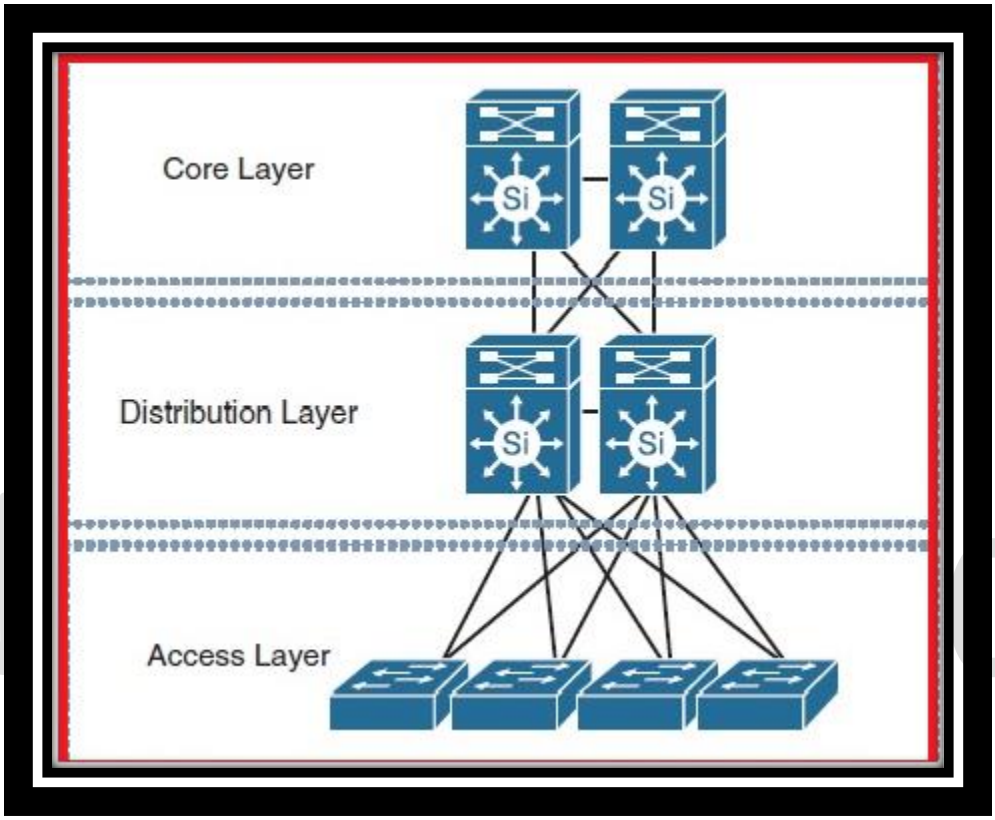

Networkforyou
Two-Tier/Three-Tier
Architectures and
Fabric Capacity Planning
Networkforyou

## Two-Tier & Three-Tier Architectures:




### Core Layer:

- We used CISCO three-layer hierarchical architecture for more than a decade.
- Core Layer consists of **biggest, fastest and most expensive routers with highest model**.
- In the Three Tier Architecture, the **Core Layer is the one coordinating everything**.
- Its only role is to forward traffic, the fastest it can; here you don't apply any policy.
- Whereas several distributions switches, Core layer is considered as **backbone of networks**.
- Core Layer routers or switches move information on the network as **fast as possible**.
- The **Core switches talk with distribution switches using dynamic routing protocols**.
- The Core Layer can provide the **high-speed switching, reliability and fault tolerance**.
- At Core Layer most advanced and **expensive switches used**.


- Core also referred to as the network backbone, this layer is responsible for **transporting large amounts of traffic quickly.**
- Core layer provides interconnectivity between distribution layer devices it usually consist of high speed devices, like high end routers and switches with redundant links.

**Distribution Layer:**

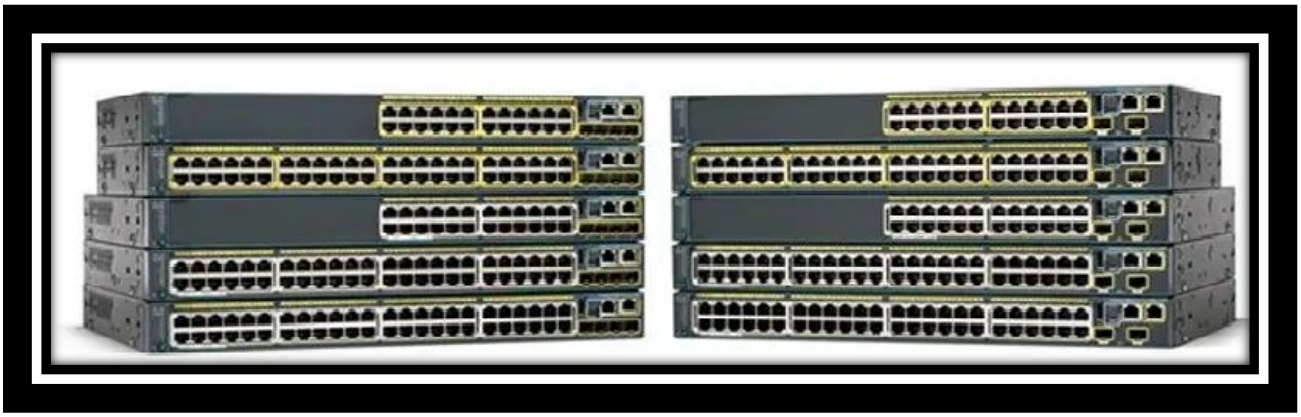
- The Distribution Layer is located between the **Access Layer and Core Layers**.
- In Distribution Layer we can **defines policy for network**.
- Distribution Layer ensures that packets are properly routed between subnets and VLANs.
- Distribution Layer can provide, Aggregation of Local Area Network or WAN links.
- In this Layer we can provide **Policy-based security in form of access control lists (ACL) and filtering**.
- Also Provide, Routing services between LANs and VLANs and between routing domains.
- These layers also provide **Redundancy, load balancing, aggregation and summarization**.
- Broadcast domain control, routers or multilayer switches do not forwards broadcasts.
- Distribution layer is the smart layer in the three layer model.
- **Routing, filtering and QOS policies are managed at the distribution layer**.
- Distribution layer devices also often manage individual branch office WAN connections.

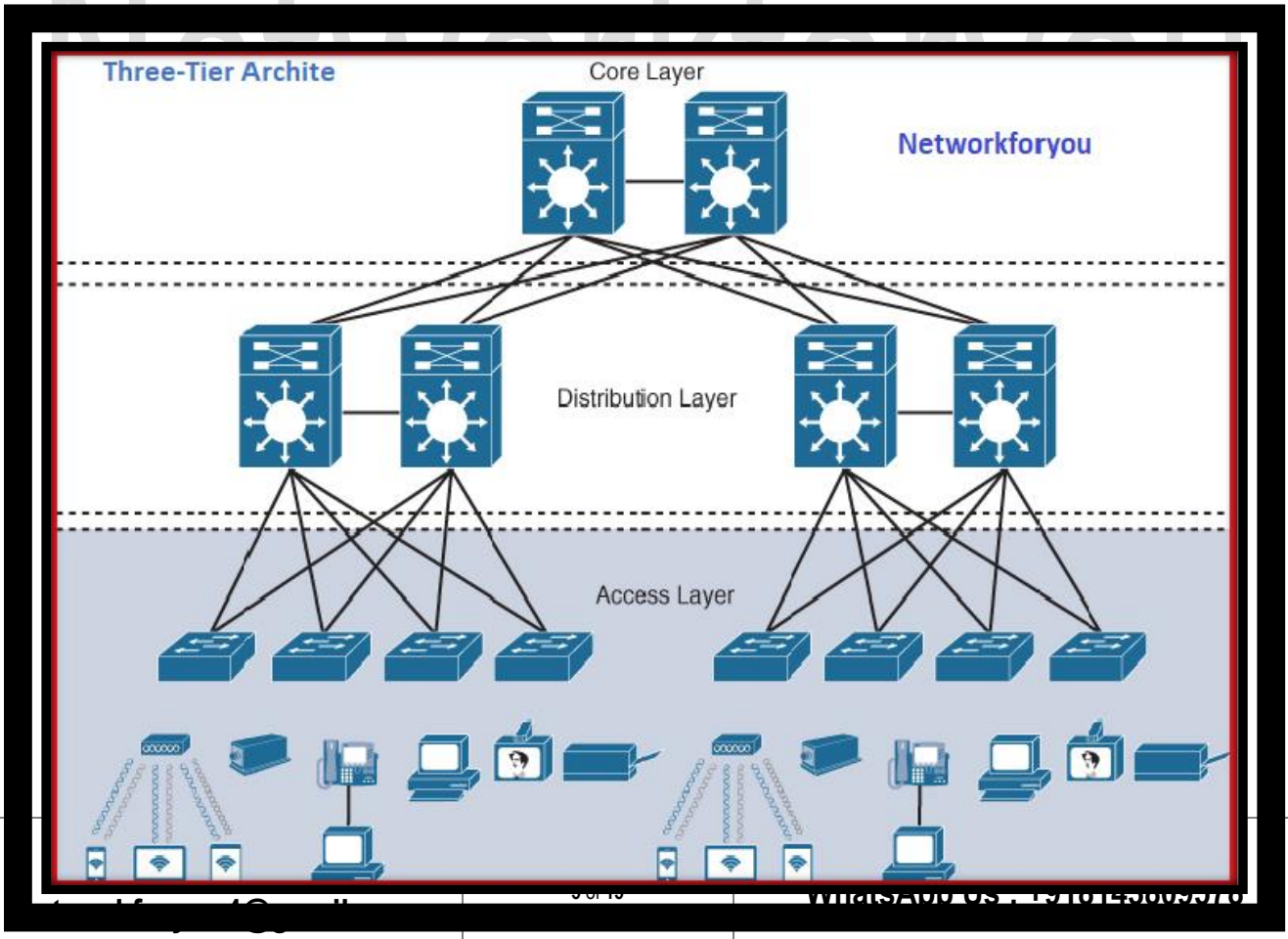
- This layer is also called the workgroup layer

**Access Layer:**

- The Access Layer is the **one closer to the users**; at this layer we find the users themselves.
- The Access Layer, also commonly referred as the network edge, is where end user devices or endpoints connect to the network. Or it is the level where host computer are connected to the network.
- It provides high bandwidth device connectivity using **wired and wireless access** technologies.
- The Access layer includes access switches which are connected to the end devices.
- Access layer switches ensure that packets are delivered to the end points.
- The Main purpose of the Access Layer is to **physically connect users to the network.**
- **There is just a cable between end user and access layer network.**

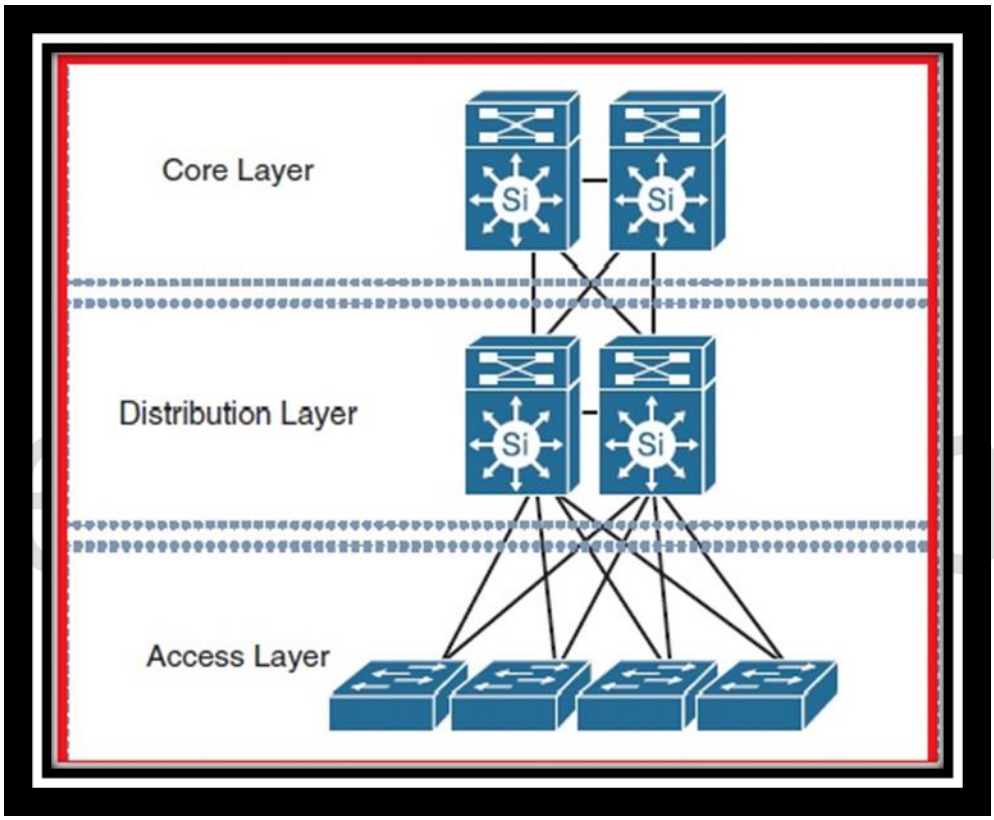
- There are **security policies we want to enforce in order to allow access to the network.**
- **Like we can configure Port-security and Network Access Control in this layer.**
- Also this layer provides **QOS Classification, ARP Inspection, Spanning tree, Power Over Ethernet and VLANs.**





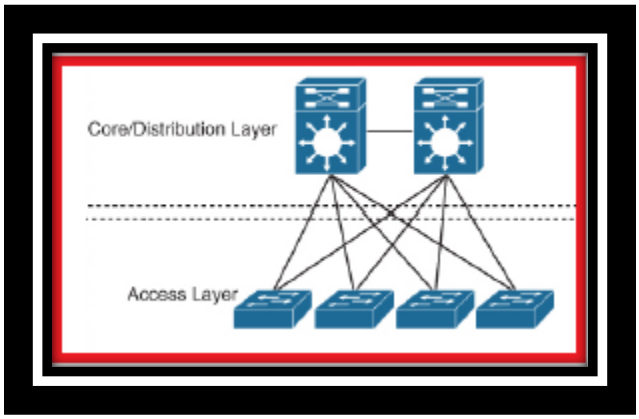
## Three Tier:

- The Three Tier (3 Tier) Architecture is **a great solution for large enterprises**.
- CISCO Suggests 3 Tier hierarchical network model that consists of three layers.
- The Three Tier is the Core Layer, the Distribution layer, and the Access layer.
- CISCO Three-Layer network model is the preferred approach to network design.




## Two Tier:

- Two Tier design model is more suitable for **small to medium-size networks**.
- **Core and distribution functions can be combined into one, also known as collapsed core**.
- Collapsed Core is when distribution and Core layer functions are implements by single device.
- The Primary motivation for the collapsed core design is to **reduce the network cost**.
- In two Tiers still maintaining most of the benefits of the three-tier hierarchical model.




**Benefits of Hierarchical Model:**

- Three-layer or 2 –layer network model allows in **creating high performance networks**.
- It allows better network management and isolates causes of **network trouble and issue**.
- Cisco Three Layer Network Model allows **better filter & policy creation application**.
- Cisco Three Layer Network Model allows us to **efficiently accommodate future gro**wth.
- Three Layer or Two Layer Network Model provides better **redundancy & availability**.
- Multiple links across multiple devices provides better **redundancy and availabilities**.
- **If one switch is down, we have another alternate path to reach the destination**.
- When network grows, we can easily add **more distribution or access layer switches**.
- Main benefits help to design, deploy & maintain scalable hierarchical internetwork.

**Fabric Capacity Planning:**

What is network capacity planning?

- Network Capacity Planning is **ensuring that the network has the resources it needs to prevent an impact on business-critical applications.**
- Whether you're ensuring that there is enough bandwidth through a service provider, or verifying the load on network devices, having full awareness in a single view.
- A fabric network is an **overlay network (virtual network)** built over an **underlay network (physical network)** using overlay tunneling technologies such as VXLAN.

- Fabric networks overcome shortcomings of **traditional physical networks by enabling host mobility, network automation, network virtualization, and segmentation, and they are more manageable, flexible, secure (by means of encryption), and scalable than traditional networks**.
- **Now we have next-generation overlay fabric technologies Software-Defined Access (SD-Access) for campus networks and Software-Defined WAN (SD-WAN) for WAN networks**
- The Cisco SD-Access fabric is one of the main components of the **Cisco Digital Network Architecture (Cisco DNA).**
- Cisco DNA is the solution for the future of intent-based networking in Cisco enterprise networks. SD Access provides policy-based network segmentation, host mobility for wired and wireless hosts, and enhanced security as well as other benefits in a fully automated fashion.
- **Cisco SD-Access was designed for enterprise campus and branch network environments and not for other types of network environments, such as data center, service provider, and WAN environments.**
- Traditional WANs are typically designed using MPLS or other overlay Solutions, such as Dynamic Multipoint Virtual Private Network (DMVPN) or Intelligent WAN (IWAN) to provide connectivity between different campus and branch sites.
- However, with the **rise of software as a service** (SaaS) cloud applications such as Microsoft Office 365 and Salesforce.com, and public infrastructure as a service (IaaS) cloud services from Amazon Web Services **(AWS),** Google Compute Engine **(GCE),** and **Microsoft Azure**, traffic patterns are changing so that the majority of enterprise traffic flows to public clouds and the Internet. Such changes are creating new requirements for security, application performance, cloud connectivity, **WAN** management, and operations that traditional WAN solutions were not designed to address.
- The Cisco **SDWAN fabric is a cloud-based WAN solution for enterprise and data center networks** that was developed to address all the new WAN requirements.



## SOFTWARE-DEFINED ACCESS (SD-ACCESS):

- There are many operational challenges in enterprise campus networks due to manual configuration of network devices. Manual network configuration changes are slow and lead to misconfigurations that cause service disruptions on the network, and the situation is make worse in a constantly changing environment where more users, endpoints, and applications are constantly being added.
- The constant growth in users and endpoints makes configuring user credentials and maintaining a consistent policy across the network very complex.
- If policies are inconsistent, there is an added complexity involved in maintaining separate policies between wired and wireless networks that leaves the network vulnerable to security breaches. As users move around the campus network, locating the users and troubleshooting issues also become more difficult.

- In other words, traditional campus networks do not address the existing campus network needs. With SD-Access, an evolved campus network can be built that addresses the needs of existing campus networks by leveraging the following capabilities, features, and functionalities:

**Network Automation, Network assurance and analytics, Host mobility, Identity services, Policy enforcement, Secure segmentation and Network virtualization**

• **Network automation:** SD-Access replaces manual network device configurations with network device management through a single point of automation, orchestration, and management of network functions through the use of **Cisco DNA Center**. This simplifies network design and provisioning and allows for very fast, lower-risk deployment of network devices and services using best-practice configurations.

• **Network assurance and analytics**: SD-Access enables proactive prediction of network-related and security-related risks by using telemetry to improve the performance of the network, endpoints, and applications, including encrypted traffic.

• **Host mobility:** SD-Access provides host mobility for both wired and wireless clients.

• **Identity services:** Cisco Identity Services Engine (ISE) identifies users and devices connecting to the network and provides the contextual information required for users and devices to implement security policies for network access control and network segmentation.



• **Policy enforcement:** Traditional access control lists (ACLs) can be difficult to deploy, maintain, and scale because they rely on IP addresses and subnets. Creating access and application policies based on group-based policies using Security Group Access Control Lists (SGACLs) provides a much simpler and more scalable form of policy enforcement based on identity instead of an IP address.

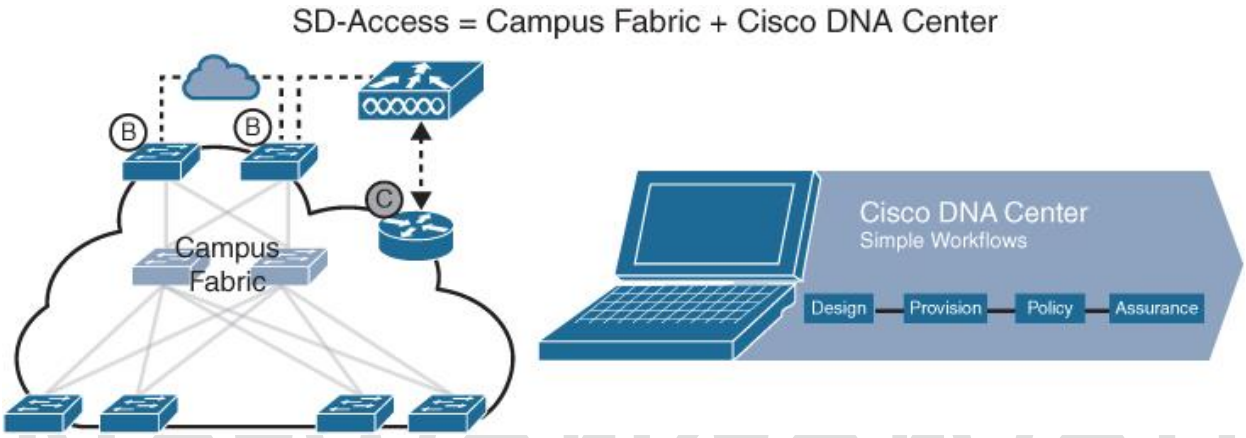
• **Secure segmentation:** With SD-Access it is easier to segment the network to support guest, corporate, facilities, and IoT-enabled infrastructure.

• **Network virtualization:** SD-Access makes it possible to leverage a single physical infrastructure to support multiple virtual routing and forwarding (VRF) instances, referred to as virtual networks (VNs), each with a distinct set of access policies.

## What Is SD-Access?

SD-Access has two main components:

- Cisco Campus fabric solution
- Cisco DNA Center

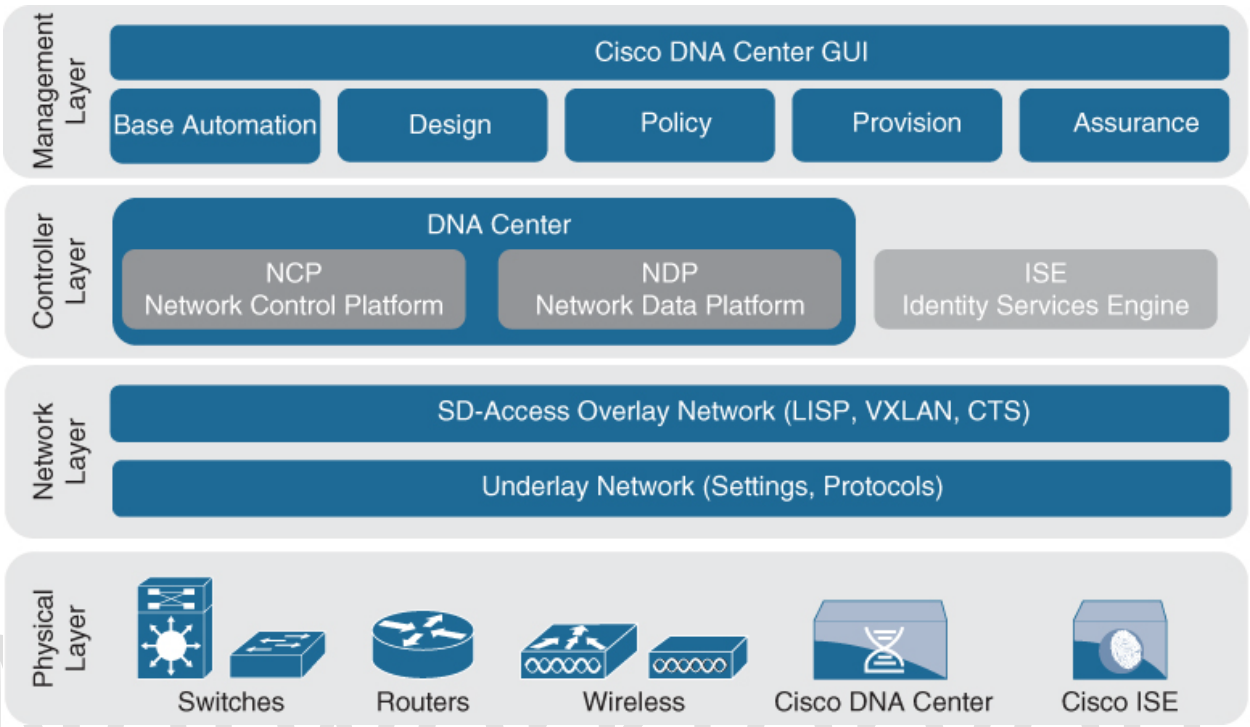





- The campus fabric is a Cisco-validated fabric overlay solution that includes all of the features and protocols (**control plane, data plane, management plane, and policy plane**) to operate the network infrastructure.
- When the **campus fabric solution is managed using the command-line interface (CLI) or an application programming interface (API) using Network Configuration Protocol (NETCONF)/YANG, the solution is considered to be a campus fabric solution**.
- When the **campus fabric solution is managed via the Cisco DNA Center**, the solution is considered to be **SD-Access**, as illustrated in Figure

## SD-Access Architecture:

- Cisco SD-Access is based on existing hardware and software technologies.
- What makes Cisco SD-Access special is how these technologies are integrated and managed together. The Cisco SD-Access fabric architecture can be divided into four basic layers as given below





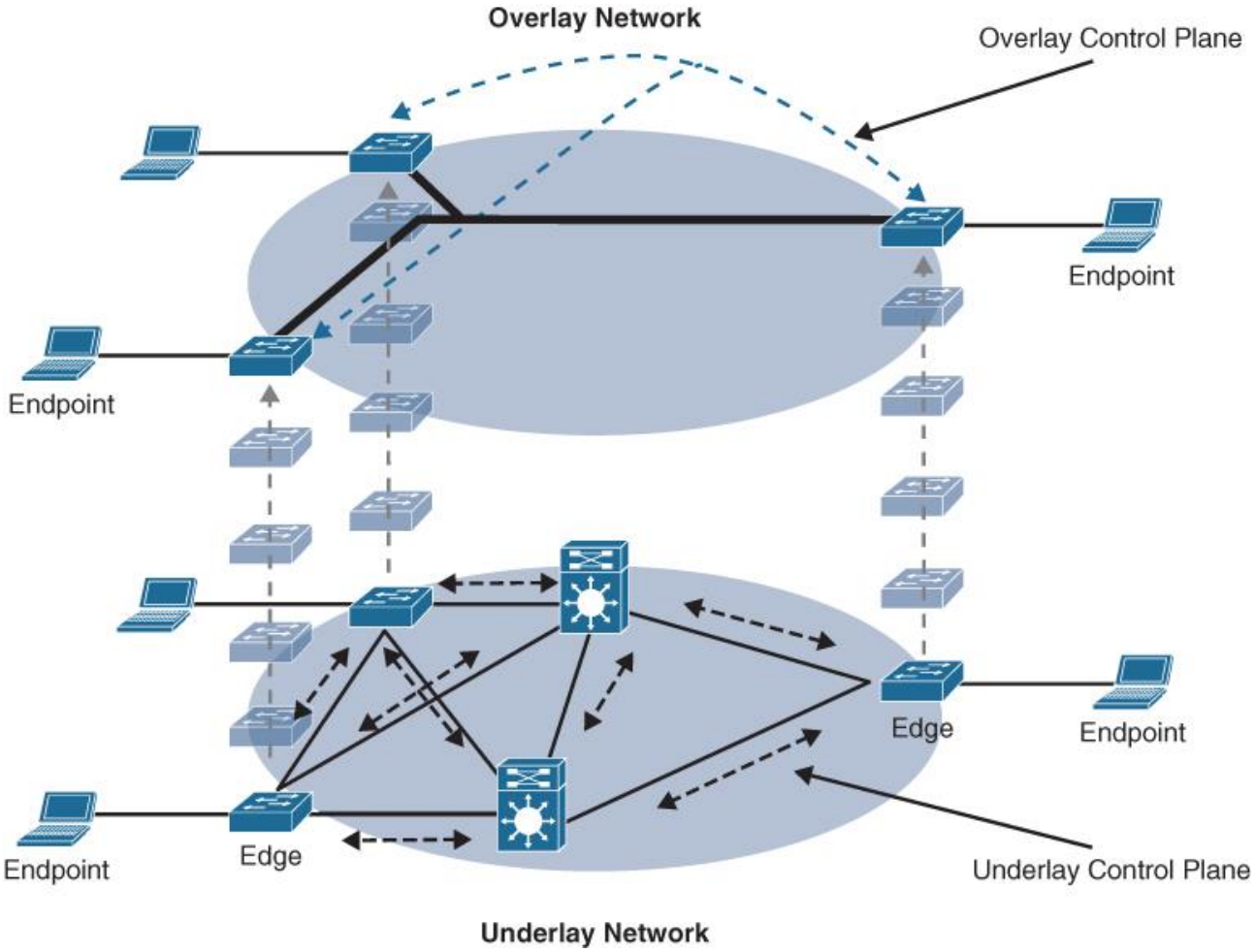

**Physical Layer:**

- While Cisco SD-Access is designed for user simplicity, abstraction, and virtual environments, everything runs on top of physical network devices— namely switches, routers, servers, wireless LAN controllers (WLCs), and wireless access points (APs).
- All Cisco network devices that actively participate in the SD-Access fabric must support all of the hardware Application-Specific Integrated Circuits (ASICs) and Field-Programmable Gate Arrays (FPGAs) and software requirements
- Cisco access layer switches that do not actively participate in the SD-Access fabric but that are part of it because of automation are referred to as SD-Access extension nodes.
- The following are the physical layer devices of the SD-WAN fabric:
  • **Cisco switches:** Switches provide wired (LAN) access to the fabric. Multiple types of Cisco Catalyst switches are supported, as well as Nexus switches.
  • **Cisco routers:** Routers provide WAN and branch access to the fabric. Multiple types of Cisco ASR 1000, ISR, and CSR routers, including the CSRv and ISRv cloud routers, are supported.
  • **Cisco wireless:** Cisco WLCs and APs provide wireless (WLAN) access
  To the fabric.

• **Cisco controller appliances**: Cisco DNA Center and Cisco ISE are the two controller appliances required.

## Network Layer

- The network layer consists of the **underlay network and the overlay network**. These two sublayers work together to deliver data packets to and from the network devices participating in SD-Access.
- All this network layer information is made available to the controller layer.
- The network underlay is the underlying physical layer, and its sole purpose is to transport data packets between network devices for the SD-Access fabric overlay.
- The overlay network is a virtual (tunneled) network that virtually interconnects all of the network devices forming a fabric of interconnected nodes.



## SOFTWARE-DEFINED WAN (SD-WAN)

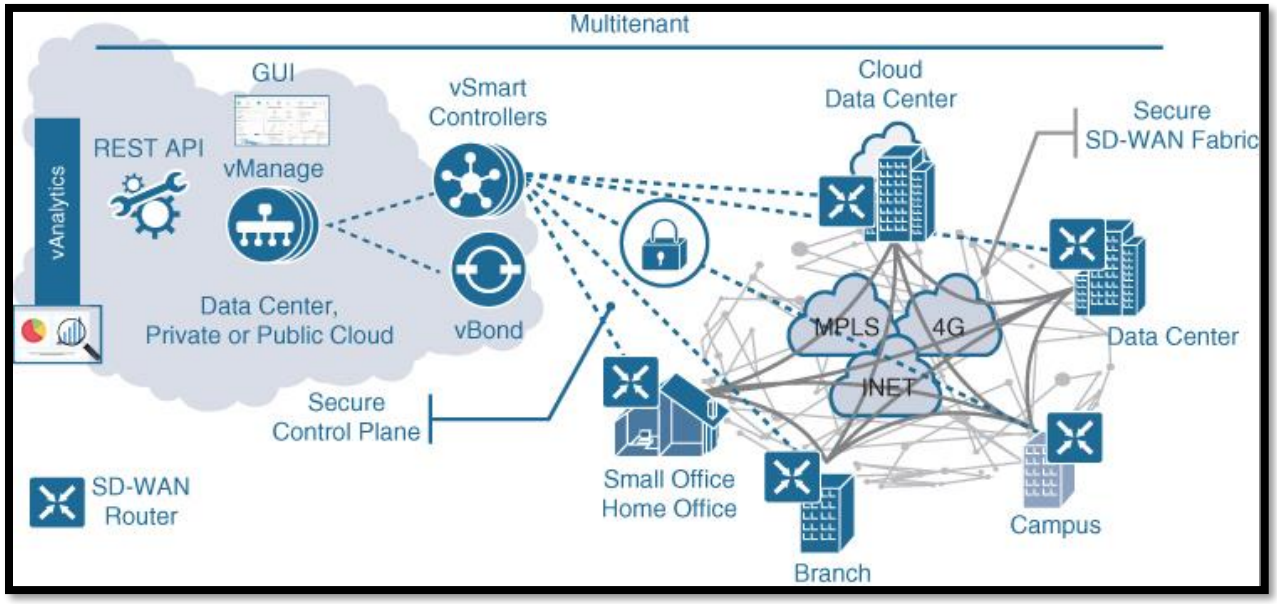
Managing enterprise networks is becoming more complex, with customers agreement a multicloud approach, applications moving to the cloud and mobile devices growing exponentially in the network, and the Internet edge moving to the branch. This digital transformation is powering the adoption of SD-WAN by customers looking to do the following:

• Lower costs and reduce risks with simple WAN automation and orchestration.
• Extend their enterprise networks (such as branch or on-premises) seamlessly into the public cloud.
• Provide optimal user experience for SaaS (**software as a service**) applications.
• Leverage a transport-independent WAN for lower cost and higher diversity. This means the **underlay network can be any type of IP-based network, such as the Internet, MPLS, 3G/4G LTE, satellite, or dedicated circuits.**
• Enhance application visibility and use that visibility to improve performance with intelligent path control to meet SLAs for business-critical and real-time applications.
• Provide end-to-end WAN traffic segmentation and encryption for protecting critical enterprise compute resources. Cisco currently offers **two SD-WAN solutions**:
• Cisco SD-WAN (**based on Viptela**): This is the preferred solution for organizations that require an SD-WAN solution with cloud-based initiatives that provides granular segmentation, advanced routing, advanced security, and complex topologies while connecting to cloud instances.
• **Meraki SD-WAN:** This is the recommended solution for organizations that require unified threat management (UTM) solutions with SD-WAN functionality or that are existing Cisco Meraki customers looking to expand to SD-WAN. **UTM is an all-in-one security solution delivered in a single appliance and typically includes the following security features: firewall, VPN, intrusion prevention, antivirus, antispam, and web content filtering.**



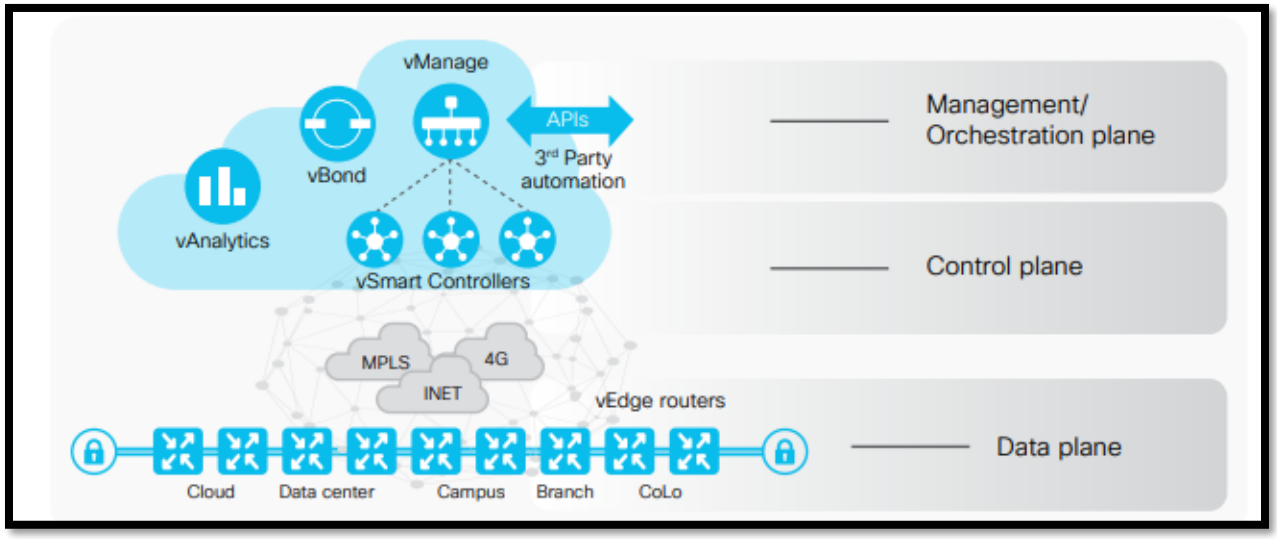
## Cisco SD-WAN Architecture:

- Cisco SD-WAN (based on Viptela) is a cloud-delivered overlay WAN architecture that facilitates digital and cloud transformation for enterprises, and it addresses all the customer requirements.
- Below block diagram show how SD-WAN can be used to provide secure connectivity to remote offices, branch offices, campus networks, data centers, and the cloud over any type of IP-based underlay transport network,such as the Internet, 3G/4G LTE, and MPLS. It also illustrates how some of the components to manage then SD-WAN fabric can be deployed on a data center, private cloud, or public cloud.




The Cisco SD-WAN solution has four main components and an optional analytics service:

• vManage Network Management System (NMS): This is a single pane of glass (GUI) for managing the SD-WAN solution.
• vSmart controller: This is the brains of the solution.
• SD-WAN routers: SD-WAN involves both vEdge and cEdge routers. This is WAN router present in Customer. Cisco SD-WAN routers deliver the essential WAN, security, and multicloud capabilities of the Cisco SD-WAN solution, and they are available as hardware, software, cloud, or virtualized routers that sit at the perimeter of a site, such as a remote office, branch office, campus, or data center.
• vBond orchestrator: This authenticates and orchestrates connectivity between SD-WAN routers and vSmart controllers.
• vAnalytics: This is an optional analytics and assurance service.




Vedge: First time Vedge is connect to Vbond with Transport Layer Security (TLS) protocol to get authentiaiton