Chapter 7: Network Evolution

Connecting Networks

Cisco | Networking Academy®
Mind Wide Open™

Chapter 7

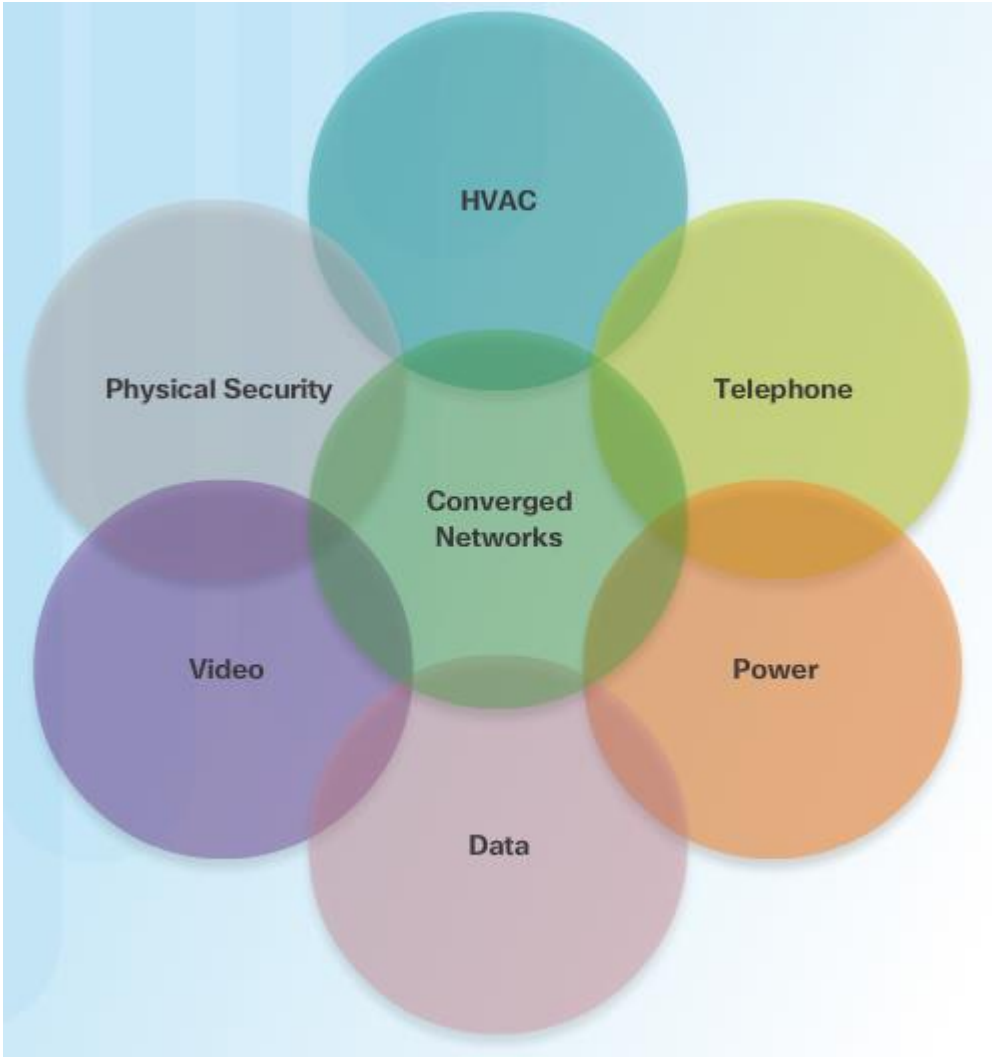
- 7.1 Internet of Things
- 7.2 Cloud and Virtualization
- 7.3 Network Programming

7.1 Internet of Things

Cisco | Networking Academy®
Mind Wide Open™

IoT Elements

- IoT = connecting things of physical world to the Internet
- Cisco estimates that 50 billion things will be connected to the Internet by 2020.
- 99% of things are currently unconnected.
- Dissimilar networks are converging to share the same infrastructure with:
  - security
  - analytics
  - management



Cisco IoT System: Six Pillars

- An model designed to managed large-scale systems of different endpoints and platforms.
- It uses a set of new and existing products and technologies
- Identifies foundational elements:
  - Connectivity, Fog Computing, Security, Data Analytics, Management and Automation, Application Enablement Platform

Cisco IoT System: Six Pillars

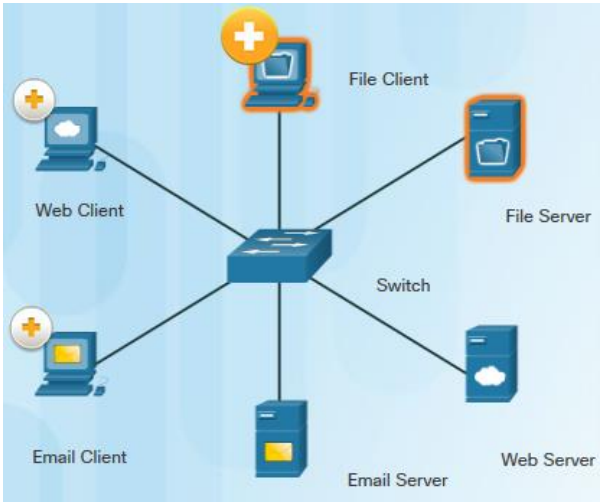
1. Network Connectivity

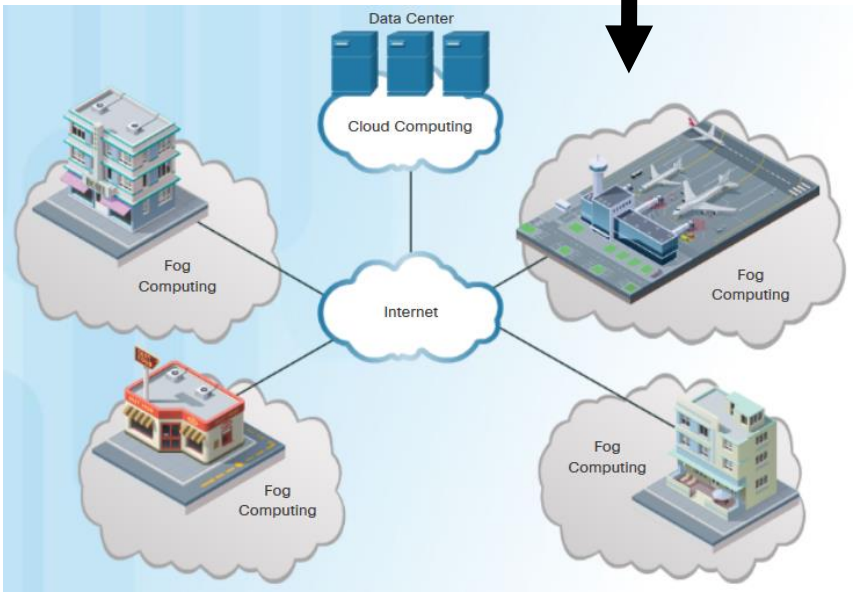
- It identifies devices that can be used to provide IoT connectivity to many diverse industries and applications.
- IoT devices:
  - Industrial routers and switches
  - IoT gateways
  - Wireless devices
  - Low-power, wide-area wireless devices
  - Embedded routers and switches

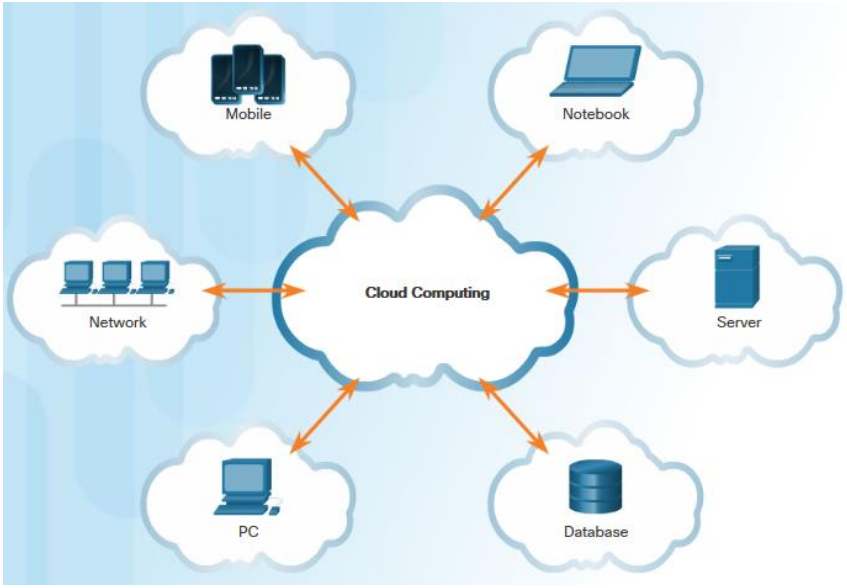
Cisco IoT System: Six Pillars

2. Fog Computing

- Client-server model: client devices request services of servers
- Cloud-computing model: services dispersed globally in distributed data centers
- Fog computing model: computing moved to edge devices that run applications locally







Cisco IoT System: Six Pillars

3. Security

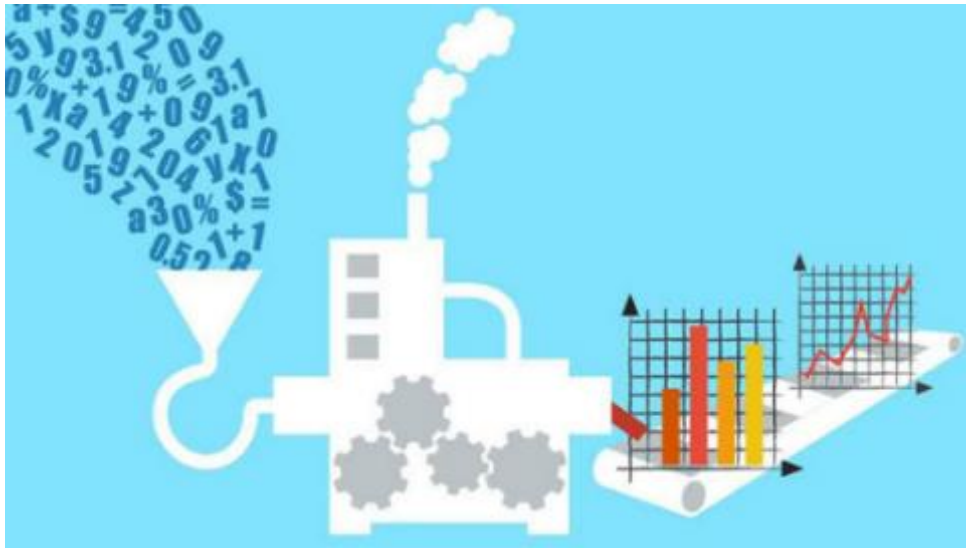
It offers scalable cybersecurity solutions, enabling an organization to quickly and effectively discover, contain, and remediate an attack to minimize damage.

- Operational technology (OT) security: power plants, factory process lines, ...
- IoT network security: securing switches, routers, ASA, FirePower IPS
- IoT physical security: surveillance IP cameras, etc.

Cisco IoT System: Six Pillars

4. Data Analytics

- Analytics infrastructure consists of distributed network components and IoT-specific, application programming interfaces (APIs).
- Number of sensors and other IoT end devices grows exponentially
  - They produce a constant stream of data
  - Structured and unstructured data
- Process data rapidly and transformed into actionable intelligence.



Big Data processing:

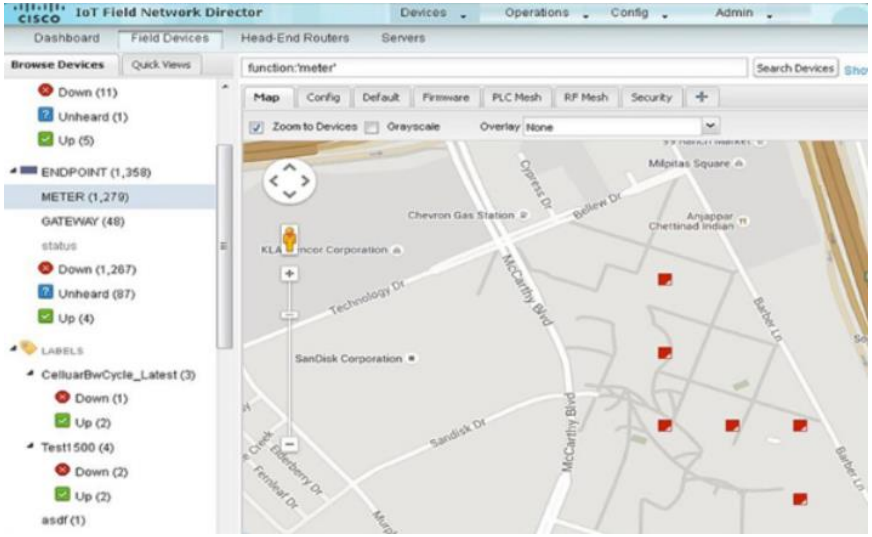
- Apacha Hadoop
- Spark
- Cassandra
- Kafka

Six Pillars of the IoT System

5. Management and Automation

Products can be customized for specific industries to provide enhanced security and control and support.

- IoT Field Network Director: management system for IoT networks
- Cisco Prime (former CiscoWorks): network management software
- Cisco Video Surveillance Manager: system for physical security and video surveillance



Cisco IoT System: Six Pillars

6. Application Enablement Platform (AEP)

- It provides the infrastructure for application hosting and application mobility between cloud and fog computing.
- Fog nodes host applications -> applications closer to the object they need to monitor, control, analyze
  - Routers with Cisco IOx (IOS + Linux) allow to host applications

7.2 Cloud and Virtualization

Cisco | Networking Academy®
Mind Wide Open™

Cloud Computing

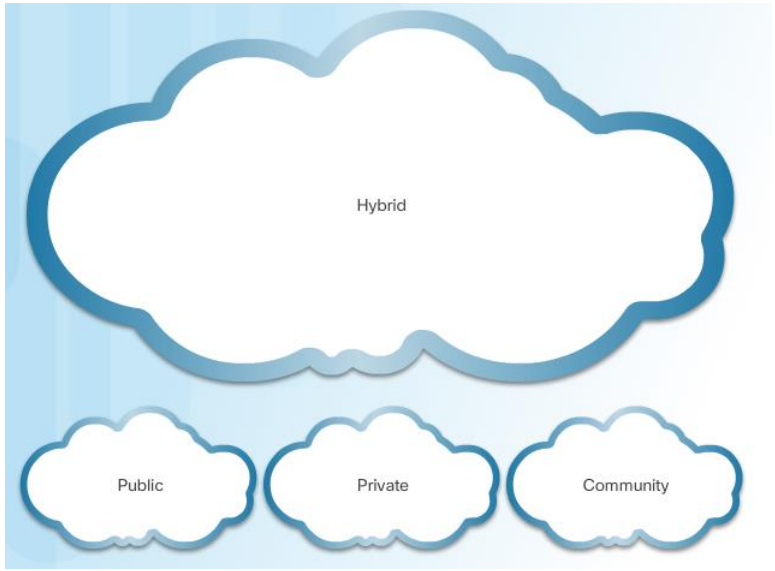
- On-demand access to a shared pool of configurable computing resources.
- It involves large numbers of computers connected through a network that can be physically located anywhere.
- Cloud provider offers services and computing in a virtual environment.

Cloud Computing Services

- *Software as a Service (SaaS)*
  - Applications delivered over the web to the end users (email, communication, Offfice 365)
- *Platform as a Service (PaaS)*
  - A user controls software development while the provider provides the networks, servers, storage, OS, middleware, database, etc.
- *Infrastructure as a Service (IaaS)*
  - Network hardware and software to power servers, storage, networks and operating systems.
- *IT as a Service (ITaaS)*
  - IT professionals support applications, platforms and infrastructures.

Cloud Models

- *Public clouds*
  - available to the general population over the Internet
- *Private clouds*
  - intended for a specific organization, strict access security.
- *Hybrid clouds*
  - made up of two or more cloud models; access based on user access rights.
- *Community clouds*
  - created for exclusive use by a specific community, such as healthcare organizations, with special authentication and confidentiality requirements.



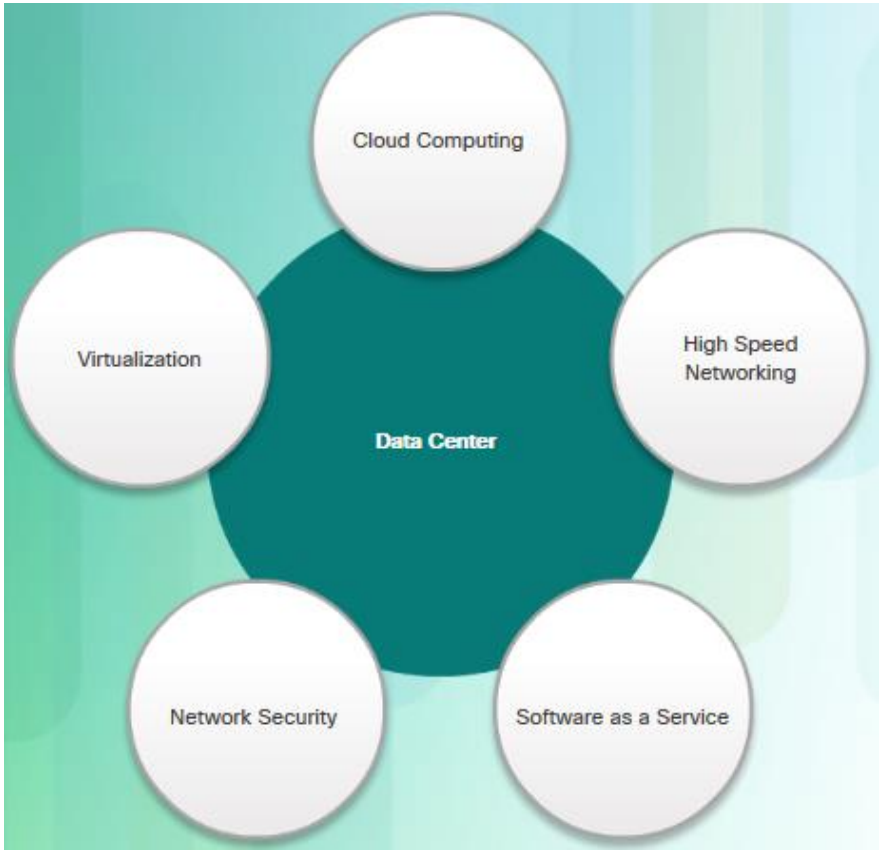
Cloud Computing vs. Data Center

Data center

- A data storage and processing facility run by an in-house IT department or leased offsite.

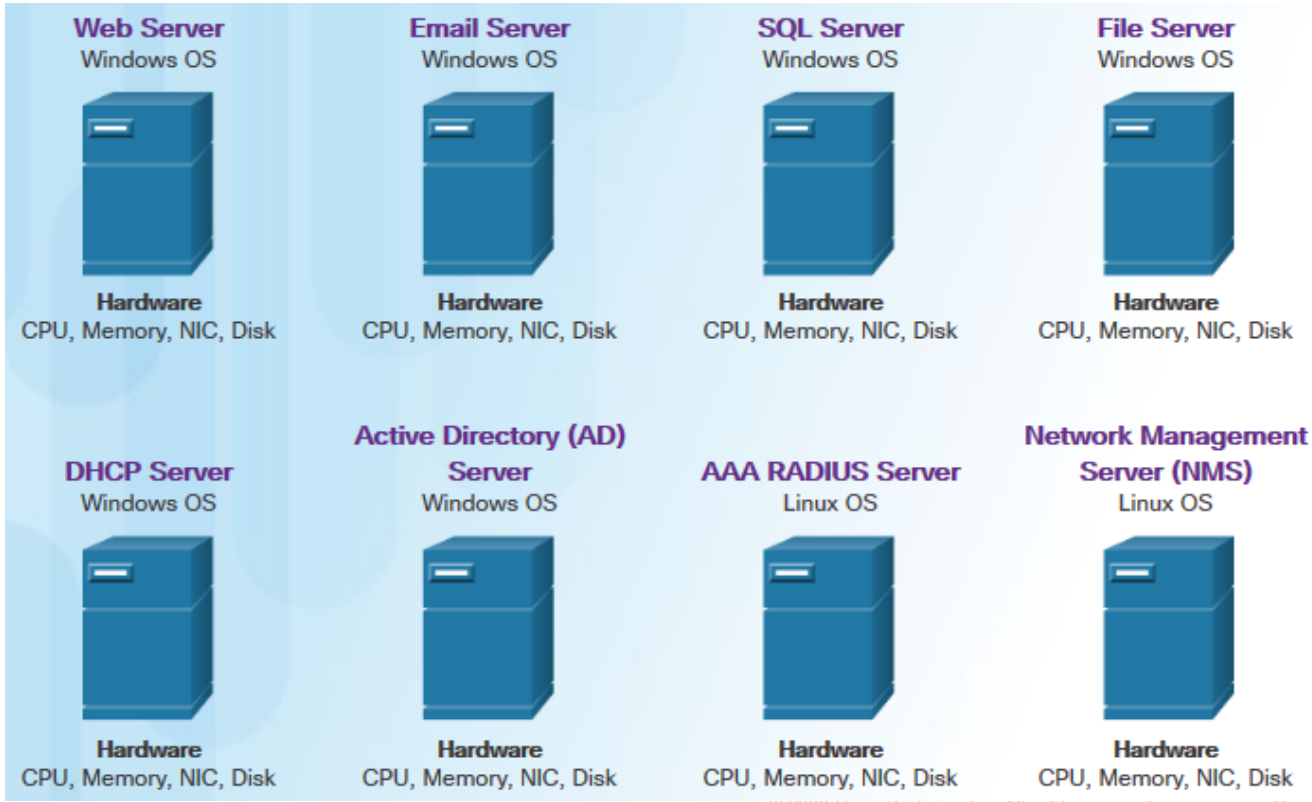
Cloud computing

- An off-premise service that offers on-demand access to a shared pool of configurable computing resources.
- A service provided by data centers.
- Cloud service providers use data center to host their cloud services and cloud-based resources.



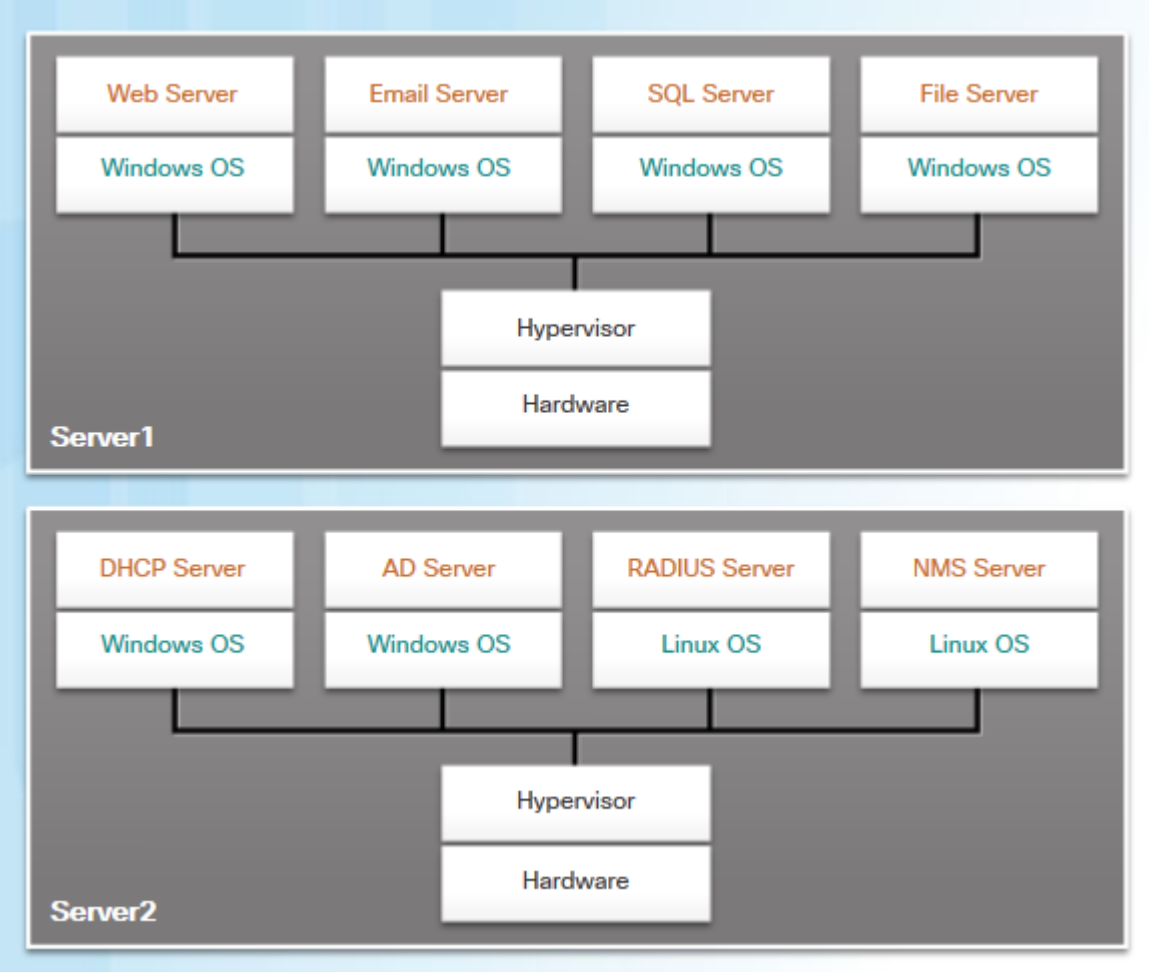
Server virtualization

- Dedicated servers
  - Historically, enterprise networks consisted of a set of application servers required for network services
  - Advantages: independent devices, medium performance required
  - Disadvantages: underused machines, purchase and maintenance costs, energy, individual configuration and management



Server virtualization

- Consolidates resources and decreases number of required servers.
- Multiple operating systems with applications residing on a single hw

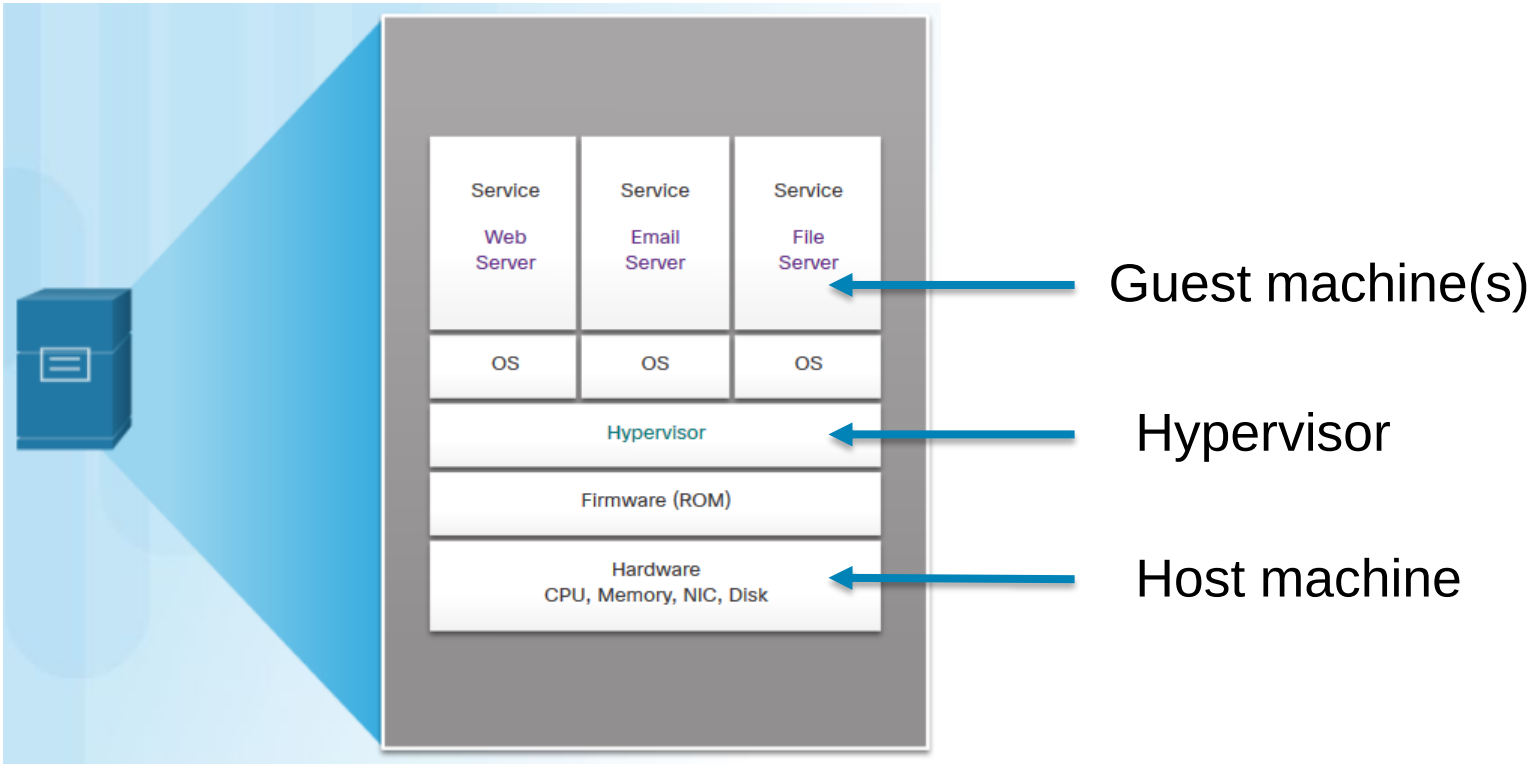


Benefits

- Less energy consumed
- Less space required
- Easier prototyping
- Faster server provisioning
- Increased server uptime
- Improved disaster recovery
- Legacy support

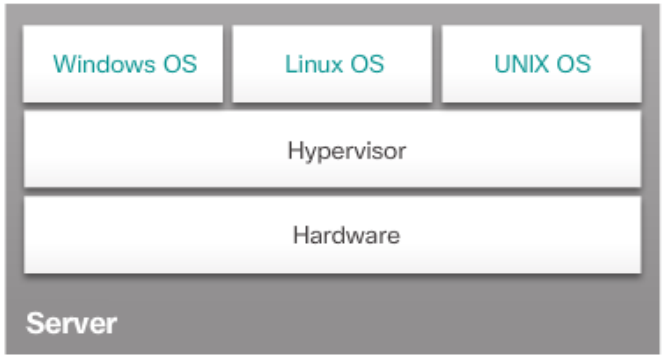
Server virtualization

- Separates the OS from the hardware allowing multiple operating systems to exist on a single hardware platform.
- The hypervisor
  - Adds an abstraction layer on top of the real physical hardware used to create virtual machines.
  - Each virtual machine runs a complete and separate operating system.



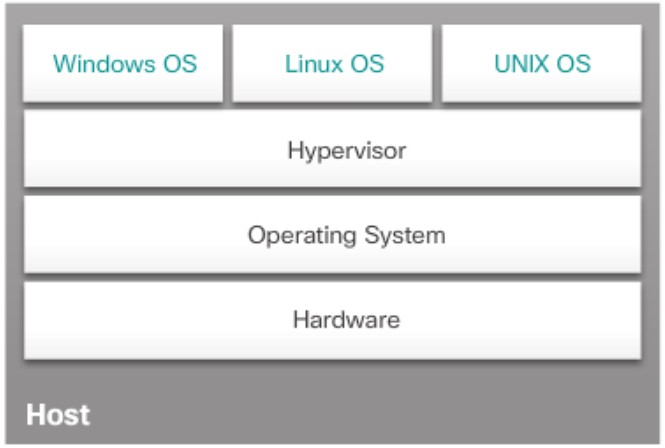
Type 1 and 2 Hypervisors

- Type 1 “Bare Metal” approach in which the hypervisor is installed directly on the hardware, e.g, enterprise servers, data centers.



  - Direct access to the hw resources.
  - More efficient, scalable, robust.
  - It requires management console.
  - E.g., Oracle VM Server for Sparc, Microsoft Hyper-V, VMware ESXi

- Type 2 “Hosted” approach in which the hypervisor is installed on top of an existing operating system.



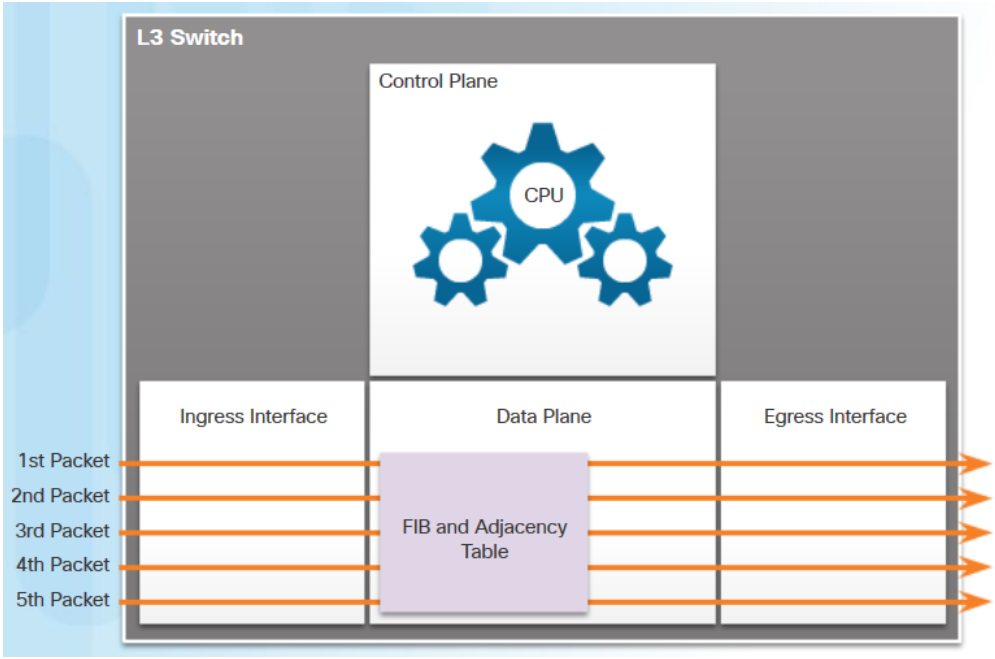
  - Guest OS runs as a process on the host.
  - Cheaper solution, less scalable.
  - Can run on common hardware and OS.
  - E.g., VMware Player, VirtualBox, Mac OS X Parallels, QEMU

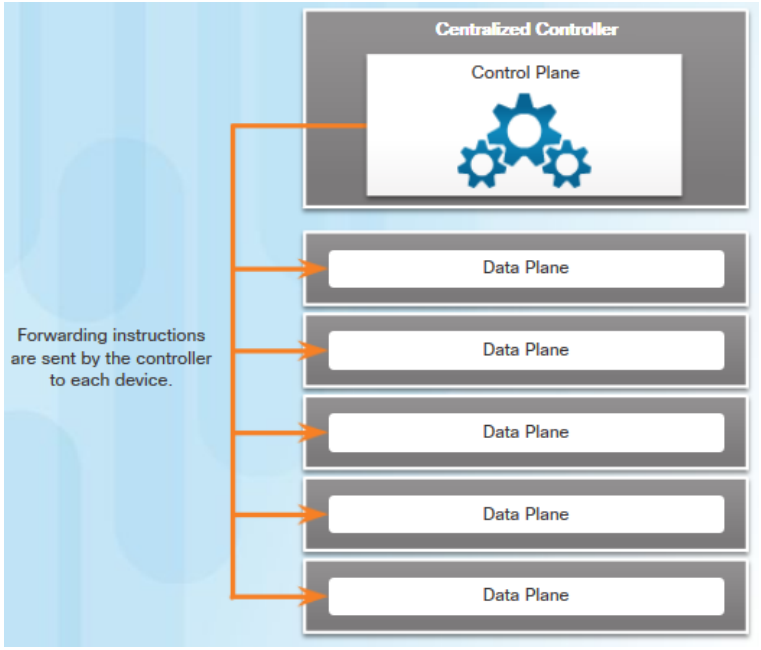
7.3 Network Programming

Cisco | Networking Academy®
Mind Wide Open™

Control Plane and Data Plane

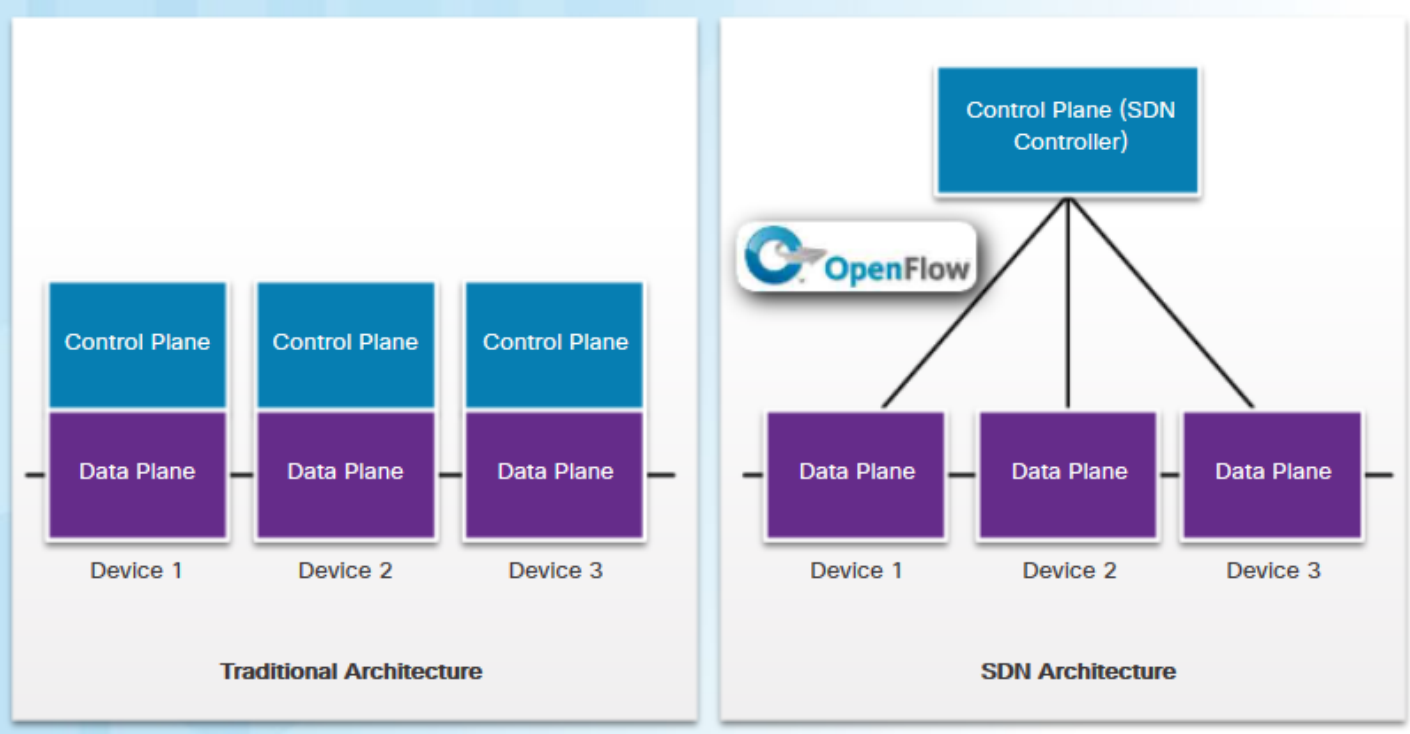
- A network device contains the following planes:
  - Control plane - Uses CPU process to calculate Layer 2 and Layer 3 route forwarding information.
  - Data plane - Forwards traffic flows using a data plane processor, such as a digital signal processor (DSP), without the CPU getting involved.
- SDN virtualizes the network, removing the control plane function from each device and performing it on a centralized controller.





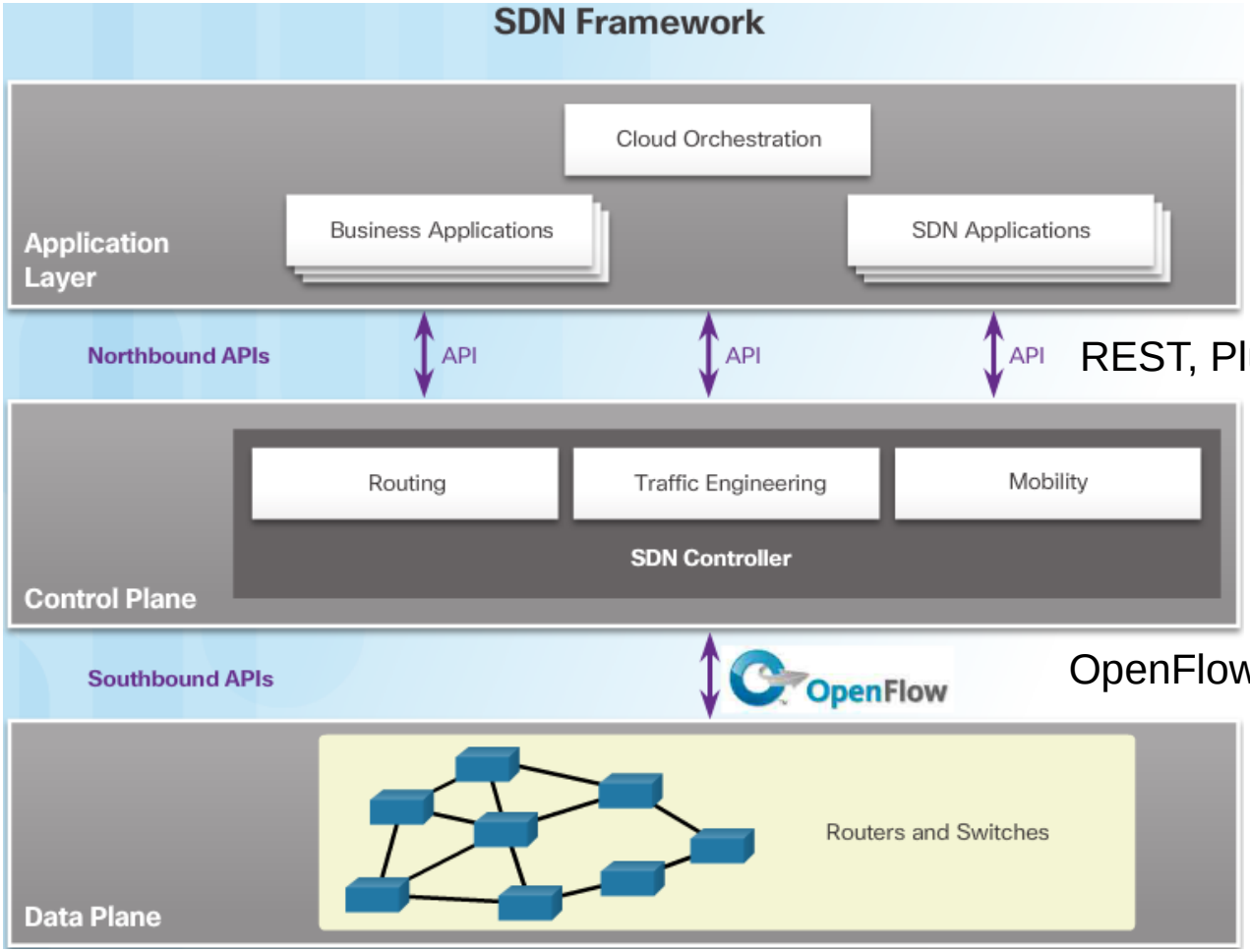
Software-Defined Networking

- Traditional Architecture
  - The control plane and data plane in the same device.
- SDN Architecture
  - SND virtualizes network -> control plane moved to a central SDN controller
  - SDN controller = a logical entity that controls data planes of virtual switches



Software-Defined Networking

- The SDN framework uses northbound APIs to communicate with upstream applications and southbound APIs to define the behavior of downstream routers and switches.



SDN Controller

- It defines the data flows that occur in the SDN data plane.
- Each flow traveling through the network gets permission from the controller.
- The controller populates 3 tables implemented in hardware via OpenFlow protocol:

Flow table

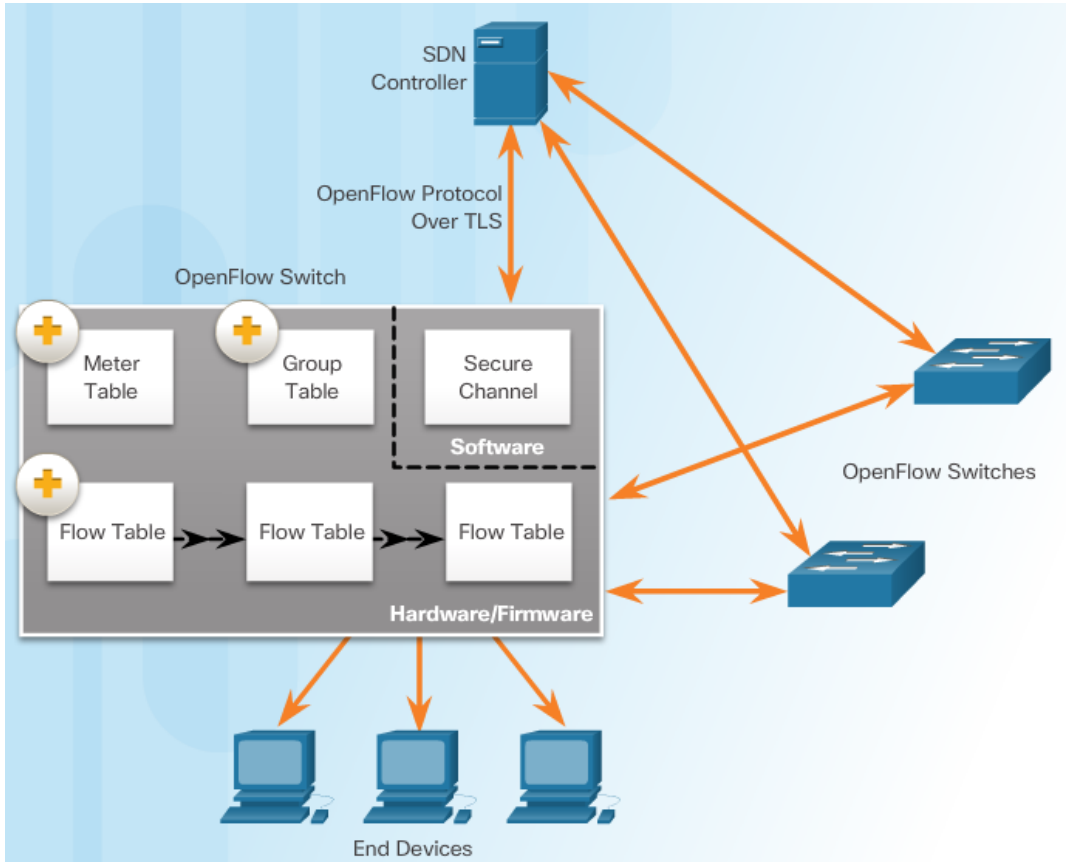
- matches incoming packets to a particular flow and specifies the functions that are to be performed on the packets.

Group table

- triggers a variety of actions that affect one or more flows.

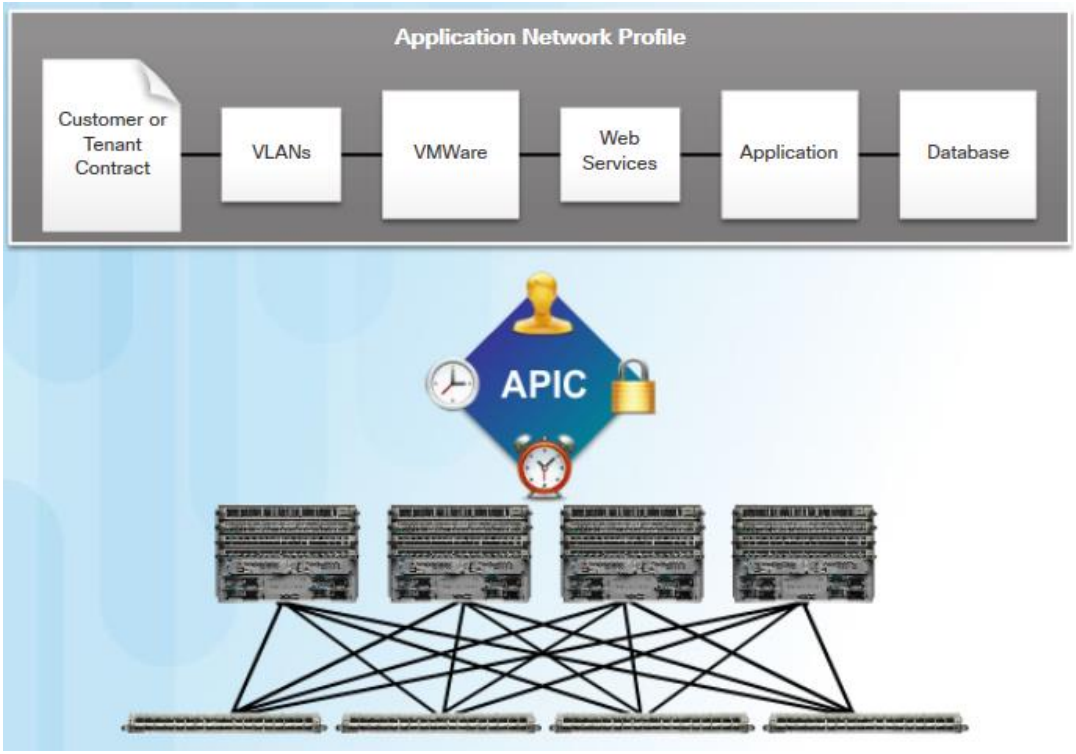
Meter table

- triggers a variety of performance-related actions on a flow.



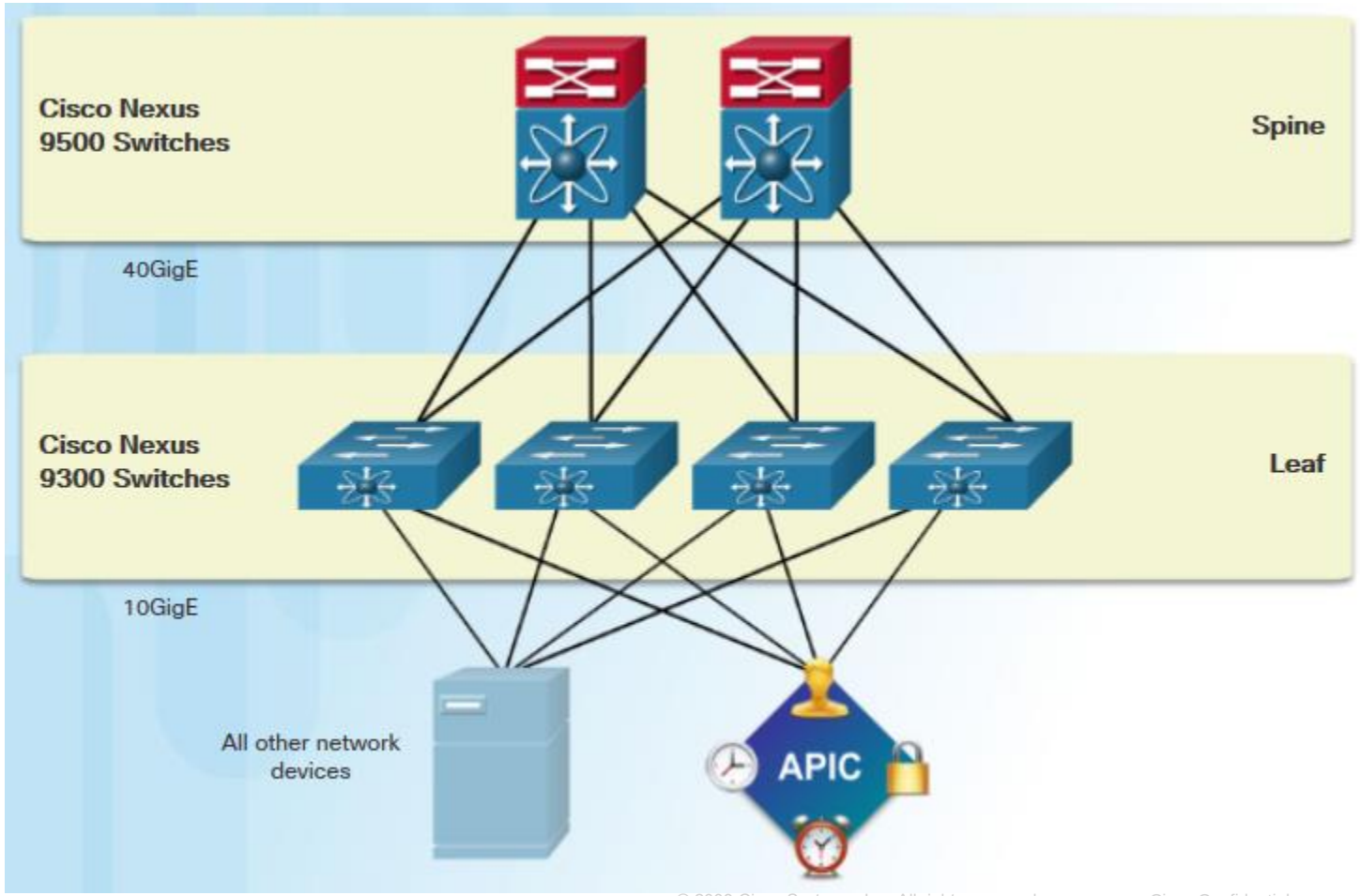
Cisco Application Centric Infrastructure (ACI)

- The ACI automates the network, accelerates application deployments, etc.
- ACI components:
  - *Application Network Profile (ANP)* - a collection of end-point groups (EPG), their connections, and the policies that define those connections
  - *Application Policy Infrastructure Controller (APIC)* - manages switches
  - *Cisco Nexus 9000 Series switches* - with application-aware switching fabric



Spine-Leaf Topology with Cisco ACI

- APIC controller
  - defines the switching policy
  - programs the leaf switches to forward traffic based on the defined policy



SDN Types

- *Device-based SDN* - applications running on the device itself, e.g., Cisco OnePK
- *Controller-based SDN* - centralized controller that has knowledge of all devices in the network. The applications manage devices and manipulate flows via API, e.g., OpenDaylight.
- *Policy-based SDN* - policy layer included, e.g., Cisco APIC-EM.