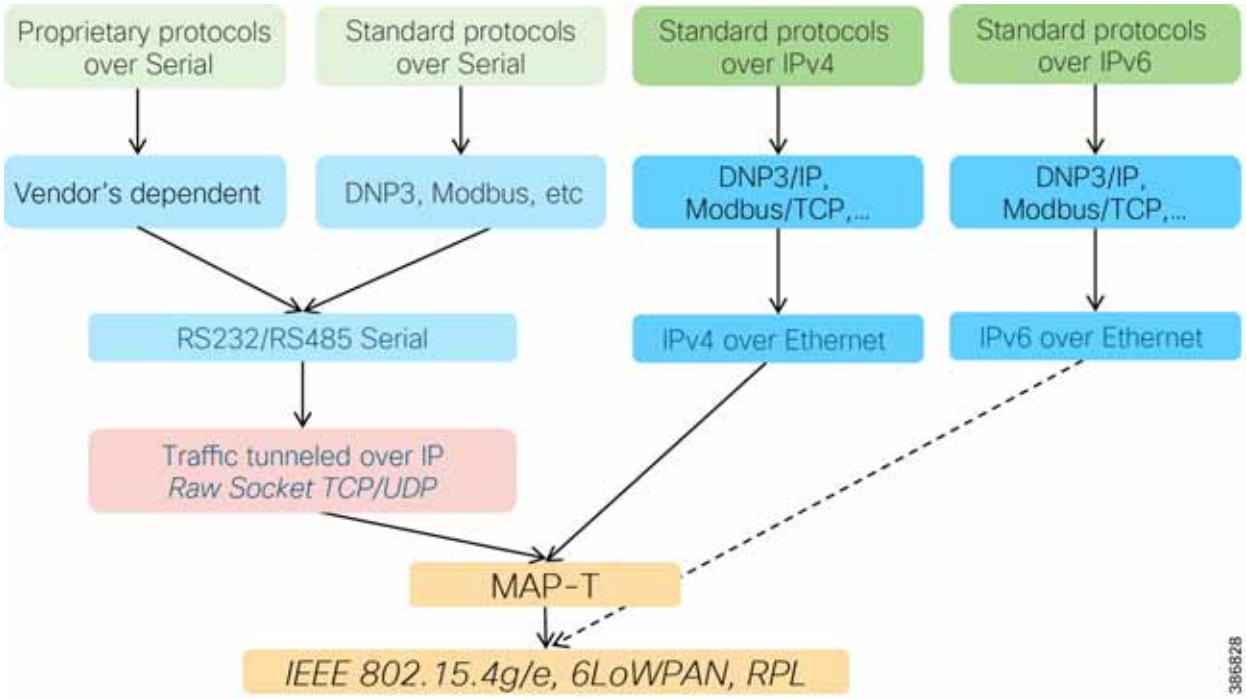
In each of the access methods above we support three communication types Native IP, Gateway encapsulation, and RAW Socket SCADA traffic.

- 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.

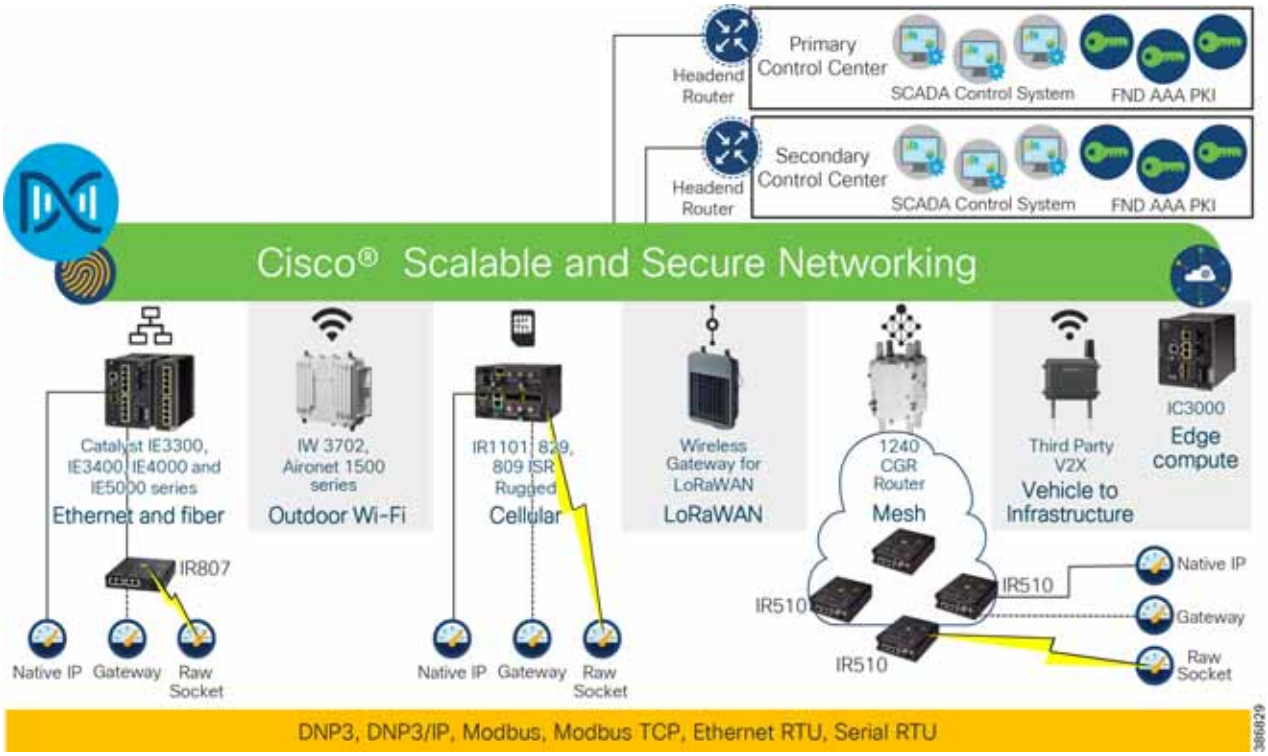
- Modbus RTU RS232 using Raw Socket – Makes the use of a compact, binary representation of the data for protocol communication. RTU messages are transmitted continuously without inter-character hesitation. Application layer protocol.
- Modbus TCP - Variant of Modbus where the checksum is completed at lower layers
- DNP3 RTU RS232 using Raw Sockets – Distributed Network Protocol. IEEE 1815 standards-based SCADA communications protocol. Consists of both the application and data link layer with a pseudo-transport layer.
- DNP3/IP – DNP3 over a TCP/IP network
- DNP3 RTU (Serial) to DNP3 IP using protocol translation

Figure 11 SCADA Protocols



The supported deployment models are displayed below:

Figure 12 SCADA High Level Architecture



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.

https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Distributed-Automation/Feeder-Automation/DG/DA-FA-DG/DA-FA-DG.html

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.

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 2.1 that includes basic set and get functions across CR-Mesh.
- What is the latency requirement of the application? For CCI 2.1 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 daisy chain or tree topology? Depth of the daisy chain and/or tree can impact the operation of set and get procedures and may limit the depth of topology deployments. In CCI 2.1, 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.

Conclusions

Digital transformation for cities and communities 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