

# Network Evolution

CCNA Routing and Switching

Connecting Networks v6.0



# Sections & Objectives

- 7.1 Internet of Things
  - Explain the value of the Internet of Things.
    - Describe the Cisco IoT System.
    - Describe the pillars of the Cisco IoT System.
- 7.2 Cloud and Virtualization
  - Explain why cloud computing and virtualization are necessary for evolving networks.
    - Explain the importance of cloud computing.
    - Explain the importance of virtualization.
    - Describe the virtualization of network devices and services.
- 7.3 Network Programming
  - Explain why network programmability is necessary for evolving networks.
    - Describe software-defined networking.
    - Describe controllers used in network programming.

# Internet of Things

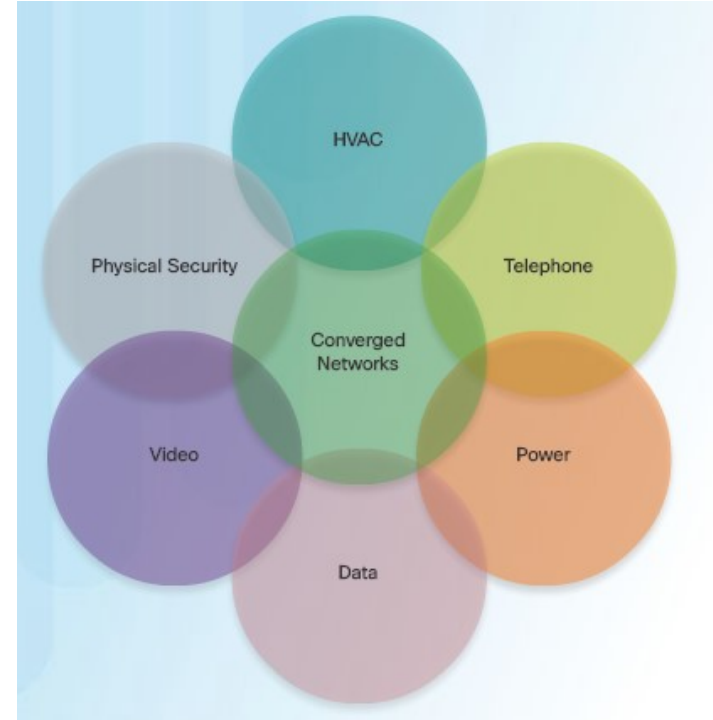
# What is the IoT?

- It is predicted that the Internet will interconnect 50 billion things by 2020.
- Using existing and new technologies, we are connecting the physical world to the Internet.
- It is by connecting the unconnected that we transition from the Internet to the Internet of Things (IoT).



# The Converged Network and Things

- Dissimilar networks are converging to share the same infrastructure.
- This infrastructure includes comprehensive security, analytics, and management capabilities.
- The connection of the components into a converged network that uses IoT technologies increases the power of the network to help people improve their daily lives.



# The Six Pillars of the Cisco IoT System

- Cisco IoT System uses six pillars to identify foundational elements.



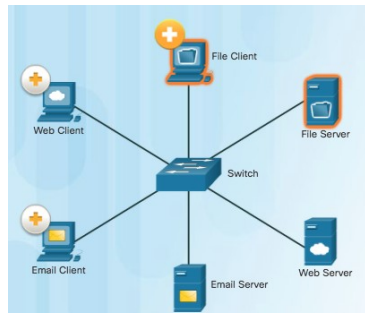
# The Network Connectivity Pillar

- All IoT devices need network connectivity and the equipment needed varies depending on the type of network.
- Home networks typically consist of a wireless broadband router, while business networks will have multiple switches, APs, a firewall or firewalls, routers, and more.

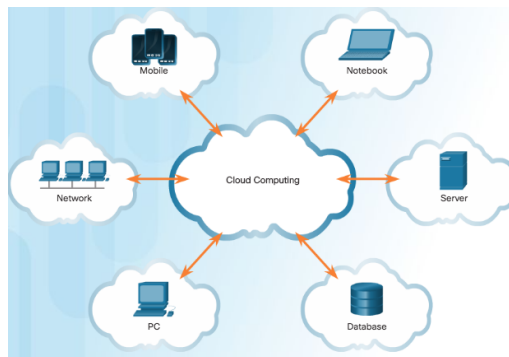
# The Fog Computing Pillar

### ■ Fog computing

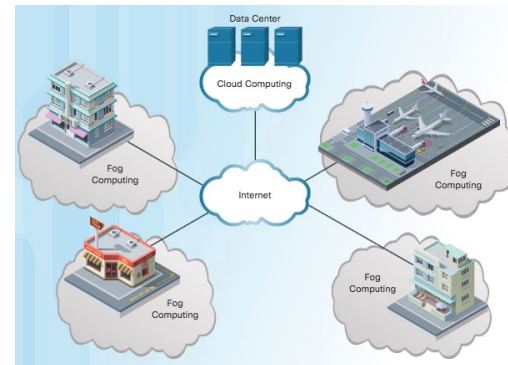
- This IoT network model identifies a computing infrastructure closer to the network edge.
- Edge devices run applications locally and make immediate decisions.
- Data does not need to be sent over network connections.
- Enhances resiliency by allowing IoT devices to operate when network connections are lost.
- Enhances security by keeping sensitive data from being transported beyond the edge where it is needed.



Client-Server Model



Cloud Computing Model



Fog Computing Model



# The Security Pillar

- IoT introduces new attack vectors not typically encountered with normal enterprise networks.
- Cybersecurity solutions include:
  - Operational Technology (OT) specific security – OT is the hardware and software that keeps power plants running and manages factory process lines.
  - IoT Network security – Includes network and perimeter security devices.
  - IoT Physical security - Cisco Video Surveillance IP Cameras.



Cisco Industrial  
Security Appliance



Cisco FirePOWER Appliance



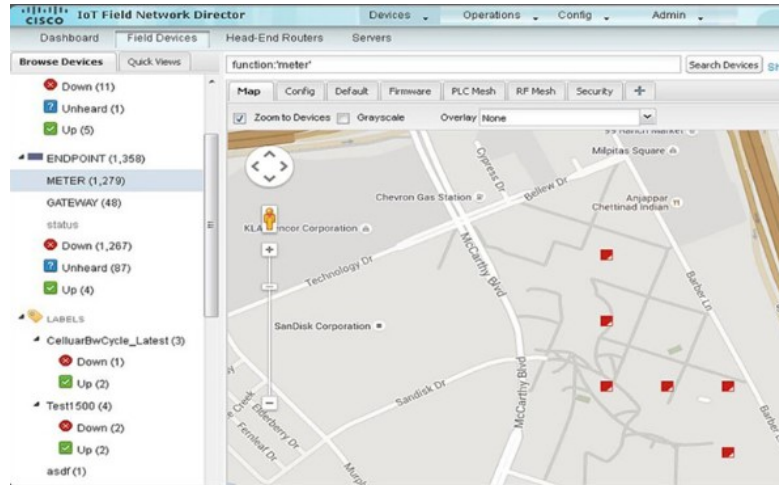
Cisco Video  
Surveillance  
Cameras

# Data Analytics Pillar

- IoT can connect billions of devices capable of creating exabytes of data every day. To provide value, this data must be rapidly processed and transformed into actionable intelligence.
  - Need to bring centers of data together and take advantage of data.

# Management and Automation Pillar

- IoT expands the size and diversity of the network to include the billions of smart objects that sense, monitor, control, and react. Each of these areas also has distinctive requirements, including the need to track specific metrics.
- Cisco management and automation products can be customized for specific industries to provide enhanced security and control and support.
- Management Tools: Cisco IoT Field Network Director, Cisco Prime, Cisco Video Surveillance Manager, and more.



# Application Enablement Platform Pillar

- Provides the infrastructure for application hosting and application mobility between cloud and Fog computing.
- Cisco IOx which is a combination of Cisco IOS and Linux, allows routers to host applications close to the objects they need to monitor, control, analyze, and optimize.

# Cloud and Virtualization

# Cloud Computing

## Cloud Overview

- Cloud computing
  - The “pay-as-you-go” model where capital expenditures are transferred to operating expenses.
  - Large numbers of networked computers physically located anywhere.
  - Providers rely heavily on virtualization.
  - Reduce operational costs by using resources more efficiently.
  - Supports a variety of data management issues:
    - Enables access to organizational data anywhere and at any time
    - Streamlines the organization’s IT operations by subscribing only to needed services
    - Eliminates or reduces the need for onsite IT equipment, maintenance, and management
    - Reduces cost for equipment, energy, physical plant requirements, and personnel training needs
    - Enables rapid responses to increasing data volume requirements

## Cloud Computing

# Cloud Services

- Cloud computing services defined by the National Institute of Standards and Technology (NIST):
  - **Software as a Service (SaaS):** Access to services, such as email and Office 365 that are delivered over the Internet.
  - **Platform as a Service (PaaS):** Access to the development tools and services used to deliver the applications.
  - **Infrastructure as a Service (IaaS):** Access to the network equipment, virtualized network services, and supporting network infrastructure.
  - **IT as a Service (ITaaS):** IT Professionals support applications, platforms and infrastructure.

## Cloud Computing

# Cloud Models

- **Public clouds:** Application and services made available to the general population. Services may be free or are offered on a pay-per-use model, such as paying for online storage. Uses the Internet to provide services.
- **Private clouds:** Applications and services are intended for a specific organization or entity, such as the government. A private cloud can be set up using the organization's private network, though this can be expensive to build and maintain. A private cloud can also be managed by an outside organization with strict access security.
- **Hybrid clouds:** Made up of two or more clouds (example: part private, part public), where each part remains a distinctive object, but both are connected using a single architecture.
- **Community clouds:** A community cloud is created for exclusive use by a specific community. For example, healthcare organizations must remain compliant with policies and laws (e.g., HIPAA) that require special authentication and confidentiality.



# Cloud Computing versus Data Center

- **Data center:** Typically a data storage and processing facility run by an in-house IT department or leased offsite.
- **Cloud computing:** Typically an off-premise service that offers on-demand access to a shared pool of configurable computing resources. These resources can be rapidly provisioned and released with minimal management effort.

Cloud computing is possible because of data centers.



Cloud computing is often a service provided by data centers.

# Cloud Computing and Virtualization

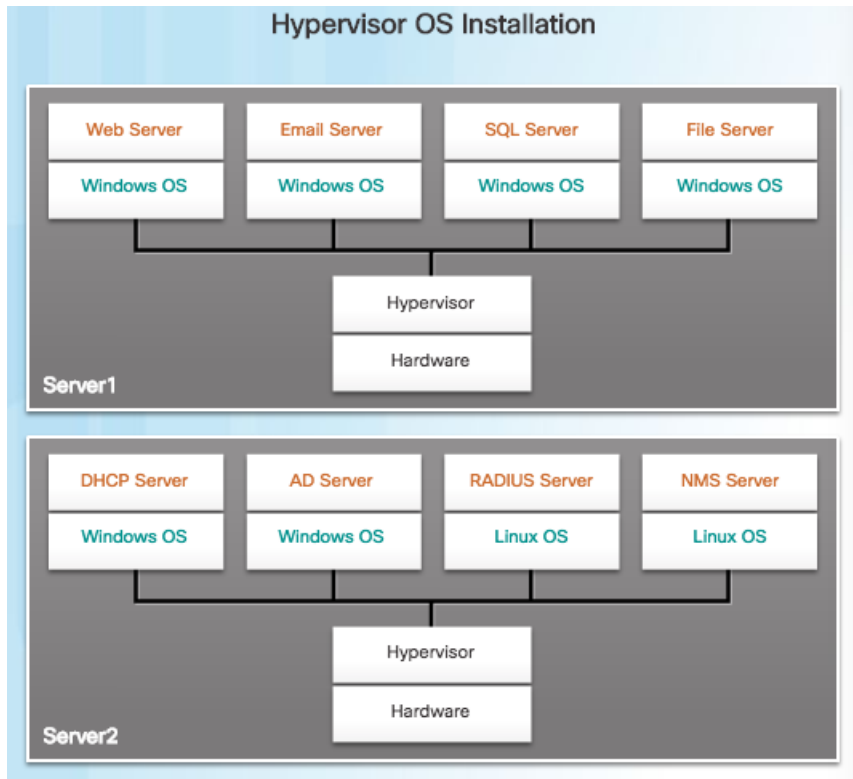
- Virtualization is the foundation of cloud computing. Without it, cloud computing would not be possible.
- Cloud computing separates the application from the hardware.
- Virtualization separates the OS from the hardware.
- Amazon Elastic Compute cloud (Amazon EC2) web service provides a simple way for customers to dynamically provision the computer resources they need. These virtualized instances of servers are created on demand in Amazon's EC2.

# Virtualization

## Dedicated Servers



# Server Virtualization



- In the figure, the previous eight dedicated servers have been consolidated into two servers using hypervisors to support multiple virtual instances of the operating systems.
- Hypervisor is a program, firmware, or hardware that adds an abstraction layer on top of the real physical hardware.
- The abstraction layer is used to create virtual machines which have access to all the hardware of the physical machine such as CPUs, memory, disk controllers, and NICs.
- It is not uncommon for 100 physical servers to be consolidated as virtual machines on top of 10 physical servers that are using hypervisors.

# Advantages of Virtualization

- One major advantage of virtualization is overall reduced cost:
  - Less equipment is required - Server consolidation and lower maintenance costs.
  - Less energy is consumed - Consolidating servers lowers the monthly power and cooling costs.
  - Less space is required - Fewer servers, network devices, and racks reduce the amount of required floor space.
- Additional benefits of virtualization:
  - Easier prototyping
  - Faster server provisioning
  - Increased server uptime
  - Improved disaster recovery
  - Legacy Support

## Virtual Network Infrastructure

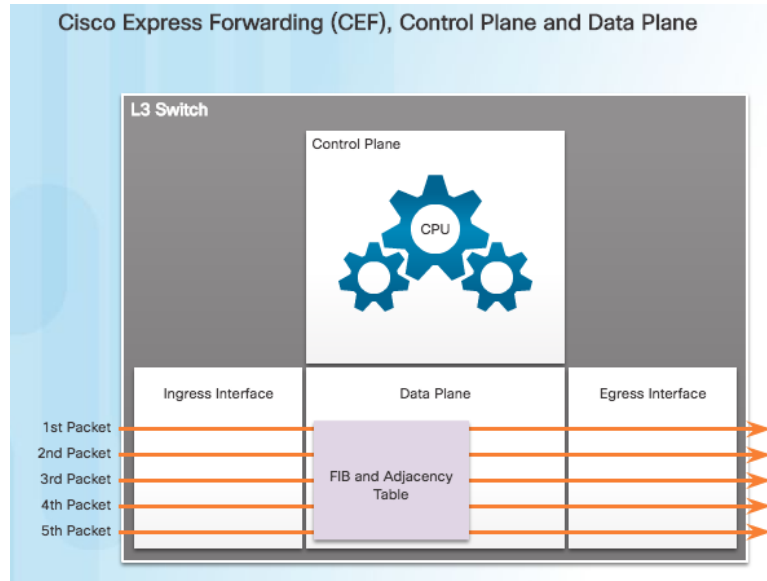
# Network Virtualization

- Server virtualization hides server resources from server users. This practice can create problems if the data center is using traditional network architectures.
- For example, Virtual LANs (VLANs) used by VMs must be assigned to the same switch port as the physical server running the hypervisor. However, VMs are movable, and the network administrator must be able to add, drop, and change network resources and profiles. This process is difficult to do with traditional network switches.
- Another problem is that traffic flows differ substantially from the traditional client-server model. Typically, a data center has a considerable amount of traffic being exchanged between virtual servers (referred to as East-West traffic). These flows change in location and intensity over time, requiring a flexible approach to network resource management.
- Existing network infrastructures can respond to changing requirements related to the management of traffic flows by using Quality of Service (QoS) and security level configurations for individual flows. However, in large enterprises using multivendor equipment, each time a new VM is enabled, the necessary reconfiguration can be very time-consuming.

# Network Programming

# Control Plane and Data Plane

- A network device contains the following planes:
  - Control plane - Regarded as the brains of a device. Used to make forwarding decisions. Information sent to the control plane is processed by the CPU.
  - Data plane - Also called the forwarding plane, this plane is the switch fabric connecting the various network ports on a device. The data plane of each device is used to forward traffic flows.

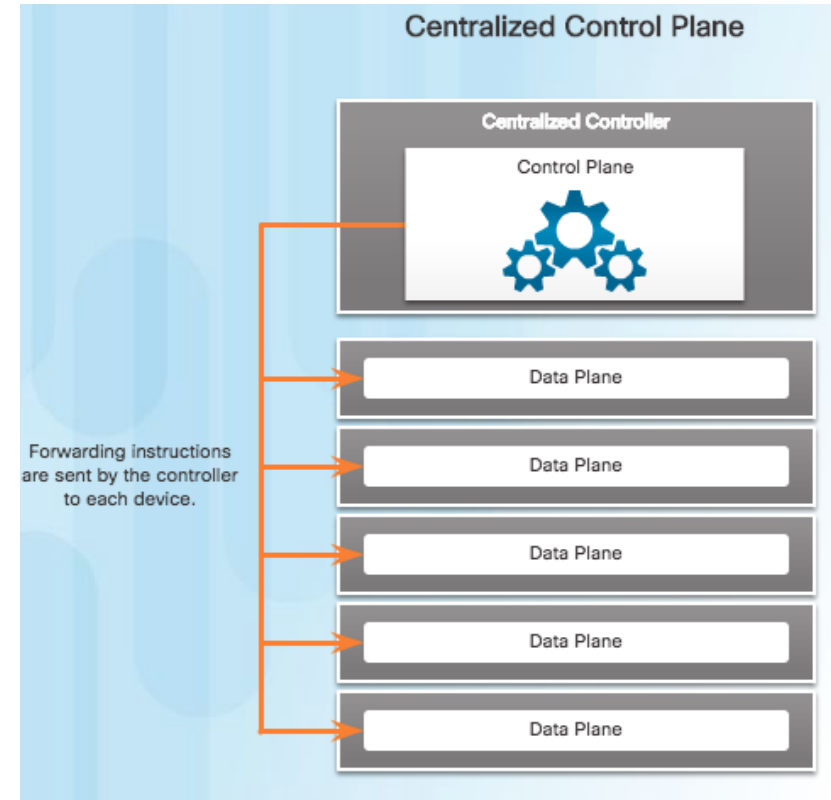


CEF is an advanced, Layer 3 IP switching technology that enables forwarding of packets to occur at the data plane without consulting the control plane. Packets are forwarded directly by the data plane based on the information contained in the Forwarding Information Base (FIB) and adjacency table, without needing to consult the information in the control plane.



# Control Plane and Data Plane (Cont.)

- To virtualize the network, the control plane function is removed from each device and is performed by a centralized controller.
- The centralized controller communicates control plane functions to each device.
- Each device can now focus on forwarding data while the centralized controller manages data flow, increases security, and provides other services.



# Software-Defined Networking

## Virtualizing the Network

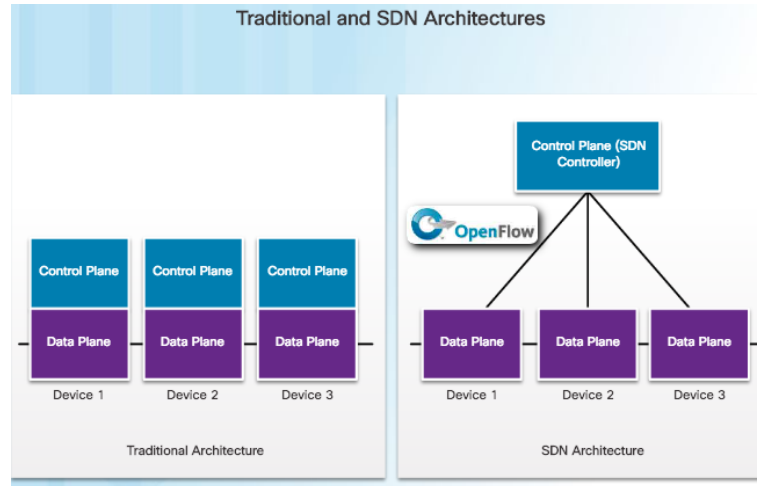
- Two major network architectures have been developed to support network virtualization:
  - Software Defined Networking (SDN) - A network architecture that virtualizes the network.
  - Cisco Application Centric Infrastructure (ACI) - A hardware solution for integrating cloud computing and data center management.
- These are some other network virtualization technologies, some of which are included as components in SDN and ACI:
  - OpenFlow - The OpenFlow protocol is a basic element in building SDN solutions.
  - OpenStack - This approach is a virtualization and orchestration platform available to build scalable cloud environments and provide an infrastructure as a service (IaaS) solution.



# Software-Defined Networking

## SDN Architecture

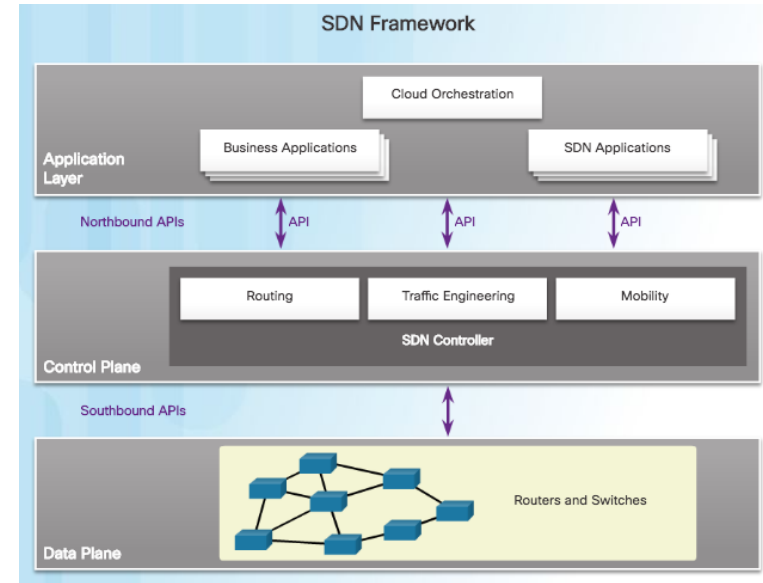
- In a traditional router or switch architecture, the control plane and data plane functions occur in the same device. Routing decisions and packet forwarding are the responsibility of the device operating system.
- Software defined networking (SDN) is a network architecture that has been developed to virtualize the network. SDN can virtualize the control plane. SDN moves the control plane from each network device to a central network intelligence and policy-making entity called the SDN controller.



# Software-Defined Networking

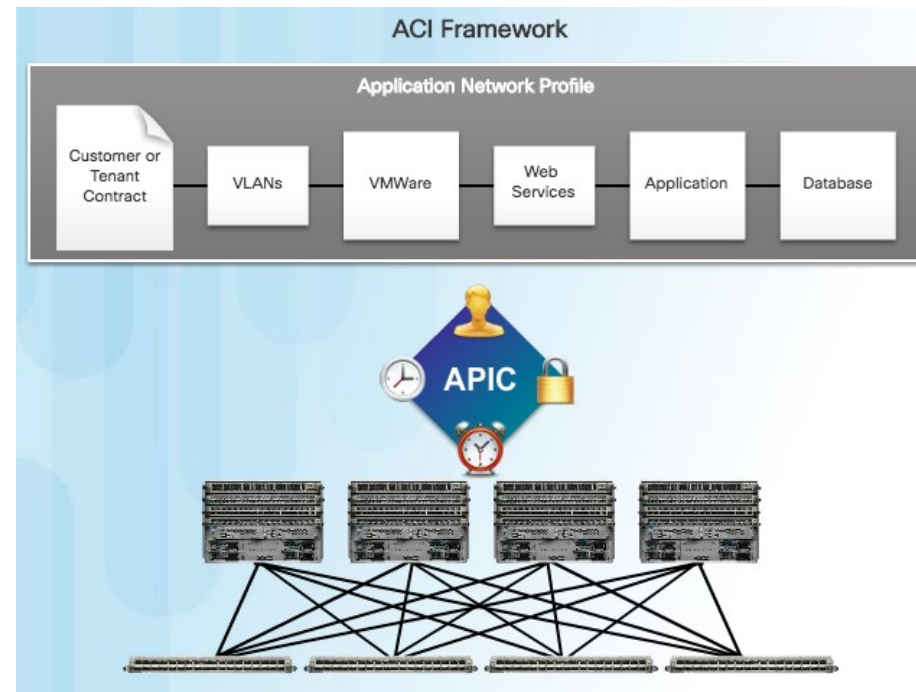
## SDN Architecture (Cont.)

- The SDN controller enables network administrators to manage and dictate how the data plane of virtual switches and routers should handle network traffic.
- The SDN controller uses northbound APIs to communicate with the upstream applications. These APIs help network administrators shape traffic and deploy services.
- The SDN controller also uses southbound APIs to define the behavior of the downstream virtual switches and routers.
- An API is a set of standardized requests that define the proper way for an application to request services from another application.
- OpenFlow is the original and widely implemented southbound API.



# Core Components of ACI

- Three core components of the ACI architecture:
  - Application Network Profile (ANP) - Collection of end-point groups (EPG), their connections, and the policies that define those connections.
  - Application Policy Infrastructure Controller (APIC) – The brains of the ACI architecture. A centralized software controller that is designed for programmability and centralized management. Translates application policies into network programming.
  - Cisco Nexus 9000 Series switches – Provide an application-aware switching fabric and work with an APIC to manage the virtual and physical network infrastructure.



APIC is positioned between the ANP and the ACI-enabled network infrastructure. The APIC translates the application requirements into a network configuration to meet those needs.

# Spine-Leaf Topology

- Cisco ACI fabric is composed of the APIC and the Cisco Nexus 9000 series switches using two-tier spine-leaf topology, as shown in the figure.
- Leaf switches always attach to the spines, but they never attach to each other.
- Spine switches only attach to the leaf and core switches (not shown).
- Cisco APICs and all other devices in the network physically attach to leaf switches.
- When compared to SDN, the APIC controller does not manipulate the data path directly.
- The APIC centralizes the policy definition and programs the leaf switches to forward traffic based on the defined policies.

