White paper
Cisco public

The bridge to possible

Intent-Based Networking and Extending the Enterprise

Contents

IoT for Enterprise, Software-Defined Access, and Intent-Based Networking

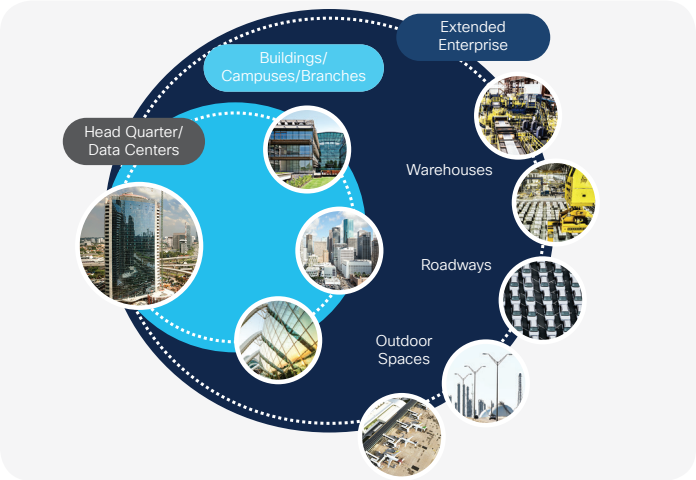
Cisco's Software-Defined Access (SD-Access) solution provides policy-based automation from the edge to the cloud. Secure segmentation for users and things is enabled through a network fabric, drastically simplifying and scaling operations while providing complete visibility and delivering new services quickly. By automating day-to-day tasks such as configuration, provisioning, and troubleshooting, Cisco® SD-Access reduces the time it takes to adapt the network, improves issue resolution, and reduces the impact of security breaches.

Intent-based networking uses the SD-Access solution to deliver a network that has the intelligence and automation to meet an organization's business needs. Intent-based networking applies business intent to network configurations. The intent-based network continuously monitors and adjusts to ensure alignment to business intent. This is achieved through a closed-loop system that includes policy based automation, network analytics, and machine learning.

The business benefits of intent-based networking are speed and agility, an IT staff focused on delivering business value, and a reduced risk of compliance. With increasing use of network-based automation, operational results are achieved faster, issues are contained more rapidly, and downtime is reduced.

Software-Defined Access and Extending the enterprise for IoT

Figure 1. Extending the enterprise with intent-based networking



Network administrators are being asked to extend network connectivity beyond the air-conditioned space more and more to connect and manage Internet of Things (IoT) devices as well as traditional enterprise end devices being deployed in outdoor or extreme-temperature environments (Figure 1). The new types of end devices that connect to an enterprise managed network are coming from other industries. Industrial Programmable Logic Controllers (PLCs), power generation equipment, and robots are just a few examples of new devices making their way into the realm of items managed by enterprise network administrators.

The trend to provide more network connectivity and enable more services beyond the air-conditioned space will only continue.

The SD-Access solution can be extended to manage the ever-increasing presence of outdoor, roadway, and IoT devices. Cisco's vision is to design an enterprise wide solution that not only focuses on policy-based automation and simplified security, but also incorporates the varying needs of the enterprise to manage nonstandard devices (IoT devices). The SD-Access solution is designed in a way that allows for an extension of the SD-Access fabric to easily incorporate and provide services for the IoT devices. Customers can take advantage of Cisco's SD-Access solution to manage not only the network and network devices that are traditionally found in the enterprise, but also nontraditional devices.

Extended nodes

Within the SD-Access solution, the Cisco networking products that connect to the fabric edge devices are called "extended nodes" because they extend the reach of the solution. More on this later. Cisco's Industrial Ethernet (IE) switching products are a great example of providing networking connectivity outside the wiring closet and the SD-Access fabric. The Cisco IE switches are extended nodes.

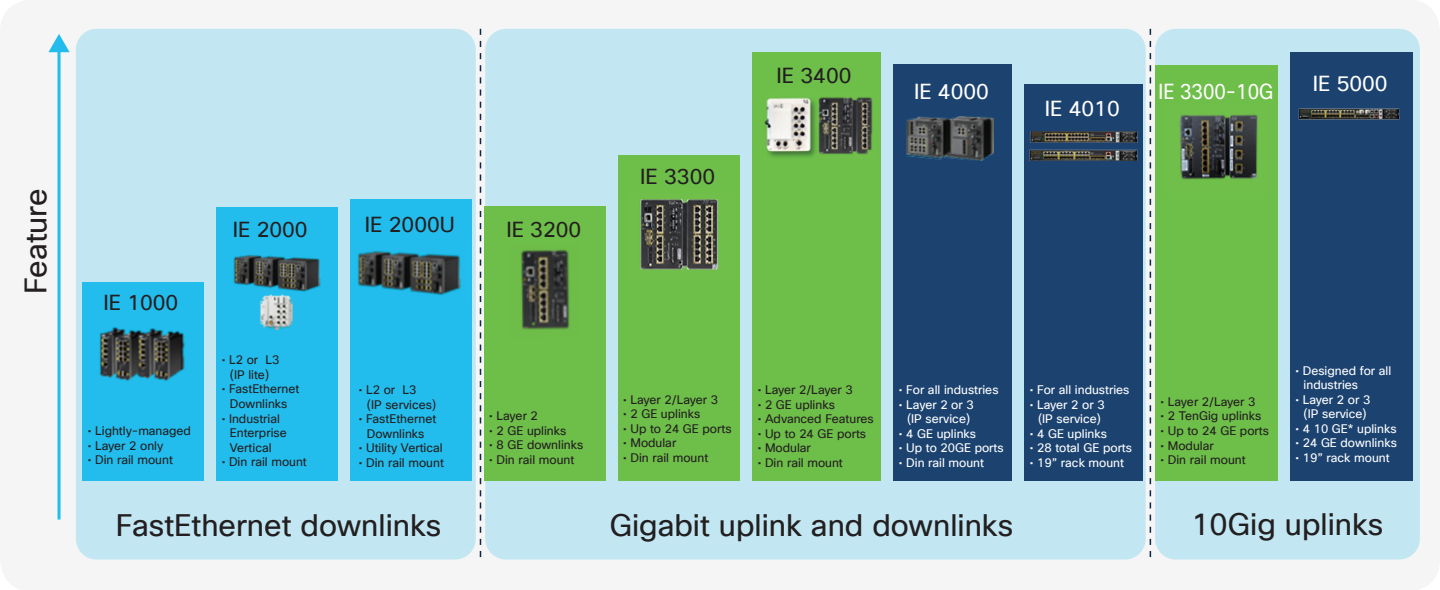
Extended nodes are managed as part of the SD-Access solution by Cisco DNA Center and enjoy all the operational benefits of Cisco DNA Center, such as having policy and intent turned into networking configuration at scale that can be applied to extended nodes. Having this single-pane-of-glass management solution to cover all networking needs saves time and money.

The bridge to possible

Cisco Industrial Ethernet switching portfolio

Cisco provides a comprehensive portfolio of networking devices to enable enterprise network engineers to extend the enterprise network with operational efficiency (Figure 2).

Figure 2. Cisco Industrial Ethernet switching portfolio



Cisco's Industrial Ethernet portfolio has all the quality of Cisco IOS® and IOS XE Software and Cisco networking in a rugged and temperature-tolerant package. The switches are engineered to meet more stringent industry standards and compliance requirements than enterprise-class networking products. The Cisco IE switches operate in very hot (+70°C) and very cold (-40°C) environments and are fanless, making them quiet and able to operate in dusty environments. They support Power over Ethernet (PoE) and come in DIN rail and 19-inch rack-mount form factors. The IE switches run Cisco IOS or IOS XE Software and interoperate with other Cisco networking products. Network engineers can use existing operational processes and procedures to manage the switches.

Software-Defined Access solution overview

What is the Software-Defined Access solution?

As stated earlier, Software-Defined Access is the enterprise networking industry's first intent-based networking solution. It provides automated network management and is a simplified policy-based security platform.

The solution components are divided into the software applications and the physical infrastructure.

The primary software solution components are Cisco DNA Center, the Cisco Identity Services Engine (ISE), and the Analytics and Assurance engine. Cisco DNA Center is the primary application for designing, defining policy, and provisioning the network infrastructure. The ISE provides the security behind the solution. The Analytics and Assurance engine gives insight into network and user performance.

The physical infrastructure is composed of Cisco routers, switches, and wireless access points, as you would expect. This physical layer is also referred to as the underlay. The underlay makes up the physical components of the SD-Access fabric. It is analogous to the traditional Layer 2 and Layer 3 network.

The secret sauce for binding the fabric together is the new and specific capabilities of the network components that enable the SD-Access solution. All network components support a special frame encapsulation and can maintain routing tables and reachability tables based on the encapsulation, as well as support programmable APIs to enable automation. The SD-Access fabric provides a transport layer for all virtualization and protocols. The fabric operates as a logical entity that comprises the physical components. It is a self-contained network entity that provides routing and security for the end devices attached to it. It's easiest to envision the fabric as a single logical entity. It's often depicted as a cloud.

Basic device roles in the SD-Access fabric:

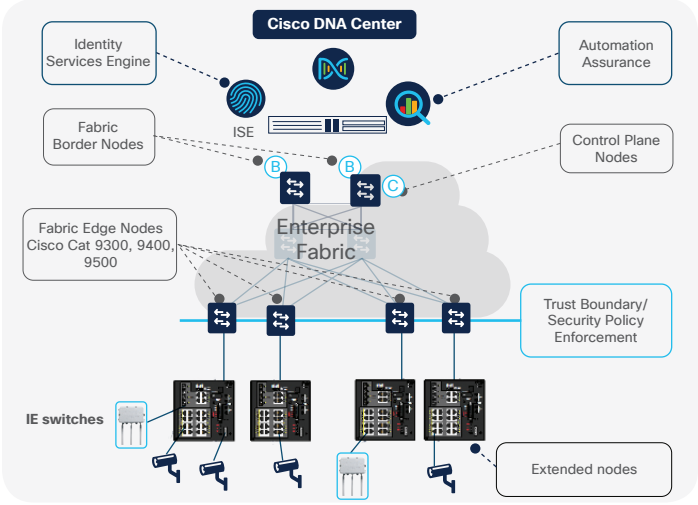
- **Control plane node:** Contains the settings, protocols, and tables to provide the endpoint-to-location mapping system for the fabric overlay.
- **Fabric border node:** Contains the settings, protocols, and tables to provide internal and external routing between the fabric overlay and outside networks.
- **Fabric edge node:** Contains the settings, protocols, and tables to provide (wired) endpoint onboarding and host mobility for the fabric overlay. The fabric edge nodes act as the security point. All traffic that enters or leaves the fabric from the edge devices is secured at this point.
- **Extended nodes:** Networking devices that are not deployed in the air-conditioned wiring closet. These devices are deployed outdoors, in the ceiling, or in roadside cabinets. Extended nodes are typically Ethernet switches and must connect to a fabric edge node. Extended nodes support Macro Segmentation. Macro Segmentation is policy at the virtual network level.
- **Policy Extended nodes:** Policy Extended nodes, are just like Extended nodes, in all the physical characteristics. Policy Extended nodes are Industrial Ethernet switches that connect to a fabric edge node. Like extended nodes, policy extended nodes operate in Layer 2 mode. Policy Extended Nodes support Micro Segmentation. Micro segmentation supports security within a virtual network allowing for finer grain control of all devices connecting within a virtual network.

The Cisco IE switches are extended nodes with direct connections to the fabric edge nodes.

Components of the SD-Access solution

Figure 3 shows the components of the Cisco SD-Access solution.

Figure 3. SD-Access solution components



An overlay is a virtual network running over the fabric. There can be many overlays per fabric. Since an overlay is a virtual network, you can think of services such as IP voice, wireless guest access, and parking garage video surveillance as being mapped to overlays. When the parking garage video surveillance is created, there is an overlay (or virtual network) for that service.

The fabric overlay is the key to building policy-based segmentation as well as to providing dynamic services where needed. The creation and management of the fabric overlay is fully automated within Cisco DNA Center. This includes updates to the control plane protocols and IP addressing. IP pools are assigned to fabric overlays at the time of creation. Separation of services as part of the intent based networking security policy is called Macro segmentation. Separating guest wireless into its own virtual network is an example of macro segmentation.

Every fabric overlay exists across the entire fabric. This means that wherever a network service needs to be deployed, it's as easy as making an Ethernet connection to a fabric edge or fabric extended node. Adding devices to an existing service is very easy: Simply associate an Ethernet port on a fabric edge device or fabric extended node device with the correct overlay. Then connect the end device needing the service from that overlay into the provisioned Ethernet port on the fabric edge or fabric extended node. Done!

Benefits of Micro Segmentation

As eluded to above, Micro Segmentation is security policy applied to different devices in the same virtual network (or overlay network). This means two devices in the same virtual network can have different security policies. Therefore they can be prevented from communicating with each other even if they are in the same IP subnet, or even the same Vlan.

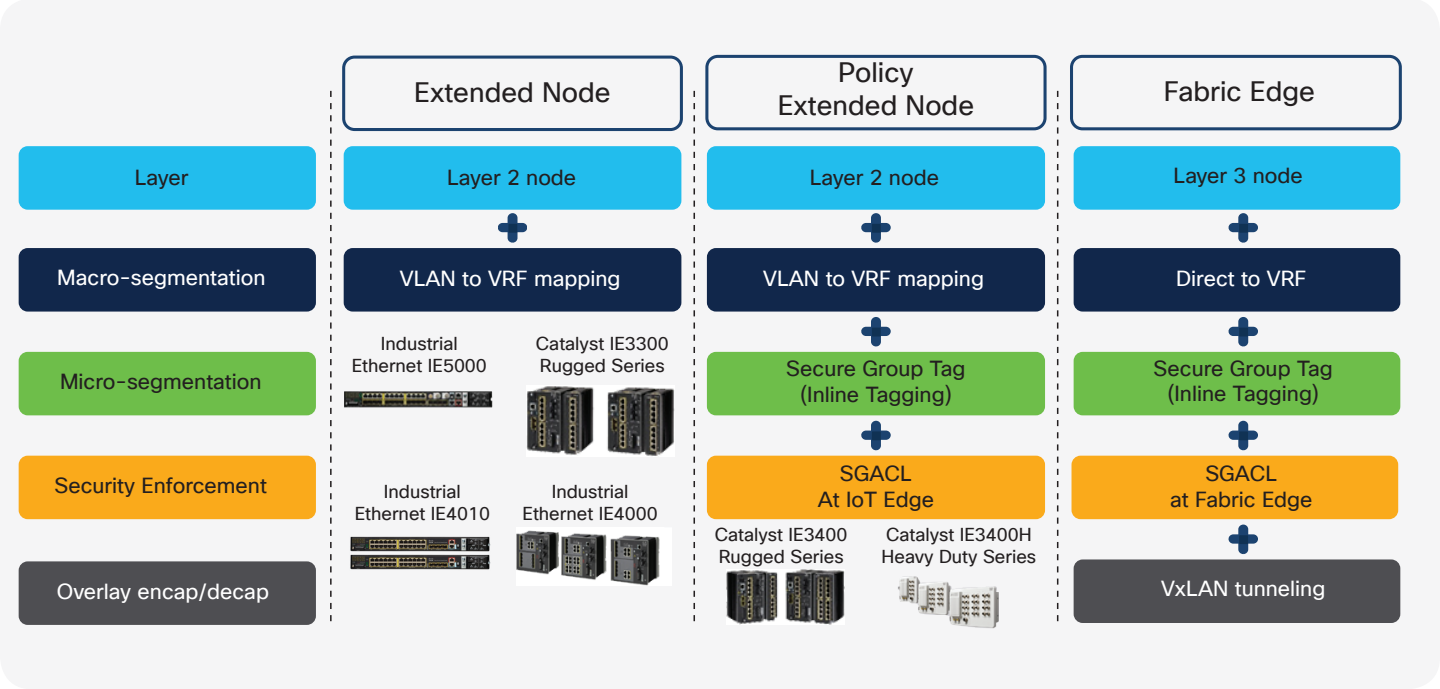
Micro Segmentation uses Scaleable Group Tags, and Scaleable Group ACLs to implement security policy within a virtual network.

Micro Segmentation is supported on Fabric Edge and Policy Extended Node devices.

Not all Cisco products capable of supporting Extended Node can also support Policy Extended Node.

The image below show the Industrial Ethernet support matrix for Extended Node, Policy Extended Node and Fabric Edge.

Figure 4. Extended Node, Policy Extended Node and Fabric Edge



Only the IE3400 and IE3400H support Policy Extended Node.

Advantages of the SD-Access solution

Other than the ease of adding end devices to an existing service, other notable advantages of the solution are as follows.

Address-agnostic security

The need to manage firewalls and trying keep up with the ever-changing IP subnets goes away. Physical location no longer plays a role in the security policy.

In the SD-Access solution, the fabric provides security based on policies defined in Cisco DNA Center. Changes in security policy are pushed to the fabric by Cisco DNA Center. As devices attach to the fabric edge nodes and extended nodes, they get associated with a security policy that is used within the fabric. IP or MAC addresses are no longer the primary means of identifying people and IoT devices. This is why security in the SD-Access solution is address-neutral or address-agnostic.

Cisco ISE works with Cisco DNA Center to profile, identify, and house the security policies. Think of the ISE as providing all the identity and policy services for the physical and network layers. The ISE is responsible for placing the profiled users and devices into the security group and host pool. The fabric then uses the assigned security group to permit or deny communications within the fabric – just as firewalls do today, but using the profile and not the IP address.

Extended Nodes and Policy Extended nodes work differently in how they implement security. Extended nodes do not implement the security policy. They do communicate with the ISE to profile the IoT devices that connect to them. The correct virtual network and IP address pool are applied to the IoT device at the access port on the extended node. The fabric edge nodes implement the security policy.

For Extended nodes, the SD-Access solution uses Security Group Tags (SGTs) and the SGT Exchange Protocol (SXP) within Cisco TrustSec® for implementing security policies. The fabric edge nodes apply the SGT to the Ethernet frames during ingress to the fabric. This works the same for devices directly connected to the access ports on the fabric edge nodes as it does for the access ports on the extended nodes. Once an Ethernet frame from a device is in the fabric, it carries the SGT applied at ingress with it while in the fabric. Security policies defined in Cisco DNA Center are implemented in the fabric by checking the permission of the SGT associated with the Ethernet frame. The fabric edge devices are the “trust boundary” because the action and policy of SGT tagging happens here.

Policy extended nodes act very much like fabric edge devices for security. Policy Extended nodes also apply the SGT to ingressing Ethernet frames for directly connected end devices. As the ethernet frame is forwarded throughout the fabric, the SGT is carried along with it. And just like the fabric edge devices the security enforcement is also implemented on the interfaces of the policy extended nodes. Policy extended nodes extend the trust boundary to their access interfaces.

Subnet stretching

Because the overlays exist over the entire fabric, IoT devices (or any end device really) can connect into the fabric from anywhere and get the correct virtual network association. IoT devices can be in the same Layer 2 broadcast domain even though they are connected to different fabric edge devices. The broadcast domain within the overlay extends too. This is useful for extended nodes and IoT devices. It means that network administrators no longer need to stretch a VLAN across the network, or run a fiber cable across the network to connect devices to the same VLAN. Having any subnet available anywhere in the fabric provides flexibility that network administrators will come to love.

Under the covers, it’s all about the VLAN on the fabric edge or extended node access port. The VLAN maps to the overlay, which maps to the IP subnet. Cisco DNA Center takes care of this, and the network administrator doesn’t need to know the VLAN IDs.

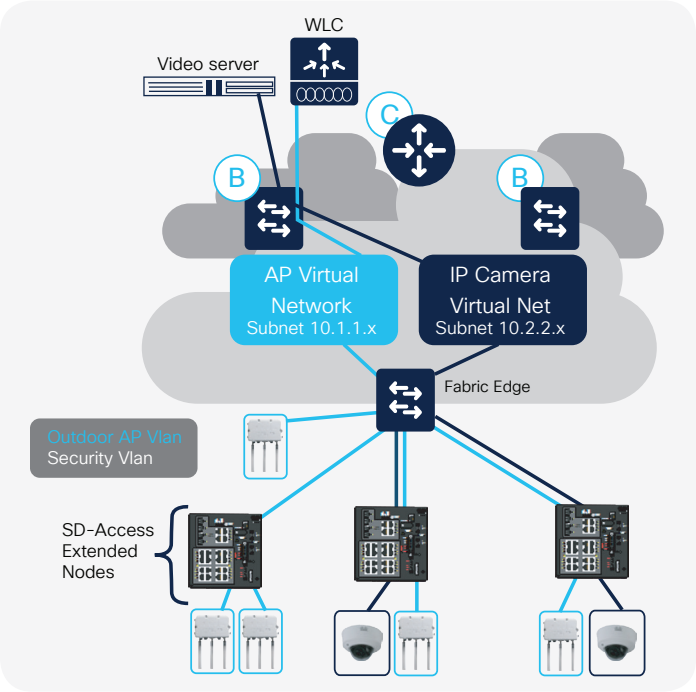
IP pools for end devices managed by Cisco DNA Center

The IP subnets (referred to as IP pools in Cisco DNA Center) for the IoT devices and other enterprise devices are associated with the overlay at creation. The process of creating a new virtual network includes associating an IP address pool of any size to the virtual network.

If the IoT devices require Dynamic Host Configuration Protocol (DHCP) service, it’s up to the network administrator to associate a DHCP server with the IP Pool. This is not currently managed by Cisco DNA Center.

Warehouse use case

Figure 5. Warehouse deployment based on SD-Access



The network service needed in warehouses provides a good and simple example of how the SD-Access solution can be deployed outside of the normal enterprise site (Figure 4). Warehouses are often set up, configured, and managed by IT network engineers. Many enterprises that have warehouses have more than one of them and want to replicate operations as much as possible to save on capital expenditures and operational costs. Plus warehouses require ruggedized networking products because of dust, heat, cold, dampness, etc. Cisco's Industrial Ethernet switching products are very popular in warehouse networks because they are well suited to this environment. These products are fully managed by Cisco DNA Center and work within the SD-Access solution.

Most warehouses need IP video surveillance for security, wireless access points 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. For networking purposes, it makes sense to think of a warehouse as a small enterprise building or even a branch office. Just more devices and fewer people, and the devices have to function without air conditioning.

The networking needs of a warehouse are similar to those of many different network deployment types. 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.

Many warehouses do not have an IT network engineer on site. Instead, IT staff manage the warehouse network remotely. They need to be able to deploy new devices and new services quickly. Time is critical and expensive, since the installer is likely an hourly contractor or had to travel from the corporate office to be on site.

The SD-Access solution addresses all these needs. It's managed remotely from Cisco DNA Center. One Cisco DNA Center application can manage multiple warehouse sites with a feature called Multisite. This allows the network engineer not only to centrally manage the inventory of network devices, but also to define security policy once. Then each site gets the same policy pushed to it. The Cisco DNA Center application allows the customer to scale across sites regardless of their size, because the security policies are all the same.

In this example, the warehouse has a small office area that does have air conditioning. The SD-Access solution requires nonruggedized components to be present to implement the fabric. A Cisco Catalyst® 9300 Series Switch is needed as the fabric edge node. It would be placed in the office. Also, there is a WAN link of some sort. This would also be present in the office. The fabric edge device would then connect to a "ruggedized" networking device such as a Cisco IE-4000 or IE-4010 switch. These switches provide PoE and PoE+ to connect access points and IP cameras as well as other devices.

In Figure 4, the fabric consists of a single fabric edge node and a single border/control router node. The fabric is extended by the IE switches, which are deployed out in the warehouse.

Cisco DNA Center is used to configure the Ethernet interfaces on the fabric edge to connect to the extended node switches. The extended nodes always operate in Layer 2 mode; they never route Ethernet frames based on IP address. The Ethernet interfaces between the fabric edge device and the extended node switches are trunk interfaces that carry multiple VLANs.

Cisco DNA Center is also used to create two separate virtual networks for the access points and the IP cameras. When the virtual networks are created, an IP address pool (subnet) is associated with each virtual network as well as a VLAN. Cisco DNA Center pushes the configuration for the virtual network to the border router and fabric edge device. For security purposes, the network engineer is required to separate the video surveillance data from all other network data. Cisco DNA Center and the SD-Access solution make this easy. Because the video surveillance data traffic is mapped to a virtual network, a natural separation of network data traffic occurs.

Cisco TrustSec helps ensure that any device attached to the network via a fabric edge device doesn't get routed to a resource it's not supposed to.

Summary

Extending the network to provide more connectivity is now the same as adding to an enterprise network. The products are different, but the processes and techniques to build it out are the same. The SD-Access solution can easily be extended.

More information

Cisco.com has lots of documentation on IE switching, Cisco DNA Center, and the SD-Access solution.

IE switching products: https://www.cisco.com/c/en/us/products/switches/industrial-ethernet-switches/index.html

SD-Access solution: https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access/index.html

Intuitive and intent-based networking: https://www.cisco.com/site/us/en/products/networking/access-software/dna-subscription-wireless/index.html

Solution white paper on enterprise SD-Access solutions: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/software-defined-access/white-paper-c11-739642.html

C11-740444-01 07/20