Extended Enterprise Design Guide

Extended Enterprise Introduction

The Extended Enterprise Cisco Validated Design (CVD), which is documented in this Design Guide, provides a design foundation for incorporating a broad set of technologies, features, and applications to help customers extend the enterprise IT (Information Technology) services to outdoor spaces. CVDs provide the foundation for systems design and are based on common use cases or engineering system priorities. Each guide incorporates a broad set of technologies, features, and applications to address customer needs. Most important, each guide has been comprehensively tested by Cisco engineers to help ensure a faster, more reliable, and fully predictable deployment.

Extended Enterprise CVD

Every enterprise has production, storage, distribution, and outdoor facilities. IT reach extends beyond the traditional carpeted space to non-carpeted spaces as well. IT can now extend network connectivity, security policy, and management to the outdoors, warehouses, and distribution Centers—with the same network operating systems and network management offering automation, policies, and assurance. The Cisco Digital Network Architecture (Cisco DNA) is based on automation and analytics to delivery policy end-to-end at scale. Cisco DNA enables customers to capture business intent and activate it network wide in the campus and in non-carpeted spaces where the operations happen.

This CVD outlines the steps for both IT and operations teams to accomplish business goals by digitizing the operations in the outdoor spaces of an enterprise. It includes design guidance for implementing extended enterprise use cases with the customer’s existing Cisco DNA Center.

Comments and Questions

To learn more on Extended Enterprise solutions, please visit:

- https://www.cisco.com/go/extendedenterprise
- https://www.cisco.com/go/iotcvd

Scope and Audience for this Document

This design guide provides an overview of the requirements driving the evolution of extended enterprise network designs followed by a discussion of the latest technologies and designs that are available for building an extended network to address those requirements. It is a companion to the associated design and deployment guides (DIGs) for Enterprise Networks, which provide configurations explaining how to deploy the most common implementations of the designs as described in this guide. The intended audience are technical decision makers who want to understand Cisco's extended enterprise offerings, technology options available, and the leading practices to design the best network for the needs of an extended enterprise.

This CVD discusses the Extended Enterprise design for non-fabric technology, with Cisco DNA Center. The Extended Enterprise design guide for fabric technology will be published in a later release. For the associated deployment guides, design guides, and white papers, see the following pages and Appendix A—Related Documentation, page S3:

- Cisco Enterprise Networking design guides: https://www.cisco.com/go/designzone
- Cisco IoT Solutions design guides: https://www.cisco.com/go/iotcvd
- Cisco Extended Enterprise Solutions overview: https://www.cisco.com/go/extendedenterprise
The Value of the Extended Enterprise CVD to an Organization

As your organization grows, customers must plan how to extend the enterprise network infrastructure to support the network requirements of non-carpeted spaces. Planning, testing, and implementing various components and shared services for an extended network poses a large challenge for organizations. In contrast, by using the Extended Enterprise CVD’s modular approach that tests and validates the foundation infrastructure, security, automation, assurance, and shared services, organizations can reduce costs, risks, and operational issues and increase deployment speed.

An organization can benefit in the following ways by deploying the Extended Enterprise CVD:

- Summarized and simplified design choices for accelerating design, deployment and operation of the extended networks
- Simplicity through a single pane of glass (SPOG) for managing carpeted and non-carpeted spaces—including design, policy, provision, and assurance for all network devices
- Consistent security policy enforcement across carpeted and non-carpeted spaces
- Reduced cost of deployment through Plug and Play (PnP) for provisioning Industrial Ethernet switches and outdoor access points
- Scalability provided by intent-based networking, assurance, guided remediation, and troubleshooting
- High Availability and Reliability in non-carpeted spaces for resilient operations

Business Overview

Introduction to Cisco® Digital Network Architecture (DNA)

The top-of-mind issue in IT organizations today is digital transformation. The Enterprise Network is at the heart of every digital transformation. Most enterprises have thousands of users, thousands of applications, and often tens of thousands of network-enabled devices. Global Internet Protocol (IP) traffic is projected to nearly triple from 2017 to 2022; additionally, 10 billion more Internet of Things (IoT) devices are expected to come online within the same time frame (according to Cisco Visual Networking Index™ forecasts1).

Each year various new devices in different form factors with increased capabilities and intelligence are introduced and adopted in the market. A growing number of machine-to-machine (M2M) applications, such as smart meters, video surveillance, healthcare monitoring, transportation, and package or asset tracking, are providing a major contribution to the growth of devices and connections. By 2022, M2M connections will be 51 percent of the total devices and connections (according to Cisco Visual Networking Index™ forecasts).

Manual management of network operations is becoming increasingly untenable for IT departments, a challenge that is exacerbated by the myriad inconsistent and incompatible hardware and software systems and devices in the enterprise. In contrast, an intent-based, closed-loop architecture that includes automation and analytics platforms significantly frees up IT time and resources, and allows them to be reallocated to driving strategic projects and digital transformation. Cisco DNA Center is the platform that introduces automation and analytics into the enterprise network. Cisco DNA Center is a single pane of glass for designing a network, provisioning the network, administering policy for the network, and assuring the network.

The primary purpose of the automation platform in Cisco DNA Center is to “talk” to the network; in other words, to translate the expressed business intent into optimal platform-specific configurations on the network devices. In a complementary manner, the primary role of the analytics platform is to “listen” to the network, specifically to gather, correlate, and make sense of all the network telemetry generated by network devices in order to correlate this data with the expressed business intent.

Cisco DNA Center provides a road map to digitization and a path to realize immediate benefits of network automation, assurance, and security. Cisco Software-Defined Access (SD-Access) is the Cisco DNA Center evolution from traditional campus Local Area Network (LAN) designs to networks that directly implement the intent of an organization. SD-Access is enabled with an application package that runs as part of the Cisco DNA Center software for designing, provisioning, applying the policy, and facilitating the creation of an intelligent campus wired and wireless network with assurance.

Fabric technology, an integral part of SD-Access, enables wired and wireless campus networks with programmable overlays and easy-to-deploy network virtualization, permitting a physical network to host one or more logical networks as required to meet the design intent. In addition to network virtualization, fabric technology in the campus network enhances control of communications, providing software-defined segmentation and policy enforcement based on user identity and group membership.

SD-Access Extension is for extending the enterprise network to provide more connectivity to non-carpeted spaces of an enterprise. The products for extending the enterprise network are different, but the processes and techniques to build it out are the same.

Introduction to Extended Enterprise

The Extended Enterprise is where business operations happen: outdoor spaces such as distribution centers, warehouses, ports, or campus parking lots. Enterprises are looking to innovate and differentiate their offerings by digitizing their operations beyond the traditional carpeted spaces. However, the initiatives on digitizing the operations require network connectivity to be extended beyond the traditional air-conditioned spaces—to connect and manage IoT devices as well as to deploy traditional enterprise end devices in outdoor or extreme-temperature environments. Customers require ruggedized Ethernet switches and outdoor access points to extend network connectivity to non-carpeted spaces because of the harsh environments in outdoor spaces. In addition, security concerns for extended networks should be addressed with consistent network policies. Customers require speed with agility to deploy and manage networks in non-carpeted spaces while meeting the required compliance and regulatory goals, as illustrated in Figure 1.

With digitization, enterprises are challenged to improve operational efficiency, deliver new service offerings, and increase customer satisfaction. Delivering these business outcomes require a new approach to networking, one that is intent-based, in order to manage the challenges of scale and security faced by the enterprise.

Figure 1  Extended Enterprise Objectives and Challenges

By connecting the Extended Enterprise to your core IT managed networks, you can:
Extended Enterprise Design Guide

Extended Enterprise Introduction

- Unleash the power of data from the edge to gain operational insights and improve processes and systems
- Enable new digital experiences for your customers and increase customer satisfaction
- Generate new incremental revenue for your business by digitizing your extended enterprise
- Manage the entire enterprise network centrally and reduce OpEx
- Simplify, secure, and control IT-run industrial extended enterprise environments

Extended Enterprise Network Requirements

Many enterprises have warehouses, parking lots, and distribution centers; typically, multiple. Because of dust, heat, cold, dampness, and humidity, these outdoor facilities require ruggedized networking products. Enterprises want to replicate operations as much as possible to save on capital expenditures and operational costs.

Figure 2 Extended Enterprise Use Cases

With the explosive growth in IoT and industrial devices connecting to the core network, combined with the need to secure against threats and secure network access, IT must oversee, manage, and secure extended spaces, and ensure business integrity. Therefore, network teams are being asked to extend network connectivity beyond the air-conditioned spaces more and more in order to connect and manage IoT devices and traditional enterprise end devices being deployed in outdoor or extreme-temperature environments. The overall goal is to drive efficiency and reduce OPEX in the non-carpeted spaces with Industrial Networking.

Outdoor facility networking requirements mean that IT needs to be able to quickly provision devices and services, manage the network device inventory and software versions of the network devices, and do it all securely. Most enterprises also have a need to enable outdoor connectivity to campus parking lots in adverse weather conditions for assets such as IP cameras, Video encoders, and Wi-Fi Access Points.

Enterprises that have distribution centers need reliable network operation without air-conditioning costs. Operational efficiency of the connected equipment is of key interest to distribution centers and IT executives. Consolidation of warehouse and distribution center networks into one centrally-managed network greatly simplifies Extended Enterprise networks managed by IT through the Cisco DNA Center and SD-Access Fabric. The Cisco DNA Center can provide a SPOG for managing Enterprise and Extended Enterprise networks. This Extended Enterprise Design Guide addresses the network requirements described in the next section.
Flexible Industrial Ethernet Network Foundation for Harsh Environments in Non-Carpeted Spaces

Extended Enterprise environments require network devices to operate in very hot (+70°C), very cold (-40°C), and dusty environments. Extended Enterprise network devices need to be hardened for vibration, shock and surge, and noise immunity while adhering to overall IT network design, compliance, and performance requirements.

Extended Enterprise deployments in outdoor spaces, warehouses, and distribution centers require high-speed Gigabit Ethernet connectivity in a compact form factor modular design, which is flexible for rapid expansion, bandwidth, and capacity planning to grow with the needs of operations.

The Industrial Ethernet network in non-carpeted spaces must comply with stringent industry standards for electromagnetic emissions, immunity, and safety.

Extend Secure Connectivity to Outdoor Non-Carpeted Spaces for Users, Traditional IT Endpoints, and Things

Enterprises have an ever-increasing requirement to securely provide more network connectivity and enable more services beyond the air-conditioned space securely. Cisco’s Industrial Ethernet (IE) switching products are a great example of providing networking connectivity outside the wiring closet. These devices are deployed outdoors, in the ceiling, or in roadside cabinets. The extended access network should have the ability to support high-density industrial PoE/PoE+ providing in-line power for devices such as IP cameras and phones, badge readers, and Wireless Access Points (WAPs).

Most Extended Enterprise environments need IP video surveillance for security, WAPs for mobility, IP phones, desktop PC access, and networked printers - the same types of networked end devices you would find within an air-conditioned office building.

Capture and Translate Business Intent into Network Policies and Consistently Enforce the Policies across the Entire Network

The Cisco 2017 Security Capabilities Benchmark Study found that nearly a quarter of the organizations that have suffered an attack lost business opportunities as a result. Four in ten said those losses are substantial. One in five organizations lost customers due to an attack, and nearly 30 percent lost revenue. Hardening the security of the network devices is essential since they are common targets for security attacks.

Intent-based networking (IBN) enables conventional practices that require the alignment of manually-derived individual network-element configurations to be replaced by controller-led and policy-based abstractions that easily enable operators to express intent (desired outcome) and subsequently validate that the network is doing what they asked of it. The controllers, which provide the automation and controls that make up the IBN, reduce risk by ensuring that security policies are being applied consistently across the extended network, and help ensure that policies are compliant with Extended Enterprise business requirements. They capture and translate business intent into network policies and activate them across the infrastructure.

Operations intent-based groupings provide consistent policy and access independent of network topology in carpeted and non-carpeted spaces. Creating group-based policies leveraging attributes such as device type and location provides a much easier and scalable way to manage security policies for access control across the extended enterprise. Scalable Group Tags (SGTs) assigned from group-based policies can provide micro segmentation within a virtual network.

Simple, Centralized Network Management across the Carpeted and Non-Carpeted Spaces

Most enterprises have thousands of users, thousands of applications, and often tens of thousands of network-enabled devices. Managing network operations manually is becoming increasingly untenable for IT departments, a challenge that is exacerbated by the myriad inconsistent and incompatible hardware and software systems and devices in the enterprise.
Adding more devices to the extended network increases the management complexity. To drive simplicity, it is important for enterprises to have a SPOG for designing, provisioning, and administering policies, and ensuring the network consistently across carpeted and non-carpeted spaces. The goal is for network engineers to see everything going on in the network, everywhere in the world, from one interface.

To drive business growth and innovation, a complete network management system that is centralized across carpeted and non-carpeted spaces is required. Customers need a network management system that can automate the deployment, connectivity, and lifecycle of your infrastructure and proactively maintain the quality and security of your applications so that IT staff can focus on networking projects that enhance your core business.

Reduce Day Zero Deployment Time of Networks in the Non-Carpeted Spaces

Many Extended Enterprise environments do not have an IT network engineer on-site and the extended network must be managed remotely. IT staff need to be able to quickly deploy new devices and new services. Time is critical and expensive since the installer is likely an hourly contractor or has to travel from the corporate office to be on-site.

An extended network should automatically remotely provision and onboard new network devices with minimal network administrator and field personnel involvement. A workflow should define a network device provisioning process that includes a series of actions such as installing a software image, applying a device configuration, renumbering a switch stack, or specifying a switch stack license.

The Cisco DNA Center provides the PnP feature for zero touch network deployment in non-carpeted spaces. With PnP, you should be able to ship new industrial networking devices directly to the warehouse or a distribution center where a local person will power it up. The switch will automatically connect to the Cisco DNA Center to retrieve the correct code based on its serial number. PnP can significantly reduce the time for provisioning the extended network and for spending on upgrades by automating the steps.

Compliance to Latest Security Patches of Industrial Networking

Network Administrators are always challenged when it comes to upgrading their network, whether it is planned or ad-hoc, in order to remediate a security vulnerability. As Extended Enterprise networks become more and more complex, it becomes even harder to manage the software versions and deploy the new security patches when they become available.

To determine whether software image standards comply with the deployed devices, it is imperative that device auditing is automated and flag devices that are not compliant with standardized software image updates. Patching provides small updates to react quickly to security fixes. The Cisco DNA Center simplifies the version management and routine deployment of software updates to your network devices by helping customers plan, schedule, download, monitor, and standardize software image updates.

Secure Outdoor Wireless Connectivity in Non-Carpeted Spaces

Extended Enterprise networks require rugged outdoor Wi-Fi coverage for their outdoor clients. Wireless video cameras monitor security. In large installations, the roaming functionality provided by multiple access points enables wireless users to move freely throughout the facility while maintaining uninterrupted access to the network. The security requirements described above should be consistent for wired Ethernet or wireless LAN.

With the latest 802.11ac Wave 2 technology, transmitting data at speeds beyond 1Gbps can accommodate growth in wireless usage in outdoor spaces. One key part of 802.11ac Wave 2 technology that can help keep extended networks ahead of the capacity crunch is multi–user multiple–input and multiple–output (MU–MIMO). MU–MIMO allows an access point to transmit to multiple clients at the same time instead of sending data to a single client at a time. These parallel transmissions improve RF efficiency when client devices also support 802.11ac Wave 2.

Cisco outdoor access points can be deployed as traditional access points or wireless mesh access points. Cisco Flexible Antenna–Port technology uses software that is configurable for either single– or dual–band antennas. It allows customers to use the same antenna ports for either dual–band antennas to reduce footprint or single–band antennas to optimize radio coverage.
Extended Enterprise Design Guide

Extended Enterprise Introduction

Simplify Deployment of QoS across the Extended Network

Extended networks can have a variety of business needs for QoS. A safety and security operations business may want to ensure a high quality images for video cameras in the campus parking lots for video surveillance. A distribution center may want to guarantee voice quality to meet enterprise standards.

The principle goal of a QoS policy for an extended network is to express the strategic QoS policy with maximum fidelity and to generate platform specific configurations. The Cisco DNA Center can simplify the deployment of QoS across the Extended Enterprise.

Network Assurance—Visibility and Analytics on the Health of Industrial Network Devices

As networks grow in complexity, research show that network IT spends four times more time collecting the data than analyzing the problem. In a world of device explosion and extended networks, this problem will only get worse. The traditional response to onboarding incidents involves many manual steps, such as checking user credentials and DHCP issues, and radio channel analysis, all of which adds to a high incident response time.

It is imperative an extended network has onboarding analytics across the entire network—both wired and wireless. Cisco DNA Assurance uses anomaly-driven telemetry from 240+ real-time events coming from the wireless and wired infrastructure on client onboarding that helps to evaluates the time to connect and possible stages for the delay. Any delays in onboarding will be spotted and flagged by the Cisco DNA Center before the user has a chance to report the problem.

Guided Remediation and Troubleshooting of Issues in the Extended Network

A very common challenge facing IT is isolating problems; that is, finding the needle in a haystack. Further, unlike the relative predictability of wired networks, wireless networks are easily affected by more dynamic and fluctuating variables (such as Received Signal Strength Indicators and Signal-to-Noise Ratios). As such, the challenge is exacerbated and can be more aptly described as trying to find a randomly appearing and disappearing needle within a haystack! Issues come and go as more rogue devices come online. And if IT cannot replicate such transient and fluctuating Wi-Fi issues, they cannot resolve them.

To guide remediation to a network issue, it is important to have a holistic view of users, clients, applications, and the network with full context of the interactions between these elements. Furthermore, troubleshooting is not limited to currently occurring issues; Cisco DNA Center allows operators to “go back in time” via a time-series database of all measured data points to diagnose and root-cause issues that have occurred in the past.

With Cisco DNA Assurance, IT is able to go back in time up to 14 days to view the full contextual network data and interrelationships, eliminating the need to replicate the issue in order to identify and resolve a problem. All information on the user or the network device changes to the selected time.

Extend Shared Services to Extended Networks in Non-Carpeted Spaces

Most extended network deployments require access to shared services in the form of identity services, Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), IP Address Management (IPAM), IP voice/video collaboration services, application servers, and data center applications. It is important that these shared services are designed correctly in order to preserve the isolation between different virtual networks sharing those services. Most deployments require shared services across all virtual networks and other inter-virtual network communication.

High Availability, Reliability and Scale of Extended Networks to Meet Operational Needs

Most Extended Enterprise network deployments have to cater to the needs of business-critical operations. Therefore, extended network designs should enable end-to-end redundancy and high availability. The design should extend geographical scalability where longer-distance connectivity is required.
Example Use Case: Secure Connectivity for Campus Parking Lots

Every enterprise campus may have a number of parking lots to cater to the needs of their employees and guests. Campus parking lots are typically monitored by safety and security operations teams responsible for theft prevention and for ensuring safety of the employees and the guests. Digitizing the campus parking lots can help improve the overall experience of the employees such as a mobile app tracking a free electric vehicle charging station near a campus building. In addition, enabling secure outdoor wireless connectivity in the campus parking lots is desirable for business collaboration.

The safety and security operations would like to have IP video surveillance cameras installed in the parking lots to ensure the safety of employees and the guests entering/leaving the parking lot. Live streaming and video retention to comply with local policies is critical for the safety and security operations agents to monitor from remote locations. Appropriate QoS policies for campus/Wide Area Network (WAN) network bandwidth allocation is needed for live video monitoring by remote agents.

How can we address such network requirements in outdoor spaces where network devices need to be able to work in ruggedized spaces, connecting Power over Ethernet (PoE)-powered end devices such as IP cameras, phones, wireless access points, sensors, and more? The network devices should be hardened to withstand harsh environments, temperature ranges (-40°C to +75°C), vibration, shock, surge, and electrical noise. More importantly, the network devices should comply to the safety standards and certifications with high Mean Time Between Failures (MTBF).

The Cisco Industrial Ethernet switches and outdoor access points have been designed specifically to withstand the harshest industrial environments in a compact, form-factor, modular switch that is purpose-built for a wide variety of Extended Enterprise applications, such as campus parking lot environments. The Cisco Industrial Ethernet switches provide bandwidth and capacity to grow with a customer’s networking needs: full Gigabit Ethernet interfaces to connect high-speed wireless access points and High-Definition (HD) IP cameras.

An employee or guest’s mobile device or a parking lot IoT sensor, when compromised by malware, may change network communication behavior to propagate and infect other endpoints. Cisco Identity Service Engine (ISE) and Cisco Software-Defined Access (SD-Access) can address the need for complete isolation between the IoT sensors, traditional IT endpoints such as IP Camera and enterprise network by using macro-segmentation, and putting devices into different overlay networks, thus enabling the isolation.

Flexible policy creation allows the ability to have groups of device types and user roles to restricted communication within a group or amongst groups. By extending the secure connectivity to campus parking lots, IT needs to be able to quickly provision devices and services, manage the network device inventory, manage the software versions of the network devices, and do it all securely.

The primary software solution components are Cisco Industrial Ethernet Switches, Outdoor Access Points, Cisco DNA Center, Cisco ISE, and the Cisco DNA Center Assurance Engine. Cisco DNA Center is the primary application for designing, defining policy, and provisioning the network infrastructure - a SPOG across the carpeted and non-carpeted spaces of an enterprise. The ISE provides the security behind the solution. The Cisco DNA Center Assurance Engine gives insight into network and user performance. Deploying the intended outcomes for the needs of the extended enterprise operations is simplified using the automation capabilities built into the Cisco DNA Center, and those simplifications span the wired and wireless domains.
System Design

This chapter, which discusses the end-to-end system design starting with an overview of the enterprise network and followed by a detailed design for the Extended Enterprise network, includes the following major topics:

- Enterprise Network Design Overview, page 9
- Extended Enterprise Network Design, page 14
- Extended Enterprise QoS Policy Design, page 38
- Extended Enterprise Network Data Flows, page 40
- Extended Enterprise High Availability, page 46
- Extended Enterprise Scale and Dimensioning, page 48

Enterprise Network Design Overview

The enterprise is a geographically-distributed organization spread across multiple sites and campuses. The overall Enterprise network is managed by the Cisco DNA Center. Wireless and wired connectivity is provided across the enterprise. Several types of hosts or endpoints such as video surveillance cameras, Wi-Fi clients, IP Phones, and video terminals are connected to the enterprise network for different services. The application services are centrally hosted and have restricted access to authorized clients. Enterprise-wide shared services such as the DHCP server, IPAM, DNS, and ISE are hosted in the data center along with the Cisco DNA Center. Enterprise internet connectivity is protected by the firewall. Internet access is available across the organization. The Cisco DNA Center requires internet access for regular cloud updates.

The enterprise network, depending on the size and its needs, can be a two-layered or three-layered architecture. The design considerations and design details for the extended enterprise (discussed in Extended Enterprise Network Design, page 14) apply equally well to both architectures. For illustration purposes, a three-layered architecture, as shown in Figure 3, is considered to be the Enterprise Network Architecture. The three layers are the core, distribution, and access layers. The following section describes a high-level overview of these hierarchical layers and respective roles.
Hierarchical Model

The hierarchical network design model breaks the design into modular layers. Each layer implements specific functions, thus helping simplify network design, deployment, and management, and also making the network scalable. Modular structuring of the network also improves scalability and facilitates resiliency through improved fault isolation. Cisco Enterprise Network Design CVDs (please see Appendix A—Related Documentation, page 53) cover these architectures.

The three-layered architecture consists of the following:

- **Access layer**—Provides endpoints and users direct access to the network.
- **Distribution layer**—Aggregates access layers and provides connectivity to services.
- **Core layer**—Provides connectivity between distribution layers for large LAN environments.

Platform selection is primarily driven by differences in capacity, density, and features.

Enterprise Access Layer

The access layer, which is placed at a close proximity, provides connectivity to user devices and clients that are connected to the network. The access layer provides both wired and wireless connectivity and contains features and services that ensure security and resiliency for the entire network. Typically incorporating Layer 2 switches, it provides different functionalities that include:

- Layer 2 connectivity - fiber/copper and wireless to endpoints (e.g., laptops, cameras, and IP phones)
- Can provide PoE power to wired endpoints
- Enforces security by end user authentication and security policy enforcement
Acts as a QoS trust boundary (Classification, Marking)
Labels packets to enforce segmentation

Enterprise Distribution Layer

The distribution layer has several important services. It aggregates access layers and provides connectivity services. It aggregates traffic from several access layer switches and provides uniform transportation. The important features provided by distribution layer devices include:

- Layer 3 connectivity to the core layer and Layer 2 into the access
- Broadcast domain control
- Aggregation of access layer traffic and provide connectivity services
- Routing between LAN and VLANs
- Route aggregation and summarization
- Policy-based security and QoS
- Scalability, fault domain isolation, high availability, and resiliency
- Typically a Layer 3 router or a Layer 3-capable switch is used
- It can act as the fog computing platform

Enterprise Core Layer

A third layer serving as the backbone and central point of the network is often needed while catering to a large distributed network spread across multiple geographically-dispersed buildings. Having a distribution layer switch in each of the buildings helps to reduce costly fiber runs. As networks grow beyond three distribution layer switches, organizations should use a core layer to optimize the design.

The key value-adds and features of the core layer include:

- Uninterrupted connectivity to the distribution layer
- Provides site-wide redundancy, fault tolerance, resiliency, and reliability having Layer 3 connectivity to and from the core layer
- Provides high-speed switching (i.e., fast transport) to support a large-scale network
- Very low latency, avoiding CPU-intensive packet manipulations
- Non-disruption in-service upgrades

Enterprise Endpoints

The devices that connect to the enterprise access switch are called endpoints. Endpoints may be either wired clients that directly connect to the access switch node or wireless clients attached to an access point (AP). Endpoints could be a security camera, IP Phone, user laptop, tablet, or mobile phone connected to the network. Endpoints are increasing due to workforce mobility, helping users to be less tethered to the desk. However, an ever-increasing risk of endpoints loaded with insecure apps, with consistent exposure to malware across Internet protocols, exists. Therefore, endpoint security consisting of authentication, posturing, profiling, and authorization is becoming critical.
Cisco DNA Center

The Cisco Digital Network Architecture Center (Cisco DNA Center) is an open and extensible management platform with a SPOG solution for the entire enterprise to realize intent-based networking that provides network automation, assurance, and orchestration.

The Cisco DNA Center enables management of a large-scale network of thousands of devices. It can configure and provision thousands of network devices across an enterprise in minutes instead of hours. The major priorities for any large enterprise network are security, service assurance, automation, and visibility. These requirements are to be guided by enterprise policy or intent.

Cisco DNA Center Appliance

The Cisco DNA Center software application package is designed to run on the Cisco DNA Center Appliance. When the Cisco DNA Center Appliance becomes unavailable, the network still functions but automated provisioning and network monitoring capabilities are lost. For high-availability, it is recommended to configure three Cisco DNA Center Appliances to form a three-node 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. Multi-node clusters inherently can perform service/load distribution, database, and security replication. Clusters will survive loss of a single node.

Note: The first generation M4-based appliances are end-of-life declared; second generation M5-based appliances should be used.

Shared Services

Shared services, as the name indicates, is a common set of resources for the entire network and accessible by devices/clients across all scalable groups. Usually, shared services are located at a central location. Major shared services of the enterprise include the Cisco DNA Center, ISE, IPAM, DHCP, DNS, next-generation firewall (NGFW), and Syslog. Figure 3 shows the shared services design in the enterprise network.

Enterprise Security Design

An ever-growing number of cyberattacks that are carried out by individuals, organized syndicates, and state-sponsored hackers are launched daily against organizations of all types. Whether for financial gain through acquiring credit card data, extortion through ransomware, identity theft or disruption of services through access to personal data, these attacks are growing in frequency and sophistication. Furthermore, with the ever-growing availability of open-source code bases and tools, these attacks no longer require a high level of skill, enabling them to be launched by less sophisticated threat actors. To understand how to defend against today’s critical threats, please refer to the Cisco Cybersecurity 2019 threat report.

Security Attacks in IoT Devices

It is expected that a code written today will have vulnerabilities in the future. For example, Heartbleed Bug vulnerability, which is a vulnerability in OpenSSL that puts millions of devices at risk because they use common source code, was discovered after many devices had adopted the OpenSSL library as a common cryptographic library. Attacks exploiting security vulnerabilities in IoT devices are not uncommon. Reports of security attacks on IoT devices that exploit the vulnerabilities of the device frequently occur. Using default passwords and poor patching are often the common culprits.

The extensive Cisco security solution protects the enterprise network. In Extended Enterprise Security Policy Design, page 25, we discuss how to secure the Extended Enterprise network.
Enterprise QoS Design

QoS refers to the ability of a network to provide preferential or differential services to selected network traffic. QoS can ensure efficient usage of network resources while still adhering to the business objectives. An end-to-end QoS policy of a network can be configured using application policies provided by the Cisco DNA Center.

The Cisco DNA Center Application Policy constructs and their organization is depicted in Figure 4.

- Applications and Application Sets—Applications are the software programs or network signaling protocols. The Cisco DNA Center recognizes over 1400 distinct applications listed in 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 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.

- Site Scope—Network hierarchy or 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 site scope. Wired and wireless devices can have differences in the behavior, in terms of bandwidth and packet loss. Individual wireless segments may exhibit further variations. Customized policies can be created matching the characteristics of the segment and applied.

- Queuing Profile—Queuing 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

- 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.

The 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 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:

- [https://content.cisco.com/platform_home.sjs?platform=Cisco%20DNA%20Center&release=1.2.x](https://content.cisco.com/platform_home.sjs?platform=Cisco%20DNA%20Center&release=1.2.x)
Enterprise Wireless Network

The key components of enterprise wireless network are access points (APs) and the Wireless LAN controller (WLC). In a Cisco DNA Center-enabled network, intent-driven network management of AP and WLC is provided by the Cisco DNA Center. The WLC simplifies network management by centralizing the configuration and control of Wireless APs. This design approach allows the WLAN to operate as an intelligent information network and support advanced services.

All APs obtain their OS and configurations from the WLC, which performs centralized radio resource management with a global view of the network, thus improving the overall performance with better radio coverage and best use of available frequencies.

For details on the traditional wireless network design, refer to the Campus Wired and Wireless LAN CVD at the following URL:


Extended Enterprise Network Design

The Extended Enterprise Network, as shown in Figure 5, is an extension to the carpeted Enterprise Network described in Enterprise Network Design Overview, page 9 and Enterprise Wireless Network, page 14 to its non-carpeted outdoor corridors. This layer is coined the “Extended Access Layer.” Both wired and wireless network services are provided in the Extended Enterprise. The Extended Enterprise network uses ruggedized Industrial Ethernet access switches such as the Cisco IE2000 series, Cisco IE3x00 series, Cisco IE4000 series, and Cisco IE5000 series, and outdoor APs such as the Cisco AP1560 series and Cisco AP1542. Different endpoints such as security cameras, wireless clients, and display terminals connect to the Extended Access Layer. This section describes the design details of the Extended network, including roles, topology, solution components, wireless integration, and policy applications.
Extended Enterprise Design Considerations

The Extended Enterprise design is flexible enough to suit any campus outdoor requirement. There is no one size fits all. This document serves as a reference design for typical small, medium, and large density requirements. Extended Enterprise, as the name suggests, is an extension to an existing Enterprise Network.

The following design and constructs are leveraged by Extended Enterprise from the parent Enterprise Network:

- IPAM for IP Pools allocation
- Existing enterprise network:
  - The Cisco DNA Center-managed non-fabric enterprise: Cisco DNA Center, core, distribution and access, and all shared services
  - Available end-to-end network redundancy
- Design for network scaling for access and the Cisco DNA Center

**Tech Tip:** For details about the Enterprise Network Design, refer to the *Cisco Enterprise Network Design Guide* at the following URL:


The following design considerations for Extended Enterprise network are listed in this section:

- Different categories of design considerations include design, provisioning, policy and assurance of Extended Enterprise networks, devices, hosts, and services.
- Frequently, enterprise networks spread across multiple buildings and multiple geographies. The Extended Enterprise will have similar characteristics covering the non-carpeted space in each of the locations.
The Extended Enterprise is an extension to the enterprise services; therefore, the traffic characteristics (QoS, segmentation) uniformly apply. The QoS policy of the enterprise network should be applied to all Enterprise Access Layer devices. The traffic from the Enterprise and Extended Enterprise needs to co-exist and share the resources.

The Extended Enterprise design revolves around extending the enterprise network to the non-carpeted area using Cisco ruggedized switches (Industrial Ethernet Switches) and APs.

All Cisco DNA Center-supported models of access switches and APs suitable for Extended Enterprise use cases can be considered.

Extended Enterprise scale consideration: The size of the parent enterprise can range from small to large, so as the scale of the extended enterprise.

The Extended Enterprise will have several categories of services or service groups. Different categories of services need to be isolated from each other, and only controlled communication should be possible between services of different service categories.

The application servers catering to specific services need to have exclusive access only to authorized devices and clients.

High Availability design for end-to-end redundancy.

In summary, the key design components of Extended Enterprise are:

- Ruggedized switches, Non-fabric outdoor AP, shared services, and hosts connected to the extended access layer
- Devices, hosts authentication, and isolation of different categories of traffic

Tech Tip: Extended Enterprise is an extension to an enterprise network. The enterprise network can span multiple buildings and geographies.

Two different deployment scenarios are:

- **Scenario A**—Enterprises having deployed Cisco DNA Center, but not deployed SD Access fabric, as shown in Figure 5.
- **Scenario B**—Enterprises having deployed Cisco DNA Center and SD Access.

This design guide focuses on Scenario A.

A design guide for Scenario B will be addressed in the next edition of the Extended Enterprise Design Guide.
Extended Enterprise Solution Components

Cisco has a range of Industrial Ethernet switches and APs suitable for outdoor deployment. The series of switches and APs recommended for Extended Enterprise are listed in Table 1 and Table 2. A reference list of components for the enterprise network is shown in Table 3.

As shown in Figure 6, Industrial Ethernet (IE) switches can play the role of either access or aggregation.

Table 1  Extended Enterprise Wired Switching Platform

<table>
<thead>
<tr>
<th>Role</th>
<th>Cisco Platforms</th>
<th>Version</th>
<th>Description</th>
<th>CVD Verified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extended Enterprise Access Layer</td>
<td>IE2000 series</td>
<td>IOS 15.2.6E2a</td>
<td>Industrial Ethernet Switches</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst</td>
<td>IOS XE 16.11.1a</td>
<td>Ruggedized full Gigabit Ethernet with a modular, expandable up to 26 ports. Up to 16 PoE/PoE+ ports.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>IE3200 / IE3300 series</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extended Enterprise Aggregation and Access Layer</td>
<td>Cisco Catalyst IE3400 series</td>
<td>IOS XE 16.11.1a</td>
<td>Ruggedized full Gigabit Ethernet with a modular, expandable up to 26 ports.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>IE4000 series</td>
<td>IOS 15.2.6E2a</td>
<td>Ruggedized DIN rail-mounted 40 GB Ethernet switch platform. IE4010 Series Switches with 28 GE interfaces and up to 24 PoE/PoE+ enabled ports.</td>
<td>Access Layer verified</td>
</tr>
<tr>
<td></td>
<td>IE5000 series</td>
<td>IOS 15.2.6E2a</td>
<td>Ruggedized One RU multi-10 GB aggregation switch with 24 Gigabit Ethernet ports plus 410–Gigabit ideal for the aggregation and/or backbones, 12 PoE/PoE+ enabled ports.</td>
<td>Access Layer verified</td>
</tr>
</tbody>
</table>

Table 2  Extended Enterprise Wireless Platform

<table>
<thead>
<tr>
<th>Role</th>
<th>Cisco Platforms</th>
<th>Version</th>
<th>Description</th>
<th>CVD Verified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-Fabric AP</td>
<td>AP1560</td>
<td>AireOS 8.8.100.0</td>
<td>Rugged outdoor 802.11ac Wave 2 AP, supports up to 1.3–Gbps data rates with 3 x 3 MIMO</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>AP 1542d</td>
<td>AireOS 8.8.100.0</td>
<td>Rugged outdoor 802.11ac Wave 2 AP, supports up to 867–Mbps data rates with 2 x 2 MU–MIMO</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>AP 1542i</td>
<td>AireOS 8.8.100.0</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>IP Video Surveillance Camera</td>
<td>CIVS-IPC-8030</td>
<td>1.0.8</td>
<td>Outdoor 5MP HD IP Camera, up to 60 fps, supports infrared</td>
<td>Yes</td>
</tr>
</tbody>
</table>
**Tech Tip:** Cisco Industrial Wireless 3700 Series will be supported by Cisco DNA Center in an upcoming road map.

**Table 3  Enterprise Network Components involved in Validation**

<table>
<thead>
<tr>
<th>Role</th>
<th>Cisco Products</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Access Layer</td>
<td>Cat 9300</td>
<td>IOS-XE 16.6.5</td>
<td>480 Gbps stacking bandwidth. Sub-50-ms resiliency. UPOE and PoE+. 24-48 multigigabit copper ports. Up to 8 port fiber uplink. AC environment.</td>
</tr>
<tr>
<td></td>
<td>Cat 9400</td>
<td>IOS-XE 16.6.5</td>
<td>--</td>
</tr>
<tr>
<td>Enterprise Core Layer</td>
<td>Cat 9500</td>
<td>IOS-XE 16.6.5</td>
<td>Core and aggregation. Software-Defined Access Cisco StackWise®</td>
</tr>
<tr>
<td>NGFW</td>
<td>FW2140</td>
<td>--</td>
<td>U - 44 core, L - 56 core</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.2.10</td>
<td>2x Two 10 Gbps Ethernet ports, One 1 Gbps management port</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</td>
</tr>
<tr>
<td>Cisco Identity Services Engine (ISE)</td>
<td>Cisco SNS-3515 and SNS-3595 Secure Network Server</td>
<td>ISE 2.4 Patch 5</td>
<td>Policy Engine</td>
</tr>
<tr>
<td>Wireless Controller</td>
<td>Cisco WLC 5520</td>
<td>AireOS 8.8.100.0</td>
<td>Wireless Controller</td>
</tr>
</tbody>
</table>

**Extended Enterprise Design Overview**

The enterprise can be SD Access Fabric enabled or Non-Fabric. Some deployments can have a combination (as shown in Figure 6). This CVD discusses the Non-Fabric Enterprise design with the Cisco DNA Center and its Enterprise Extension to non-carpeted areas. All sections in the remainder of this document discuss the non-fabric design details.

**Figure 6  Enterprise Network Design having both SD Access Fabric and Non-Fabric**
The Cisco DNA Center-managed, Non-Fabric Enterprise follows a standard architecture similar to the one published in the Cisco Enterprise Network CVD and Campus Wired and Wireless LAN CVD. The design enables wired and wireless communications between devices in an outdoor or a group of outdoor environments, as well as interconnection to the WAN and internet edge at the network core.

Reference: Cisco Enterprise Network Design Guide:

Campus Wired and Wireless LAN website:

The internet connection is protected with a Cisco Next Generation Firewall (NGFW). The Cisco NGFW 2140 model can be used as the NGFW.

Each building floor/geographic location will have an enterprise access switch (C9300), preferably a stack of two. Ruggedized IE switches are configured as Extended Enterprise access nodes, which connect to the enterprise access switch and thus extend the enterprise network to non-carpeted space. Both wireless and wired connectivity are provided in the Extended Enterprise region. A Wireless controller (WLC) is located centrally connecting non-fabric AP from both the enterprise and the extended enterprise. The AIR-CT5520 is the recommended model for WLC. As recommended in the Cisco DNA Center User Guide, it is desirable to have less than 20ms latency between the AP to WLC, and the network latency from the Cisco DNA Center to any fabric edge should be within 50ms.

Reference: Cisco Digital Network Architecture Center User Guide, Release 1.2.10

Security and QoS policies are applied uniformly, providing uniform treatment for a given service across the Enterprise and Extended Enterprise network. Controlled access is given to shared services and other internal networks by appropriate authorization profile assignment.

Redundancy is provided for devices and links at various levels, details are covered in Extended Enterprise High Availability, page 46.

Extended Enterprise Access Network Topologies

IE switches are connected either directly or in a hierarchical manner in a star topology to the enterprise network edge switches. Based on availability of ports on the access switch and IE switch models, both fiber and copper uplinks can be used.

Star Topology

Access switches connecting in a star topology are shown in Figure 7. Two possible designs are listed below:
- Access layer IE switches connecting directly to the enterprise distribution switches representing a single level hierarchy.
- The IE switches form a multi-level hierarchy, namely aggregation and access.

Large deployments that add an aggregation layer provide better scalability and coverage. The Cisco Catalyst IE3400, Cisco IE4000, and Cisco IE5000 series switches can play the role of the aggregation layer, as shown in Figure 7. Aggregation switches can connect with the distribution layer over fiber; therefore, they can extend to a large distance and provide higher bandwidth. Figure 7 shows the IE switches connected in a hierarchical star topology. All switches in IE series can be deployed at the access layer.
For uplink redundancy, two kinds of designs are shown, suiting to two different layers (aggregation and access).

- At the aggregation level, multiple uplinks of an IE switch can connect to multiple distribution layer switches arranged in a stack. The distribution layer switches can configure StackWise redundancy. Enable port channel. The two links at the stack are seen as a single link. Load balancing and loop avoidance are dealt with automatically.

- At the access layer, multiple uplinks of an IE switch can connect to multiple aggregation layer switches. Loop avoidance is ensured with the help of Flex Link which has faster convergence than spanning tree.

Figure 7  Extended Enterprise Access and Aggregation Layer in Star Topology

Extended Enterprise Wired Access

The enterprise wired access and aggregation network shown in Figure 7 is extended to the outdoor using the ruggedized Cisco IE2000, Cisco Catalyst IE3X00, Cisco IE4000, and Cisco IE5000 switch series, which can be connected to the enterprise network in any topology as long as they are reachable from the Cisco DNA Center and meet the latency requirements. This is called the extended wired access layer. By choosing appropriate switch models, both copper and fiber access can be provided. All IE switches are managed by the Cisco DNA Center and, just like with any Catalyst switches, all Cisco DNA Center features such as discovery, inventory, topology, Software Image Management (SWIM), Assurance, and Application policy apply to these switches and hosts connected to these switches.

Various access layer features such as multiple access ports, copper/fiber access ports, PoE/PoE+, multi-GB access and uplink, port-security, and TrustSec are supported. See Extended Enterprise Security Policy Design, page 25 for details on access ports security.
Extended Enterprise Wireless Access

Extended Wi-Fi wireless access is provided in the Extended Enterprise region using outdoor access points having Cisco DNA Center support such as the AP1560 series and AP1542 series. They can be connected to any access/aggregation Industrial Ethernet switch in the extended access, to provide wireless connectivity in the outdoor non-carpeted area. The APs form a CAPWAP tunnel with the WLC and all wireless data, control and management flow through the CAPWAP.

Extended Enterprise Wireless Access Design Considerations

- Extended Enterprise wireless access spans across multiple building and geographies
- High speed wireless access in the non-carpeted space:
  - Ruggedized outdoor APs
  - Support for 802.11ac Wi-Fi
  - Support for both 2.4GHz and 5GHz
- Uniform wireless across carpeted and non-carpeted space:
  - Same SSID across carpeted and non-carpeted space
  - Same user-credentials across carpeted and non-carpeted space
  - Provision for exclusive SSIDs in non-carpeted space
  - Configurable authorization policy
  - Seamless mobility between carpeted and non-carpeted space
- Support for both voice and data services
- Support for PoE power for APs
- Support for Guest wireless
- Fast lane (priority treatment for iOS endpoints) and fast-transition (feature for fast roaming) to be supported

Extended Enterprise Wireless Deployment Model

Two types of deployment models and their recommended use are discussed in this section:

- Centralized (Local-Mode) wireless design
- FlexConnect wireless design

Centralized (Local-Mode) Deployment Model

This is also known as local-mode deployment model. In a centralized/local-mode deployment model, the WLAN is centrally located. All APs are connected to WLAN over a high-speed low-latency link. APs form a CAPWAP tunnel with WLAN. All wireless traffic (data, control, and management) from the APs is tunneled to the WLC. WLC is the single point of management for managing Layer 2 security and wireless network policies.

In a centralized deployment model, with the help of Cisco DNA Center and ISE, the policies can be applied in a consistent and coordinated manner across wired and wireless networks. It also greatly simplifies management by automation.
In addition to the traditional benefits of a Cisco Unified Wireless Network, the local-mode design provides the following features:

- Centralized IP address management, simplified configuration, and troubleshooting
- Seamless mobility, fast roaming and roaming at scale support: users remain connected to their session even while walking between various enterprise and extended enterprise zones with changing subnets
- Can support rich media such as voice with call admission control
- Centralized policy enables application inspection, network access control, policy enforcement, and accurate traffic classification

This centralized/local-mode deployment model is the default Cisco CVD validated recommended deployment model for Extended Enterprise wireless access.

**Cisco FlexConnect Local Switching Deployment Model**

In a specific use-case, where several small remote locations having WAN connectivity to the central location with <100ms latency exist, the FlexConnect local switching deployment model can be used. Typically, this applies to enterprises having a central site and several small remote branch sites.

The key features for FlexConnect local switching deployment model are:

- Cost-effective solution, helping enable enterprises to configure and control remote-site APs from the headquarters through the WAN, without deploying a controller in each remote site
- APs can switch client data through local wired network
- Only guest wireless, control traffic and Internet traffic are tunneled to centralized WLC over CAPWAP

Either a dedicated FlexConnect WLC or a shared WLC controller can be used to manage FlexConnect mode APs in the network. A list of recommended WLC models and comparison is given in Table 5.

**Guest Wireless**

Guest wireless traffic needs to be treated distinctly in the enterprise network:

- Provide guest Internet access through an Open Wireless SSID, with web authentication access control
- Define guest access policy having access only to Internet
- Guest access policy should not have access to any internal network
- Guest access can be provided both in Centralized and FlexConnect deployment models

**Security for Wireless Clients**

SSIDs can either be shared or exclusive between the Enterprise and Extended Enterprise network. In case of shared SSID, seamless roaming will be supported between the Extended Enterprise and the Enterprise network.

Wireless clients/users are mapped to user groups at ISE and authorization is defined for each user group. This holds true both for wireless and wired groups keeping their credentials and access rights the same. Wireless users get the same access rights as they roam around Extended Enterprise and Enterprise network. WLAN controller forwards the wireless packets to the shared services switch for authorization policy enforcement. The switch gets IP-SGT mapping and authorization policy from ISE and enforces policy based on the source and destination IP-SGT. This applies to east-west and north-south traffic in both directions. Security enforcement for Internet traffic is done by the security firewall.

Details on security are elaborated in Securing Wireless Access Endpoints, page 36.
Choice of Access Points

The Cisco DNA Center-supported outdoor Cisco Aironet access points are the Cisco AP1540I, Cisco AP1540D, and Cisco AP1560 series. Table 4 shows comparisons for helping select a model. Some of the key considerations are:

- If 802.3at Power over Ethernet (PoE+) is the source of power, the 1562I radios will shift from 3x3 MIMO to 2x2. This will reduce the data rate in the 2.4 GHz radio. For full functionality, direct (AC/DC) power supply is needed.

- The SFP uplink supported by AP1562 series can be used when the AP distance from the IE access switch is longer. This will require the SFP port at the IE access switch.

Table 4 Comparison of APs for Extended Enterprise Use

<table>
<thead>
<tr>
<th></th>
<th>Aironet 1540I</th>
<th>Aironet 1540D</th>
<th>Aironet 1562E</th>
<th>Aironet 1562D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radio Specifications</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Antenna type</td>
<td>Internal, wide</td>
<td>Internal, narrow</td>
<td>Dual-band or single-band, software-configurable</td>
<td>Internal, directional</td>
</tr>
<tr>
<td>Wi-Fi standards</td>
<td>802.11a/b/g/n/acW2</td>
<td>802.11a/b/g/n/acW2</td>
<td>802.11a/b/g/n/acW2</td>
<td>802.11a/b/g/n/acW2</td>
</tr>
<tr>
<td>Data rate</td>
<td>300 Mbps</td>
<td>300 Mbps</td>
<td>867 Mbps</td>
<td>867 Mbps</td>
</tr>
<tr>
<td>Radio design (Tx-Rx:SS)</td>
<td>2x2:2</td>
<td>2x2:2</td>
<td>2x2:2</td>
<td>2x2:2</td>
</tr>
<tr>
<td>RF interference avoidance</td>
<td>-</td>
<td>-</td>
<td>CleanAir</td>
<td>CleanAir</td>
</tr>
<tr>
<td>Maximum clients</td>
<td>400</td>
<td>400</td>
<td>400</td>
<td>400</td>
</tr>
<tr>
<td>Backhaul</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fiber SPF optics</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>LAN port/PoE out (802.3af)</td>
<td>1 GE (PoE in) port</td>
<td>1 GE (PoE in) port</td>
<td>SFP-based LAN port</td>
<td>SFP-based LAN port</td>
</tr>
<tr>
<td>Cable modem</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>DOCSIS/EuroDOCSIS 3.0</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Power and Environment</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Power options</td>
<td>PoE, 802.3af</td>
<td>PoE, 802.3af</td>
<td>48 VDC, PoE</td>
<td>48 VDC, PoE</td>
</tr>
<tr>
<td>Temperature range</td>
<td>-40 to 65°C</td>
<td>-40 to 65°C</td>
<td>-40 to 65°C</td>
<td>-40 to 65°C</td>
</tr>
</tbody>
</table>

Reference: Cisco Compare Outdoor Access Points

Choice of Wireless LAN Controller

Table 5 is a comparison chart of Cisco DNA Center-supported WLC models. Depending on the deployment needs, the appropriate model can be selected from the table. Refer to Extended Enterprise Scale and Dimensioning, page 48 for WLC selection based on size.

<table>
<thead>
<tr>
<th>WLC Model</th>
<th>Deployment Model</th>
<th>Preferred Topology</th>
<th>Maximum APs</th>
<th>Maximum Clients</th>
<th>Throughput</th>
<th>HA Stateful Switchover (SSO)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 8540</td>
<td>Centralized or FlexConnect</td>
<td>Large Single or Multiple Site</td>
<td>6000</td>
<td>64000</td>
<td>40 Gbps</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco 5520</td>
<td>Centralized or FlexConnect</td>
<td>Large Single or Multiple Site</td>
<td>1500</td>
<td>20000</td>
<td>20 Gbps</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco 3504</td>
<td>Centralized or FlexConnect</td>
<td>Small Local Controller Site</td>
<td>150</td>
<td>3000</td>
<td>4 Gbps</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Extended Enterprise Endpoints

The devices that connect to the extended access layer are the extended enterprise endpoints. These endpoints may be either wired or wireless clients. Different Extended Enterprise endpoints include security camera, IP Phone, user laptop, tablet, or mobile phone connected to the network. The wireless endpoints can roam across Enterprise and Extended Enterprise locations. Operators would prefer to have a seamless experience as they roam while having minimal complexity. Due to its physical nature of being out of the carpeted space, a higher threat for attacks and spoofs originating from external enterprise endpoints exist. The solution will address this security demand.

Extended Enterprise Application Servers Network

Figure 5 shows the “application servers network” block as part of the overall Extended Enterprise network diagram. Application servers are dedicated for specific services; for example, 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.

Application servers can be connected with a regular Cisco DNA Center-supported switch such as the Catalyst 9300 or with a data center switch such as the Nexus 5000/7000. Each server can be configured to be part of a specific access group (SGT) by IP-SGT mapping at ISE. The switch receives source and destination SGT using the SXP protocol from ISE. Similarly, the switch also receives group-based access policies from ISE. The switch applies access policy to all traffic destined to the application servers. For all traffic originated from application servers, source SGT tagging and policy enforcement are done by the switches.

If a limited number of application servers exist, the SG Ts can be statically assigned. This ensures that only clients having access to a specific application server are provided access. As a prerequisite, an underlying Layer 3 reachability is to be ensured from all clients to the server.

Extended Enterprise Shared Services

Shared services are common for the entire network and accessible by devices/clients across the Enterprise and Extended Enterprise. Communication between shared services and the SG Ts are selectively enabled by appropriate routing. To provide uniformity and seamless management, the Extended Enterprise can leverage the shared services network of the enterprise. Different shared services leveraged by the Extended Enterprise include the Cisco DNA Center, ISE, IPAM, DHCP, DNS, and NGFW. Figure 5 shows the shared services block in the enterprise network. No VLANs or SG Ts need to be assigned to these servers.
Extended Enterprise Security Policy Design

This section covers the security considerations and design in the Extended Enterprise context, and also discusses the role of Cisco DNA Center in securing the network.

The Rationale for Securing the Extended Enterprise Network

The common security principles for securing the Extended Enterprise network include visibility (see everything that is happening), segmentation (control the network flows), and detection of unusual behavior. Adopting these principles to secure the Extended Enterprise network is important for the following reasons:

- The wired or wireless endpoints attached to the Extended Enterprise access layer have the potential risk of infecting the enterprise endpoints in the network. Therefore, the endpoints in the Extended Enterprise must be on-boarded in the same way endpoints are on-boarded in the enterprise network. The on-boarding process involves identifying and authenticating the device.

- Endpoints in the Extended Enterprise must be able to access the internet to either download software or to report data to a cloud-based application, which introduces risk of infection from external malicious entities. To help reduce this risk, traffic from the Extended Enterprise to the internet must be monitored.

- Endpoints in the Extended Enterprise are susceptible to vulnerabilities and therefore must be updated periodically to help mitigate the risk of infection.

- Enterprise endpoints can potentially spread infection to extended endpoints; therefore, only allowing traffic that is required can help reduce this risk.

- Data center servers can also propagate infection to endpoints, whether on the Enterprise or Extended Enterprise network. Monitoring these communications and enabling security controls can help protect these communications.

- Network access can be mismanaged, potentially allowing unauthorized access from the Extended Enterprise network into the greater enterprise network.

Visibility

In the Extended Enterprise design, the Cisco ISE profiling feature provides visibility and classification of the endpoints connected to the network. Using MAC addresses as the unique identifier, ISE collects various attributes for each network endpoint to build an internal endpoint database. ISE collects this information by different probes such as DHCP, HTTP, RADIUS, SNMP, Active Directory, NetFlow, DHCP SPAN, and pxGrid. After collecting endpoint information, ISE begins the classification process. The classification process matches the collected attributes to pre-built or user-defined conditions, which are then correlated to an extensive library of profiles. These profiles include a wide range of device types, including mobile clients (iPads, Android tablets, Blackberry phones, and so on), desktop operating systems (Windows, Mac OS, Linux, and others), and numerous non-user systems such as printers, phones, cameras, and game consoles.

In addition, access layer switches provide visibility with the Cisco device sensor feature. The device sensor is used to gather raw endpoint data from network devices, which helps complete the device profile. A device with sensor capability gathers endpoint information from network devices using protocols such as Cisco Discovery Protocol, LLDP, and DHCP, subject to statically configured filters, and makes this information available to its registered clients in the context of an access session. The clients of device sensor could be internal clients or external clients. In the Extended Enterprise design, the ISE analyzer will use RADIUS accounting to retrieve additional endpoint data.
Visibility Design Considerations

The following are key design considerations for visibility of the endpoints and networking devices:

- The visibility of the device should work dynamically whenever a device is attached to the network, removed from the network, or replaced with a different type of a device. For example, an attacker can replace an authenticated device and can make use of the privileges given to the previous endpoint. In that scenario, the network must be able to detect a change and dynamically apply a new policy without any manual intervention.

- The device attributes such as make, vendor, version, serial number, and other relevant information must be obtained by the network whenever an end device is connected. It is recommended not to deploy an endpoint that does not provide the device identification attributes when queried by the networking device. These attributes are critical for designing a secure network and access policy.

- The administrator must have visibility into devices present in the network, and every networking device attached to the network must be authorized and provisioned. This requirement is critical to avoid the addition of rogue devices in a network. For example, a rogue access point deployed successfully in the Extended Enterprise may act as man-in-the-middle to intercept communication in the network.

Segmentation

Segmentation is a practice of zoning the Extended Enterprise network to create smaller domains of trust to help protect the network from the known and unknown risks in the network. Cybercriminals study ways to infiltrate the network by looking at the most vulnerable point. Segmentation helps to prevent the spread of the infection and limits it only to endpoints that an infected host can reach. Segmentation can be categorized as network-based segmentation and custom contracts. Custom contracts are an additional layer of policy enforced on top of the network segmentation. The network segmentation defines the reach of an endpoint and custom contracts define which applications are permitted or prohibited. This feature enhances the security posture because it restricts communications. For example, a camera that is allowed to communicate with a server over HTTP could become infected and attempt to scan the server. The custom contract would prohibit the activity outside of the scope of normal use.

The segmentation between different locations in the Extended Enterprise network is typically done using VLANs with ACLs at the Layer 3 distribution switch. Many benefits are associated with segmentation, such as creating functional areas (building block approach for scalability), creating smaller connected LANs for smaller broadcast or fault domains and smaller domains of trust (security groups), and helping to contain any security incidents. For example, if there is a security group access policy to restrict the communication between the VLANs, traffic from an infected host is contained within the VLAN. However, as the size of the ACL increases, the complexity of managing the ACL also increases.

The concept of network segmentation is not new, but it has evolved significantly beginning with the invention of Virtual LANs (VLANs) about 20 years ago. Initially, network segmentation was defined as the process of breaking up one “flat” network or broadcast domain into smaller segments through the use of VLANs. The original intent was to improve the overall performance of not only the network itself, but also the endpoints by minimizing the number of broadcasts devices had to process.

However, as time went on, network segmentation through the use of VLANs was implemented for security reasons—the ability to limit communications between segments through the use of ACLs to enforce a business-related policy. VLANs initially provided a very basic means of isolating one segment (VLAN) and its devices from another. Private VLANs later provided a form of micro-segmentation, by further restricting communications within a VLAN.

Over the last ten years, Cisco developed the Cisco TrustSec technology that ultimately redefined the term “network segmentation.” With TrustSec, segmentation is no longer performed based on VLANs or VRFs with IP addressing and routing. Instead, TrustSec relies on the use of role- or group-based membership, irrespective of IP addressing, to create policies allowing for segmentation of the network.
Segmentation Design Considerations

A network segmentation strategy developed to enforce security policy in support of an organization's business requirements is typically not limited to a single location. It could be needed across a campus consisting of multiple buildings with thousands of devices or across remote sites such as stores or branches, each with a handful of devices. A given network segment and the policies it represents may be extended anywhere within an organization where one of the business-relevant applications or functions reside.

Segmentation in the extended enterprise is done using Security Group Tags (SGTs). The key design considerations are the following:

- Define tags based on the device type or user profile. For example, all cameras can be defined as a group and all the users belonging to particular job profile can be classified as another group.
- Define the group tags in a central location using the Cisco DNA Center rather than deploying locally on the endpoints using a command line interface.
- Limit the number of tags to a number that is manageable. Having too many tags will make it harder to manage a large policy matrix. On the other hand, merging a lot of profiles into a smaller number of tags may result in not having a granular policy control.

TrustSec Overview

TrustSec technology assigns SGTs to wired or wireless endpoints, networking devices, and users when they connect to a network. By using these tags, an IT security architect can define an access policy and enforce that policy on any networking device. TrustSec is defined in three phases: classification, propagation, and enforcement.

Classification

When users and endpoints connect to a network, the network assigns them a specific SGT in a process called classification. In the classification process, authentication and authorization policies determine the SGT applied to the endpoint. For example, an endpoint in an extended enterprise can be classified and assigned a specific tag if the endpoint is a camera, sensor, phone, or a workstation. The process of SGT assignment is similar to how a dACL is pushed to the Cisco distribution switch when a camera asset is attached to the networking device. The only difference is that instead of a dACL, an SGT value is assigned.

Propagation

The SGT tag information is propagated in TrustSec via two methods: inline tagging and SXP tunnels.

- In the inline tagging method, the SGT tag is inserted as part of the Ethernet frame and sent from one switch or router to another device. The SGT tag that is assigned to the endpoint must propagate along with every packet generated by the endpoint. Each switch configured with SGT in-line tagging along the route propagates the same frame to the next switch and this information travels in hop-by-hop fashion to the destination.

- The second method for SGT propagation is using an SXP tunnel. This method is used when one or more devices in the path of communication does not support in-line tagging. In that scenario, the non-SGT-capable switch would ignore the SGT in the frame and would send a normal Ethernet frame on the out-going interface. In other words, for in-line tagging feature to work, all the switches in the path must support this feature. To circumvent that problem, TrustSec also supports a different mechanism to transport SGT frames over a path when a non-SGT capable networking device is present in the path from source to destination by using SXP. SXP is used to securely share SGT-to-IP address mapping.
Enforcement

The third stage of Cisco TrustSec is policy enforcement. The enforcement device controls traffic based on the tag information. A TrustSec enforcement point can be a Cisco firewall, router, or switch. The enforcement device takes the source SGT and compares it with the destination SGT to determine if the traffic should be allowed or denied. The advantage of TrustSec is that any switch, router, or firewall between the source and the destination can impose the policy, but the essential requirement is that the enforcement point must be able to map the destination IP address to the tag value.

Cisco TrustSec Design Considerations

As explained in TrustSec Overview, page 27, three important considerations should be taken when designing the TrustSec policy in the Extended Enterprise such as defining the SGT groups, propagation method, and enforcement point.

The first method is to classify a similar set of devices into an SGT group. For example, all cameras are assigned an SGT value 5 and all contractors are assigned an SGT value of 7. In our design, we have wired endpoints and wireless endpoints; therefore, an employee is assigned the same tag if they are connected by either wired or wireless access.

---

The group assignment is done in the Cisco DNA Center and the information is sent to the Cisco ISE using REST API between the Cisco DNA Center and Cisco ISE.

The second consideration is how to propagate the SGT tag information in the network. In this design, we have chosen to use SXP as the means to send SGT information from source to destination for the following reasons:

- Certain Industrial Ethernet (IE) switches don’t support in-line tagging. To understand the Cisco TrustSec capabilities for IE switches, please refer to the Cisco TrustSec 6.4 Platform Capability Matrix at the following URL: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/trustsec-6-0-platform-capability-matrix.pdf. All the IE switches can assign an SGT value to an endpoint attached to the access layer switch.
In this design, all the endpoints are authenticated to ISE by using either dot1X or MAB protocol. Therefore, ISE derives all the binding information through the RADIUS session between the networking devices and ISE.

ISE can propagate this binding information to any enforcement point in the network. The advantage of this method is consistent delivery of SGT to IP mapping information to any enforcement point in the network. In this design, the SXP tunnel established between ISE and the distribution switch allows a distribution switch to receive binding information from ISE, as shown in Figure 9:

Figure 9 SXP Tunnel Information between ISE and the Distribution Switch

The third consideration is to choose an enforcement point. In the Extended Enterprise design, we have chosen the distribution switch as an enforcement point for the following reasons:

- When a network device is defined in ISE for TrustSec policy enforcement, as the network device learns mapping information for an SGT, it will communicate with ISE to get the policies associated with that SGT as a destination. SGACLS downloaded to routers and switches consume resources, and numerous SGTs with their associated policies may lead to heavy memory usage in routers and Ternary Content Addressable Memory (TCAM) exhaustion in switches. Ultimately, some SGACLS may not be installed.

- Network devices have well-defined limits as to the number of IP to SGT mappings they can store. These mappings will consume memory as the numbers of mappings increase. If the supported numbers are exceeded, mappings will not be installed in memory and, as a result, policies specific to those mappings will not be enforced.

- The distribution switch in our Extended Enterprise design has enough TCAM resources to support a large SGT to IP binding information table. However, some of the IE switches in the Extended Enterprise don’t support enforcement capability, which limits enforcing at the access layer. Thus our design classifies at the access layer switch and enforces policy at the distribution switch.
Design the Security Policy in Extended Enterprise Network

In this section, we discuss the extended enterprise network security policy design.

Network Policy Profiles in Extended Enterprise

In the extended enterprise design, the Cisco DNA Center and Cisco ISE work in unison to provide the automation for planning, configuration, segmentation, identity, and policy services. ISE is responsible for device profiling, identity services, and policy services, dynamically exchanging information with Cisco DNA Center. The Cisco DNA Center consists of the automation and assurance components that work in unison to form a closed-loop automation system, enabling the configuration, monitoring, and reporting required to realize the full extent of the Cisco intent-based networking in campus environments.

When the Cisco DNA Center is implemented, ISE is still deployed as a separate appliance providing identity and policy services for the extended enterprise network. When creating SGTs through the Cisco DNA Center user interface, the ISE user interface is cross-launched; ISE maintains all of the scalable group information later used in Cisco DNA Center for policy creation. Although the policies and corresponding contracts are created in the Cisco DNA Center, both are communicated back to ISE through REST API calls. ISE then serves as the single point of reference for SGTs, policies, and contracts (SGACLs), which are then dynamically distributed to the network infrastructure.
Figure 11 shows an example of how policy is defined in the Cisco DNA Center:

![Cisco DNA Center Policy Example](image)

When defining custom contracts, the administrator must carefully consider the applications and ports that are needed to be allowed for the application to work properly and also filter the other protocols that are not needed for an endpoint and the application server.

User/Device Profiles in Extended Enterprise

This section describes how policy is designed in the Extended Enterprise design. As explained in The Rationale for Securing the Extended Enterprise Network, page 25, as we allow different types of users using different endpoints access network in the Extended Enterprise, the risk of these devices infecting other devices in the network must be mitigated. Policy design helps this objective by clearly defining the roles of the users and providing access only to those services that their business requires. The Cisco DNA Center helps customers to convert business requirements into a consistent policy which could be applied throughout the enterprise. Table 6 is a table of users that we have created as an example that illustrates the key concept and also shows the power of the Cisco DNA Center in orchestrating this policy.
Defining the Security Groups

After defining the high-level policy requirements, the next step is to create scalable group tags. As shown below, a device profiled as “Security” belongs to the security group “SE.” Similarly, a device profiled as “Servers” belongs to the security group “SR.” These groups are created to show an example of how a network administrator can group devices based on the type of profile. By grouping devices based on function, we can design a security policy based on the assigned groups.

Table 6 User/Device Profiles and Their Network Requirements

<table>
<thead>
<tr>
<th>User/Device Profile</th>
<th>Role</th>
<th>Policy Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>This profile belongs to devices that perform security function, for example, cameras. Camera uses wired access to connect.</td>
<td>Must be able to only communicate with a server in the data center. Must not be able to communicate with anything else in the network.</td>
</tr>
<tr>
<td>Employees</td>
<td>This is a user profile associated with employees. Any employee who accesses the network in the Extended Enterprise space must be authenticated and authorized with this profile. The employee can attach with either wired or wireless network access.</td>
<td>The employees must be able to access application servers in the data center. The same access the employees has in the enterprise space must be available when they access in Extended Enterprise network.</td>
</tr>
<tr>
<td>Contractor</td>
<td>This user profile is associated with a contractor who accesses the network in the Extended Enterprise space. The contractor can communicate only with a server in the data center. The contractor is not allowed to communicate with another employee. The contractor uses wired or wireless access.</td>
<td>The contractor is allowed to access certain services in the data center. The contractor must not be allowed to be communicated with any employee endpoints or users.</td>
</tr>
<tr>
<td>Auditor</td>
<td>This user profile is associated with an auditor who is allowed to communicate with other endpoints in the Extended Enterprise for the purpose of ensuring if the network is designed and implemented as per the best practices. The auditor accesses the network by wired or wireless network access.</td>
<td>The auditor is allowed to communicate with other endpoints in the network.</td>
</tr>
<tr>
<td>Server</td>
<td>This device profile is associated with a device which is located in the data center.</td>
<td>The server is allowed to communicate with certain user profiles that need access for their applications to work.</td>
</tr>
</tbody>
</table>

Table 7 Defining Scalable Groups in Cisco DNA Center

<table>
<thead>
<tr>
<th>User Profile</th>
<th>SGT Assigned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>SE</td>
</tr>
<tr>
<td>Servers</td>
<td>SR</td>
</tr>
<tr>
<td>Employee</td>
<td>EE</td>
</tr>
<tr>
<td>Contractor</td>
<td>CO</td>
</tr>
<tr>
<td>Auditor</td>
<td>AU</td>
</tr>
</tbody>
</table>
Defining Group-Based Access Control Policies

After defining the scalable groups, the next step is to define group-based access control policies in the Cisco DNA Center. Table 8 shows an example of these policies. For instance, the intersection of SE and CO is “NO,” which means that the communication between a packet tagged as SE and a packet tagged as CO is prohibited.

Table 8  Defining Group-Based Access Control in Cisco DNA Center

<table>
<thead>
<tr>
<th></th>
<th>SE</th>
<th>CO</th>
<th>AU</th>
<th>EE</th>
<th>SR</th>
</tr>
</thead>
<tbody>
<tr>
<td>SE</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>CO</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>AU</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>EE</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SR</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Securing the Wired and Wireless Network Access

In an enterprise deployment, we assume that a mix of wired and wireless users accessing the network would occur. All the devices either connecting by wired or wireless network access must be authenticated to ISE. The authentication of endpoints typically happens by the 802.1x protocol. However, certain endpoints such as printers and scanners may not support the 802.1x protocol. In that scenario, the access layer switch does authentication by using the MAC Authentication Bypass (MAB) protocol. After successful authentication, the session is checked against an authorization policy, which consists of several rules created in ISE. The end result of the authorization policy could be a VLAN, SGT, dACL, or other elements that could be used to enforce network policy.

This section explains the different traffic flows that could happen in an Extended Enterprise network and how to secure wired and wireless endpoints.

Extended Enterprise Traffic Flows

Three types of traffic flows exist in an extended enterprise network:

- Traffic among the peers in the extended enterprise network, which is known as East-West communication.
- Traffic between a server in a shared service zone to an endpoint in the extended enterprise, which is known as North-South communication.
- Traffic among the wireless endpoints in an Extended Enterprise network.
Figure 12  East-West Traffic Flow in an Extended Enterprise Network
Figure 13  North-South Traffic Flow in an Extended Enterprise Network
Securing Wireless Access Endpoints

Wireless devices should connect to the network infrastructure securely where possible. In an enterprise environment, you should configure WLANs to support WPA2 with AES-CCMP encryption and 802.1x authentication of devices. This is sometimes referred to as the Wi-Fi Protected Access (WPA) Enterprise on wireless devices. 802.1x authentication requires a AAA server (such as ISE) that provides centralized policy-based management and control for end users accessing the wireless network.

The AAA server will implement the RADIUS protocol between itself and the WLC. Authentication of end users is accomplished via an extensible authentication protocol (EAP) session between the wireless device and the AAA server. The EAP session is transported via RADIUS between the WLC and the AAA server. Depending upon the capabilities of the wireless device, the capabilities of the AAA server, and the security requirements of the organization, multiple variants of EAP, such as PEAP and EAP-TLS, may be implemented. PEAP makes use of standard user credentials (userid and password) for authentication. EAP-TLS makes use of digital certificates for authentication. It is highly recommended that you deploy redundant AAA servers for high availability if one or more servers become temporarily unavailable. Often the AAA server is configured to reference an external directory or data store such as Microsoft Active Directory (AD). This allows the network administrator to leverage existing AD credentials instead of duplicating them within the AAA server. This can also be extended to provide role-based access control (RBAC) for end users through the use of AD groups.
Securing the Wired Endpoints Supporting 802.1x

During 802.1x authentication, the switch or the client can initiate authentication. The switch can be configured to initiate authentication when the link state changes or periodically as long as the port remains up and unauthenticated. The switch sends an EAP-request/identity frame to the client to request its identity. Upon receipt of the frame, the client responds with an EAP-response/identity frame. However, if during bootup, the client does not receive an EAP-request/identity frame from the switch, the client can initiate authentication by sending an EAPOL-start frame, which prompts the switch to request the client's identity.

When the client supplies its identity, the switch begins its role as the intermediary, passing EAP frames between the client and the authentication server until authentication succeeds or fails. If the authentication succeeds, the switch port becomes authorized. If the authentication fails, authentication can be retried, the port might be assigned to a VLAN that provides limited services, or network access is not granted. In the Extended Enterprise design, we have provided a default tag in which minimal access is granted to the user.

Securing Wired Endpoints That Do Not Support 802.1x

As mentioned at the beginning of Extended Enterprise Security Policy Design, page 25, certain wired endpoints don't support 802.1x protocol. When such an endpoint connects to the access layer switch, the switch sends the authentication server (ISE) a RADIUS-access/request frame with a username and password based on the MAC address. If authorization succeeds, the switch grants the client access to the network.

Cisco DNA Center Assurance

In the Extended Enterprise design, we have different types of endpoints—laptops, cameras, phones and different types of users—employee, contractor accessing the network using either wired/wireless means. In such a diverse environment, it is very important to troubleshoot the problems and come to a quick resolution. When an endpoint is unable to connect successfully to the network, many reasons for having a failure could exist such as issues related to authentication service, end point OS problems, and physical network issues. The Cisco DNA Center helps operation teams quickly isolate the root cause of the problem. To obtain more information about Cisco DNA Center Assurance, please visit the Cisco DNA Center Solutions web page at the following URL: https://dnac.cisco.com/dnac-solutions/dna-assurance

Managing Device Software Images

IT teams may need to upgrade software image on networking endpoints, such as access points, switches, and routers to address the following requirements:

- A new feature is available and, to make use of that feature, the image has to be upgraded.
- A new vulnerability is disclosed, and a patch is available as a new image that needs to be installed on all networking endpoints.
- The need to standardize device images among devices to maintain consistency.
- End-of-life notifications.

The Cisco DNA Center provides a software image standardization process that includes:

- Flexible and granular organization of software images and image add-ons.
- Automated device auditing to determine compliance with defined image standards.
- An upgrade process that applies the standards and separates the distribution and activation tasks.

To obtain more information, about the Cisco DNA Center updating software images, please refer to Cisco DNA Center software upgrade training at the following URL:

https://dnac.cisco.com/dnac-solutions/dna-automation#swim
Extended Enterprise Design Guide

System Design

Extended Enterprise QoS Policy Design

This section covers Extended Enterprise QoS design details such as QoS considerations, QoS strategy, design steps, and recommendation for traffic classification and marking.

Extended Enterprise QoS Design Considerations

This section describes the various considerations that an operator must be taking into account while designing a QoS policy for the Extended Enterprise network:

- Classification and Marking at the ingress should be applied to all traffic types in the entire network hierarchy, irrespective of available bandwidth and expected traffic.
- Police traffic by defining QoS exceed policy.
- Shape traffic at the egress on sub-line rate hand-offs and complement these shapers with nested queuing policies.
- Classify IoT control traffic priority similar to network control traffic, IoT poll traffic similar to network management/telemetry data.
- Limit total strict priority queuing traffic (LLQ) to 33% of link capacity, to bound application response time of non-priority applications.
- 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. Based on destination “Server IP/Port or URL.”

Extended Enterprise QoS Design

If AutoQoS is used in the enterprise network, then AutoQoS can also be applied to Extended Enterprise network devices. All IE series switches support AutoQoS. Cisco devices are configured with AutoQoS by default.

Alternatively, the Cisco DNA Center Application Policy may be used to deploy QoS across the networks. However, if the application policy from Cisco DNA Center is used, then AutoQoS needs to be disabled on all the devices.

Extended Enterprise QoS follows the Enterprise QoS designs. The following are the Extended Enterprise QoS design steps:

- List of identified Extended Enterprise services/applications are:
  - Camera - IPVS
  - IP Phone - VOIP
  - Internet access

- When application policy is defined by the Enterprise Cisco DNA Center, enterprise application policy is applied on the distribution switch port to which the Cisco IE5000/4000/3x00/2000 series switches are connected; therefore, QoS treatment is applied to all traffic entering from the IE switches to the distribution switch.

- QoS configuration is defined for IE series switches and pushed through the template to the IE switches as Day-N template.

- The classification, marking and queuing of the enterprise should also be applied in the IE series switches. All flows/applications classified as business relevant should follow Table 9 for classification, marking, and queuing on IE series switches. All flows classified as default are marked as “DF” and all flows marked as irrelevant are marked “CS1.”
### Table 9 Extended Enterprise Traffic Classification and Marking

<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>Extended Enterprise Treatment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relevant Voice</td>
<td>Voice</td>
<td>Expedited</td>
<td>Priority Queuing</td>
<td>VoIP telephony (bearer-only) traffic; for example, Cisco IP phones.</td>
<td>Include as it is</td>
</tr>
<tr>
<td>Broadcast Video</td>
<td>Broadcast Video</td>
<td>Class Selector</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>Include as it is</td>
</tr>
<tr>
<td>Real-time Interactive</td>
<td>Real-time Interactive</td>
<td>CS4</td>
<td>PQ</td>
<td>Inelastic high-definition interactive video applications and audio and video components of these applications; for example, Cisco Jabber and Cisco WebEx.</td>
<td>Not needed, to be dropped</td>
</tr>
<tr>
<td>Multimedia Conferencing</td>
<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 TelePresence.</td>
<td>Include as it is</td>
</tr>
<tr>
<td>Multimedia Streaming</td>
<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 needed, to be dropped</td>
</tr>
<tr>
<td>Network Control</td>
<td>Network Control</td>
<td>CS6</td>
<td>BW Queue only2</td>
<td>Network control-plane traffic, which is required for reliable operation of the enterprise network, such as EIGRP, OSPF, BGP, HSRP, IKE, and so on.</td>
<td>Include as it is</td>
</tr>
<tr>
<td>Signaling</td>
<td>Signaling</td>
<td>CS3</td>
<td>BW Queue and DSCP</td>
<td>Control-plane traffic for the IP voice and video telephony infrastructure.</td>
<td>Include as it is</td>
</tr>
<tr>
<td>Operations,</td>
<td>Operations,</td>
<td>CS2</td>
<td>BW Queue and DSCP3</td>
<td>Network operations, administration, and management traffic, such as SSH, SNMP, syslog, and so on.</td>
<td>Include as it is</td>
</tr>
<tr>
<td>Administration,</td>
<td>Administration,</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>and Management</td>
<td>and Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(OAM)</td>
<td>(OAM)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transactional</td>
<td>Transactional</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>Not needed, to be dropped</td>
</tr>
<tr>
<td>Data</td>
<td>Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Low-Latency</td>
<td>(Low-Latency</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data)</td>
<td>Data)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bulk Data</td>
<td>Bulk Data</td>
<td>AF11</td>
<td>BW Queue and DSCP WRED</td>
<td>Non-interactive (background) data applications, such as email, file transfer protocol (FTP), and backup applications.</td>
<td>Not needed, to be dropped</td>
</tr>
<tr>
<td>(High-Throughput</td>
<td>(High-Throughput</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data)</td>
<td>Data)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Default</td>
<td>Default</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</td>
</tr>
<tr>
<td>Irrelevant</td>
<td>Irrelevant</td>
<td>CS1</td>
<td>Minimum BW Queue (Deferential) and DSCP</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 traffic not categorized</td>
</tr>
</tbody>
</table>
All IE switches support four egress queues. The recommended queuing profile for Cisco IE4000, Cisco 4010, and Cisco 5000 aggregation switches is shown in Table 10:

**Table 10  Traffic Class to Queue Mapping at Cisco IE Switches**

<table>
<thead>
<tr>
<th>Business Relevance</th>
<th>Application Class</th>
<th>Per-Hop Behavior</th>
<th>Queuing and Dropping</th>
<th>Queue Name</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relevant</td>
<td>Voice</td>
<td>Expedited Forwarding (EF)</td>
<td>Priority Queuing (PQ)</td>
<td>Q1 (Priority)</td>
<td>2%</td>
</tr>
<tr>
<td></td>
<td>Broadcast Video</td>
<td>Class Selector (CS) 5</td>
<td>Priority Queuing (PQ)</td>
<td>Q1 (Priority)</td>
<td>25%</td>
</tr>
<tr>
<td></td>
<td>Network Control</td>
<td>CS 1</td>
<td>BW Queue only2</td>
<td>Q2 (CBWF)</td>
<td>WTD</td>
</tr>
<tr>
<td></td>
<td>Signaling</td>
<td>CS3</td>
<td>BW Queue and DSCP</td>
<td>Q2 (CBWF)</td>
<td>WTD - 100%</td>
</tr>
<tr>
<td></td>
<td>Operations, Administration, and Management (OAM)</td>
<td>CS2</td>
<td>BW Queue and DSCP3</td>
<td>Q3 (CBWF)</td>
<td>WTD - 100%</td>
</tr>
<tr>
<td>Default</td>
<td>Default Forwarding (Best Effort)</td>
<td>DF</td>
<td>Default Queue and RED</td>
<td>Q4 (CBWF)</td>
<td>WTD - 60%</td>
</tr>
<tr>
<td>Irrelevant</td>
<td>Scavenger</td>
<td>CS1</td>
<td>Minimum BW Queue</td>
<td>Q4 (CBWF)</td>
<td>WTD - 40%</td>
</tr>
</tbody>
</table>

### Extended Enterprise Network Data Flows

A pictorial representation of device and client onboarding operations, different wired and wireless data flows and role of different network components are shown in this section for readers to more easily grasp the design.

### Extended Enterprise Wired Device Discovery and Plug-and-Play

An Extended Enterprise node can be on-boarded either through a discovery or a PnP process. PnP is a process for onboarding a new device with Zero Touch Deployment (ZTD), with no need for any pre-staging. A pre-staged device can be discovered and added to the Cisco DNA Center-managed network with the discovery process.

PnP provisioning can be for a planned device or unknown device. The planned process can be initiated for a known set of devices.
Figure 15  Extended Enterprise Wired Device Discovery and PnP

Global Configuration 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, SNMP, and NTP
   b. Device credentials: CLI, SNMP, and Https
   c. IP Address Pools

2. Configure DHCP relay/DHCP server in the access switch. Configure Cisco DNA Center IP address in option 43.

Additional Configuration for Planned Device Plug-and-Play Provisioning

3. Upload device identity information for planned list of devices manually one by one, in bulk by uploading from a CSV file, or by fetching from a smart account. Device identity information includes Serial Number, Product ID and optional stack information. Device PnP state set to unplanned.

4. Claim the device following onboarding-workflow, device PnP state is moved to planned.
Onboarding Device with Plug-and-Play

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

6. PnP agent initiates DHCP discovery with option 60 and ciscopnp string and gets the Cisco DNA Center IP address in option 43. PnP agent initiates the PnP process with the Cisco DNA Center using https.

7. 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.

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

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

10. Provisioned devices appear in the Cisco DNA Center inventory, with the last sync status as managed and provision state = not provisioned.

Onboarding a Device Using Discovery

1. Global configuration Steps 1 and 2 at the Cisco DNA Center.

2. Prestaging: Configure discovery credentials on the device (CLI, SNMP, SSH, HTTPS, and NETCONF) and plug in to the access switch having Layer 3 reachability to the Cisco DNA Center.

3. 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).

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

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 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, CTS credentials are also 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 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.
Extended Enterprise Wired Device and Wired Client Onboarding and Data Flows

Startup configurations at the Cisco DNA Center and ISE for device onboarding are shown in Figure 16 and explained in Step 1 through Step 7 below:

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. The operator defines configuration template on the Cisco DNA Center, which contains AAA config, RADIUS config, CTS config, change of authorization (CoA) config, and this entire configuration template is pushed to the networking device during networking device on-boarding.

3. Operator configure group-based access policy (security policy) in the Cisco DNA Center.

4. Cisco DNA Center auto pushes group-based security policy to ISE.

5. ISE pushes the group-based access policy in the form of SGACL to the distribution switch using CTS protocol.

6. Operator using the Cisco DNA Center enables 802.1x/MAB on the access switch port.

7. Operator using the Cisco DNA Center configures DHCP server/relay on the distribution switch.

Figure 16  Extended Enterprise Wired Device Provisioning

Wired client onboarding and data communication flows are shown in Figure 17 and enumerated in Step 8 through Step 19 below:

8. When 802.1x-capable wired client connects to an access layer switch, it triggers 802.1x authentication and access switch forwards the request to ISE/AAA.

9. On timeout (not receiving 802.1x from client), the access switch initiates MAB to ISE.

10. ISE authenticates - does profiling and allocates SGT; SGT is pushed to access switch port to which client is connected.

Figure 17  Wired Client Onboarding and Data Communication Flows
11. 802.1x success message is sent to the client from the access switch.

12. The wired client initiates the DHCP request and receives the IP address.

13. SXP is configured between the ISE as a speaker and the distribution switch as a listener. Whenever a new SGT mapping is learned by ISE, it pushes the binding information (IP-SGT mapping) through the SXP tunnel to the distribution switch, so that the distribution switch can apply the policy.

14. The wired client attached to the access layer switch initiates a data packet to a destination wired end point.

15. The distribution switch tags the packet with Source SGT. It derives the binding information for the destination-wired client from the ISE using SXP protocol.

16. The distribution switch derives a SGACL entry from ISE based on the source/destination SGT, and then takes a forwarding decision (allowed/deny).

17. If source and destination addresses are within the same VLAN and within the same access switch, then the destination is found in the local FDB, packet switched locally with no policy applied.

Figure 17  Extended Enterprise Wired Client Onboarding and Data Flow

Extended Enterprise Onboarding WLAN Controller and Access Points

Startup configurations and steps for onboarding WLC and AP are shown in Figure 18 and explained in Step 1 through Step 13 below:

1. Operator provides global configurations (NW settings – AAA, DHCP, Wireless settings – SSID, WPA2 Enterprise – 802.1x, RF Profile, non-fabric, central mode) are at the Cisco DNA Center.

2. Operator initiates the discovery process for WLC. On discovery, WLC is added to the Cisco DNA Center inventory.

3. Provisioning is initiated for the WLC in the inventory (site-assignment and global-config-deploy).

4. Global-config pushed to WLC.
5. Operator configures a template having “AP-VLAN and enable 802.1x” at Cisco DNA Center and pushes to the enterprise access switch (AP-VLAN assigned to the port where AP is connected).

6. If already associated, WLC pushes 802.1x credentials to AP; otherwise, the operator manually configures on AP.

7. AP initiates 802.1x, access switch forwards the request to ISE.

8. ISE authenticates – does profiling and allocates SGT; SGT is pushed to access switch port to which AP is connected.

9. On successful authentication, AP initiates DHCP and receives WLC IP via option 43.

10. AP establishes CAPWAP with WLC. All future communications from AP (data, control, and management) are sent through the CAPWAP to WLC and then WLC forwards it to the destination. Therefore, unlike wired communication, in this case access switch cannot do tagging and distribution switch cannot do policy enforcement.

11. Operator configures group-based access policy (security policy) in the Cisco DNA Center.

12. The Cisco DNA Center auto-pushes group-based security policy to ISE.

13. ISE pushes the group-based access policy in the form of SGACL to the shared service switch using CTS protocol.

**Figure 18  Extended Enterprise Onboarding WLAN Controller and Access Points**

**Extended Enterprise Wireless Client Onboarding and Data Flows**

Wireless client onboarding and data communication flows are shown in Figure 19 and enumerated in Step 14 through Step 20 below:

14. Wireless client initiates a data traffic to another wireless client either within the same SSID or in a different SSID.

15. Traffic is forwarded by the AP to the WLC over CAPWAP.

16. WLC directs the traffic to the shared services switch for authorization policy enforcement.
17. Shared services switch returns the packet to WLC if authorized.

18. WLC forwards the packet to the destination client via the destination AP/

19. The wireless client initiates a data traffic to a wired client (steps 15 and 16 are followed).

20. Shared services switch forwards the packet to destination via the wired access switch.

Steps for data flow from wireless clients to shared services/application servers follows Step 19 to Step 20 (similar to wireless to wired data flow) above.

**Figure 19  Extended Enterprise Onboarding Wireless Client and Data Flow**

---

**Extended Enterprise High Availability**

High availability (HA) will ensure uninterrupted service. Therefore, HA is needed for every critical component and link in the overall network. This section discusses HA design for the entire solution.

**Extended Enterprise Wired Access/Aggregation Layer Redundancy**

High availability is provided at distribution layer by configuring Cisco StackWise-480. Two aggregation layer switches are configured for redundancy. The aggregation/access switches configure the EtherChannel to connect two links to two switches in the stack. If any of the switches or links fail, the operation will continue with no interruption.

The aggregation layer has Cisco IE switches that do not support StackWise-480. To provide redundancy, Flex Link/STP is configured at the aggregation layer. Flex Links provide link-level redundancy as an alternative to Spanning Tree Protocol (STP). STP is automatically disabled on Flex Links interfaces. Two uplink ports of access switch connect to two aggregation layer switches.

The distribution to core network redundancy is not in the scope of this document.
Extended Enterprise Wireless Access Layer Redundancy

A common way to provide redundancy at the wireless access layer is to do dense deployment of APs or overlap-based deployment. You can ensure each location is covered by more than one nearby access points (preferably 3 nearby APs should cover an area).

Cisco WLC 5520 Redundancy

For high availability of WLC, deploy a pair of controllers in High Availability Stateful Switchover (HA SSO) configuration, as shown in Figure 20. HA SSO model provides box-to-box redundancy with one controller in active state and a second controller in hot standby state. Link Aggregation (LAG) is configured at WLC since LACP and PAgP are not supported by the controller.

In a Cisco DNA Center-managed network, WLC HA SSO pair configuration is done by the Cisco DNA Center. The Cisco Campus-LAN-WAN Design Guide provide details for configuring redundancy for WLC.

Figure 20  WLC HA SSO Link Aggregation

Shared Services Switches Redundancy

All shared services switches are provided with redundancy. Depending on the type of the switch and connected devices, StackWise-480 or EtherChannel or Flex Link or LAG are configured for redundancy.

Shared Services High Availability

Cisco DNA Center Redundancy

Cisco DNA Center redundancy is provided by clustering three Cisco DNA Center appliances together. Clustering provides both a sharing of resources and features, as well as 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 single host cluster only provides software high availability; it does not provide hardware high availability. Thus, we recommend three-host cluster configuration to be used for Extended Enterprise. Detailed configuration is provided in the Cisco DNA Center Administration Guide at the following URL:

Application Servers Redundancy

Depending on the provisioning, UCS server level redundancy and/or application level redundancy can be configured for each application server.

Extended Enterprise Scale and Dimensioning

This section illustrates scaling considerations and available options at different layers of the network and provides steps for computing dimensions for an Extended Enterprise network deployment.

Extended Enterprise Solution Scaling Considerations

The Extended Enterprise solution consists of the Extended Enterprise access, aggregation layer, enterprise distribution, core layer, and the data center layer.

**Tech Tip:** Please refer to appropriate Cisco documentation to compute the scaling details of enterprise layers, which is not part of the scope of this document. Usually the Cisco enterprise layers are highly scalable, thus with appropriate usage/expansion of network devices one can accommodate the Extended Enterprise traffic.

In this section, we cover the scaling details for the access, aggregation layer, and data center layer. The data center layer is a shared service between the Enterprise and the Extended Enterprise. Here, the overall capacity of the data center layers is shown; this section, in conjunction with Extended Enterprise Solution Components, page 17, can help derive the possible scalability of shared services.

Extended Enterprise Access and Aggregation Layer Scaling

The Cisco Industrial Ethernet Portfolio has various features suiting different deployment criteria. The access/aggregation layer switches shown in Table 11 are modular in size with various form factors, port sizes, and features. Thus, the Cisco Extended Enterprise access/aggregation layer is highly scalable from a very small to very large size with a suitable quantity of IE switches and outdoor APs. A comparison of IE switches is given in Table 11 as a reference to select suitable models based on the deployment need.

**Table 11  Cisco Industrial Ethernet Portfolio Comparison**

<table>
<thead>
<tr>
<th>Product Family</th>
<th>Cisco IE2000 IP67</th>
<th>Cisco Catalyst IE3200 series</th>
<th>Cisco Catalyst IE3300 series</th>
<th>Cisco Catalyst IE3400 series</th>
<th>Cisco IE4000 series</th>
<th>Cisco IE4010 series</th>
<th>Cisco IE5000 series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td>Access</td>
<td>Access</td>
<td>Access</td>
<td>Access</td>
<td>Access/Aggregation</td>
<td>Access/Aggregation</td>
<td>Access/Aggregation</td>
</tr>
<tr>
<td>Form Factor</td>
<td>Wall mountable</td>
<td>Fixed DIN Rail</td>
<td>Modular DIN Rail</td>
<td>Advanced Modular DIN Rail</td>
<td>DIN Rail</td>
<td>Rack mount</td>
<td>Rack mount</td>
</tr>
<tr>
<td>Total Ethernet Ports</td>
<td>18</td>
<td>10</td>
<td>Expandable to 26 ports of GE</td>
<td>Expandable to 26 ports of GE</td>
<td>Up to 20 Gigabit Ethernet ports</td>
<td>Up to 28 Gigabit Ethernet ports</td>
<td>28</td>
</tr>
<tr>
<td>PoE/PoE+</td>
<td>Yes (8)</td>
<td>Yes (8)</td>
<td>Yes (up to 24), Power budget - 360W</td>
<td>-</td>
<td>Yes (8 (GE), 240W)</td>
<td>Yes (24), 385W</td>
<td>Yes (12), 360W</td>
</tr>
<tr>
<td>SDA Extended Node</td>
<td>No</td>
<td>No</td>
<td>HW Ready</td>
<td>HW Ready</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SDA fabric Edge node</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>HW Ready</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
Cisco DNA Center Scaling (Shared Service)

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.

Cisco ISE Scalability Considerations

This deployment uses Cisco ISE as the authentication and authorization server for the wired and wireless networks using the RADIUS protocol. Cisco ISE uses Microsoft Active Directory (AD) as an external identity source to access resources such as users, computers, groups, and attributes. Cisco ISE supports Microsoft AD sites and services when integrated with AD.

Cisco ISE is key to the Extended Enterprise solution for providing security services such as profiling endpoints, AAA services to endpoints, and SXP for distributing the binding information. It's important to take into account the following considerations before deploying Cisco ISE:

- The distribution model is a key consideration; the decision lies mainly in the number of endpoints that would need ISE services. The two types of deployment models are standalone and distributed. The standalone deployment model is suited for smaller scale deployment models whereas the distributed model is for large scale deployment models. To obtain more information on the scaling requirements, refer to Table 13.

- The profiling service in Cisco Identity Services Engine (ISE) identifies the devices that connect to your network and their location. The endpoints are profiled based on the endpoint profiling policies configured in Cisco ISE. Cisco ISE then grants permission to the endpoints to access the resources in your network based on the result of the policy evaluation. Cisco ISE has many probes to understand the endpoints attached to the network.

Reference:


<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IE2000 IP67</td>
<td>Yes</td>
<td>374,052 Hours</td>
<td>6,13,125 Hours</td>
<td>6,810,960 Hours</td>
<td>5,572,640 Hours</td>
<td>591,240 Hours</td>
</tr>
</tbody>
</table>
Extended Enterprise Access Layer Dimensioning Calculations

In Table 12, we show the number of access ports and bandwidth requirement for different type of devices and endpoints connected to the enterprise wired access layer. Based on the deployment needs of an Extended Enterprise, you can estimate the number of devices (Camera and APs) and the number of access points needed for a given location. So, by using the information in Table 12, you can compute number ports and bandwidth requirement for an average site of 100 square meters.

Table 12  Devices and Endpoints Access Port Requirement

<table>
<thead>
<tr>
<th>Device/Endpoint</th>
<th>User Traffic Bandwidth</th>
<th>Switch Port Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Camera (covers ~30 meters)</td>
<td>4 to 6 MB</td>
<td>One Fast Ethernet (FE) PoE</td>
</tr>
<tr>
<td>Access Point (covers ~1600 SFT)</td>
<td>Up to 1GB</td>
<td>One Gigabit Ethernet (GE) PoE</td>
</tr>
<tr>
<td>Wireless user</td>
<td>Up to 100MB</td>
<td>NIL</td>
</tr>
<tr>
<td>Wired user</td>
<td>Up to 100MB</td>
<td>One FE Non PoE</td>
</tr>
</tbody>
</table>

In Table 13, we show for a given density of access port and bandwidth requirement the recommended models of the Extended Enterprise access and aggregation switches. The number of sites that can be aggregated by an aggregation level switch and the model of aggregation switch depends on the bandwidth generated by the site locations. If the aggregate bandwidth is up to 4GE, Cisco IE4000 series switches can be used, if the aggregate bandwidth is from 4 to 40GE, Cisco IE5000 series switches should be used as an aggregate level switch.

Table 13  Different Sizing Considerations for an Extended Enterprise Site

<table>
<thead>
<tr>
<th>Density of 100 square meter site</th>
<th>Number of Ports needed</th>
<th>Uplink bandwidth requirement</th>
<th>Recommended access switches</th>
<th>Recommended aggregation switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small density</td>
<td>Up to 8 FE</td>
<td>2GE</td>
<td>IE2000 series/Cisco Catalyst IE3200</td>
<td>IE4000/IE5000 series</td>
</tr>
<tr>
<td>Medium density</td>
<td>Up to 24 FE/GE</td>
<td>2GE</td>
<td>Catalyst IE3300/IE4000 series</td>
<td>IE5000 series</td>
</tr>
<tr>
<td>Large density</td>
<td>More than 24 FE/GE</td>
<td>4 to 40GE</td>
<td>IE4000/IE5000 series</td>
<td>IE5000 series</td>
</tr>
</tbody>
</table>

Refer to Table 5, Wireless LAN Controller (WLC) Model Comparison for dimensioning of the WLC. Due to their scalability and feature support for large centralized (local-mode) designs, the recommended platform of WLC is the Cisco WLC 5520.
Extended Enterprise Single Pane of Glass Management

This chapter is a brief summary of unified management of the Enterprise and Extended Enterprise networks by the Cisco DNA Center, which groups the supported features into Design, Policy, Provision, Assurance, and Platform.

Figure 21 shows different feature groups of the Cisco DNA Center and workflow in performing network operations.

**Figure 21  Cisco DNA Center Workflow**

- **Design Support**
  - Configures device global settings, network site profiles for physical device inventory, DNS, DHCP, IP addressing, software image management, PnP, and user access.
  - **PnP:**
    - Zero touch provisioning: Connect a brand new device to the network having reachability to Cisco DNA Center. The device then is on-boarded.
    - User can define an on-boarding template to be executed as part of the on-boarding workflow.
    - User-defined workflow (site assignment, software image upgrade, and onboarding template) is executed during on-boarding.
    - On-boarded device is added to inventory.
  - **Discovery and Inventory:**
    - Discover a range of devices (Cisco switch, router, and AP) and their topology.
    - Discovered devices are added to inventory.
  - **Cisco DNA Center Inventory:**
    - All devices in the inventory are polled for links, hosts, and interfaces at regular intervals and their status is maintained. The poll interval can vary from 25 minutes to 24 hours. To prevent stale devices, only the devices found active within less than a day are displayed. On an average, polling 500 devices takes approximately 20 minutes.
    - From all active devices in the inventory, several statistics are collected for reporting and assurance.
  - **Provisioning Devices in Inventory:**
    - Day N automation template can be executed on any device.
  - **Topology Design:** Network abstraction and visualization with hierarchical drill-down views.
Summary

- Manage Software Image (SWIM): Cisco DNA Center maintains image repository and maintenance updates (SMUs) for all devices in the network. Cisco DNA Center performs integrity check for the software images stored in the repository. The operator can designate a specific version of software and SMU as a golden image for each device type and role. Cisco DNA Center auto-checks the software version of devices and raises an alert for the device that has an outdated version (not matching golden image). The operator can push software to the desired list of devices. The Cisco DNA Center performs upgrade readiness check before pushing software to the device and checks system state after upgradation.

Policy Support

- Defines business intent for provisioning into the network, policy contract definition for groups.
- Policy-driven security - group-based access policy, policy to users and applications not just device. Cisco ISE is responsible for device profiling, identity services, and policy services, dynamically exchanging information with the Cisco DNA Center.
- Policy-driven QoS defined at Cisco DNA Center is auto-configured in the entire network hierarchy.

Provision Support

- Provision device as per user defined role: provision Cisco Unified Wireless Network wireless and external connectivity. Role-based provisioning in case of fabric site such as creating fabric domains, control plane nodes, border nodes, edge nodes, and fabric wireless.

Assurance Support

- Enables proactive monitoring and insights to confirm user experience meets configured intent, using network, client, and application health dashboards, issue management, and sensor-driven testing.
- Basic Assurance—Assurance then assesses the network and uses context to turn data into intelligence, making sure that changes in the network device policies achieve your intent.
- Advanced Assurance—A health score on the Cisco DNA Center dashboard can help detect performance issues and identify the most likely cause. Several 360-degree view health dashboards are presented in the Cisco DNA Center, namely System-360, Network-360, Device-360, and Client-360.
- Single Pane of Glass—To manage and automate with intuitive workflows and reusable templates.
- Unified Enterprise Network—Covering heterogeneous wired and wireless networks, spanning geographies across buildings and cities.

Platform Support

- Allows programmatic access to the network and system integration with third-party systems using APIs, using feature set bundles, configurations, a runtime dashboard, and a developer toolkit.
- Platform-related features such as intent API to programmatically access network, integrate with third party systems, and support multi-vendor devices.
- Developer toolkit.
- Runtime dashboard showing North Bound Interface and API, events summary.
- Integrates with Cisco and third party applications.

Summary

In summary, the Cisco Extended Enterprise solution enables enterprises to seamlessly extend existing enterprise networks to non-carpeted spaces such as campus parking lots, warehouses, distribution centers, ports, and airports. The solution outlines the steps for both IT and operations teams to accomplish business goals by digitizing the operations in the enterprise outdoor spaces.
Appendix A—Related Documentation

- Cisco Internet of Things Overview:

- Cisco Industrial Ethernet switching product page:

- Cisco Outdoor and Industrial Wireless product page:

- Cisco Extended Enterprise - Getting Started:

- Cisco Intent-Based Networking Overview:

- White paper: Intent-Based Networking and Extending the Enterprise:

- Design Zone for Cisco Enterprise Networks:

- Campus LAN and Wireless LAN Design Guide:

- Software-Defined Access Design Guide CVD, Solution 1.2:

- Software-Defined Access Segmentation Design Guide:
## Appendix B—Glossary

This table lists the acronyms and initialisms used in this document.

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Expansion</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>authentication, authorization, and accounting services</td>
</tr>
<tr>
<td>ACL</td>
<td>access control list</td>
</tr>
<tr>
<td>AD</td>
<td>Microsoft Active Directory</td>
</tr>
<tr>
<td>AES-CCMP</td>
<td>AES-Counter Mode CBC-MAC Protocol (AES - Advanced Encryption Standard)</td>
</tr>
<tr>
<td>AP</td>
<td>access point</td>
</tr>
<tr>
<td>CAPWAP</td>
<td>Control and Provisioning of Wireless Access Points</td>
</tr>
<tr>
<td>CDP</td>
<td>Cisco Discovery Protocol</td>
</tr>
<tr>
<td>ISE</td>
<td>Cisco Identity Service Engine</td>
</tr>
<tr>
<td>NGFW</td>
<td>Cisco Next Generation Firewall</td>
</tr>
<tr>
<td>VNI</td>
<td>Cisco Visual Networking Index</td>
</tr>
<tr>
<td>CoA</td>
<td>change of authorization</td>
</tr>
<tr>
<td>CSV</td>
<td>comma-separated values</td>
</tr>
<tr>
<td>CTS</td>
<td>Clear to Send</td>
</tr>
<tr>
<td>CVD</td>
<td>Cisco Validated Design</td>
</tr>
<tr>
<td>dACL</td>
<td>discretionary access control list</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DNA</td>
<td>Digital Network Architecture</td>
</tr>
<tr>
<td>DNAC</td>
<td>Digital Network Architecture Center</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>DSCP</td>
<td>Differentiated Services Code Point</td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
</tr>
<tr>
<td>EAP-TLS</td>
<td>Extensible Authentication Protocol-Transport Layer Security</td>
</tr>
<tr>
<td>EAPOL</td>
<td>Extensible Authentication Protocol over LAN</td>
</tr>
<tr>
<td>FDB</td>
<td>forwarding database</td>
</tr>
<tr>
<td>HA</td>
<td>High Availability</td>
</tr>
<tr>
<td>HA SSO</td>
<td>High Availability Stateful Switchover</td>
</tr>
<tr>
<td>HSR</td>
<td>High Availability Seamless Redundancy</td>
</tr>
<tr>
<td>HTTP</td>
<td>HyperText Transfer Protocol</td>
</tr>
<tr>
<td>IBN</td>
<td>Intent-Based Networking</td>
</tr>
<tr>
<td>IE</td>
<td>Industrial Ethernet</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPAM</td>
<td>IP Address Management</td>
</tr>
<tr>
<td>IPVS</td>
<td>IP Virtual Server</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>LACP</td>
<td>Link Aggregation Control Protocol</td>
</tr>
<tr>
<td>LAG</td>
<td>Link Aggregation</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Expansion</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LLDP</td>
<td>Link Layer Discovery Protocol</td>
</tr>
<tr>
<td>MAB</td>
<td>MAC Authentication Bypass</td>
</tr>
<tr>
<td>MAC</td>
<td>media access control</td>
</tr>
<tr>
<td>MIMO</td>
<td>multiple input, multiple output</td>
</tr>
<tr>
<td>MU-MIMO</td>
<td>multi-user, multiple input, multiple output</td>
</tr>
<tr>
<td>NBAR</td>
<td>Network-Based Application Recognition</td>
</tr>
<tr>
<td>NETCONF</td>
<td>Network Configuration Protocol</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>PAgP</td>
<td>Port Aggregation Protocol</td>
</tr>
<tr>
<td>PEAP</td>
<td>Protected Extensible Authentication Protocol</td>
</tr>
<tr>
<td>PnP</td>
<td>Plug and Play</td>
</tr>
<tr>
<td>PoE</td>
<td>Power over Ethernet</td>
</tr>
<tr>
<td>PRP</td>
<td>Parallel Redundancy Protocol</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial-In User Service</td>
</tr>
<tr>
<td>RBAC</td>
<td>role-based access control</td>
</tr>
<tr>
<td>REST API</td>
<td>representational state transfer application program interface</td>
</tr>
<tr>
<td>RFC</td>
<td>Remote Function Call</td>
</tr>
<tr>
<td>SD-Access</td>
<td>Software-Defined Access</td>
</tr>
<tr>
<td>SGACL</td>
<td>Security Group ACL</td>
</tr>
<tr>
<td>SGT</td>
<td>Scalable Group Tag</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>SSID</td>
<td>selected service set identifier</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>STP</td>
<td>Spanning Tree Protocol</td>
</tr>
<tr>
<td>SWIM</td>
<td>Software Image Management</td>
</tr>
<tr>
<td>SXP</td>
<td>Security Group Tag Exchange Protocol</td>
</tr>
<tr>
<td>TCAM</td>
<td>ternary content addressable memory</td>
</tr>
<tr>
<td>UCS</td>
<td>Unified Computing System</td>
</tr>
<tr>
<td>VLANs</td>
<td>Virtual Local Area Networks</td>
</tr>
<tr>
<td>VRF</td>
<td>virtual routing and forwarding</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>WLC</td>
<td>Wireless LAN Controller</td>
</tr>
<tr>
<td>WPA</td>
<td>Wi-Fi Protected Access</td>
</tr>
</tbody>
</table>