Module 13: Network Virtualization

Enterprise Networking, Security, and Automation v7.0 (ENSA)

Module Objectives

Module Title: Network Virtualization

Module Objective: Explain the purpose and characteristics of network virtualization.

Topic Title	Topic Objective
Cloud Computing	Explain the importance of cloud computing.
Virtualization	Explain the importance of virtualization.
Virtual Network Infrastructure	Describe the virtualization of network devices and services.
Software-Defined Networking	Describe software-defined networking.
Controllers	Describe controllers used in network programming.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

13.1 Cloud Computing

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cloud Overview

Cloud computing addresses 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

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cloud Services

The three main cloud computing services defined by the National Institute of Standards and Technology (NIST) in their Special Publication 800-145 are as follows:

- **Software as a Service (SaaS)** - The cloud provider is responsible for access to applications and services that are delivered over the internet.
- **Platform as a Service (PaaS)** - The cloud provider is responsible for providing users access to the development tools and services used to deliver the applications.
- **Infrastructure as a Service (IaaS)** - The cloud provider is responsible for giving IT managers access to the network equipment, virtualized network services, and supporting network infrastructure.

Cloud service providers have extended this model to also provide IT support for each of the cloud computing services (ITaaS). For businesses, ITaaS can extend the capability of the network without requiring investment in new infrastructure, training new personnel, or licensing new software.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cloud Models

There are four primary cloud models:

- **Public clouds** - Cloud-based applications and services made available to the general population.
- **Private clouds** - Cloud-based applications and services intended for a specific organization or entity, such as the government.
- **Hybrid clouds** - A hybrid cloud is made up of two or more clouds (example: part private, part public), where each part remains a separate object, but both are connected using a single architecture.
- **Community clouds** - A community cloud is created for exclusive use by a specific community. The differences between public clouds and community clouds are the functional needs that have been customized for the community. For example, healthcare organizations must remain compliant with policies and laws (e.g., HIPAA) that require special authentication and confidentiality.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cloud Computing versus Data Center

These are the correct definitions of data center and cloud computing:

- **Data center**: Typically, a data storage and processing facility run by an in-house IT department or leased offsite. Data centers are typically very expensive to build and maintain.
- **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.

Data centers are the physical facilities that provide the compute, network, and storage needs of cloud computing services. Cloud service providers use data centers to host their cloud services and cloud-based resources.

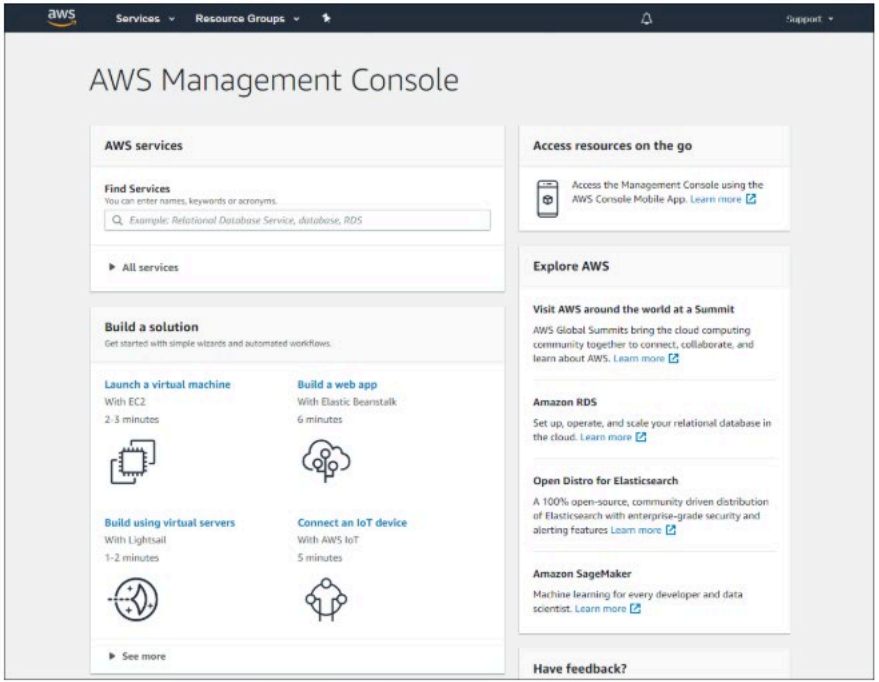
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

13.2 Virtualization

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cloud Computing and Virtualization

- The terms “cloud computing” and “virtualization” are often used interchangeably; however, they mean different things. Virtualization is the foundation of cloud computing. Without it, cloud computing, as it is most-widely implemented, would not be possible.
- Virtualization separates the operating system (OS) from the hardware. Various providers offer virtual cloud services that can dynamically provision servers as required. These virtualized instances of servers are created on demand.

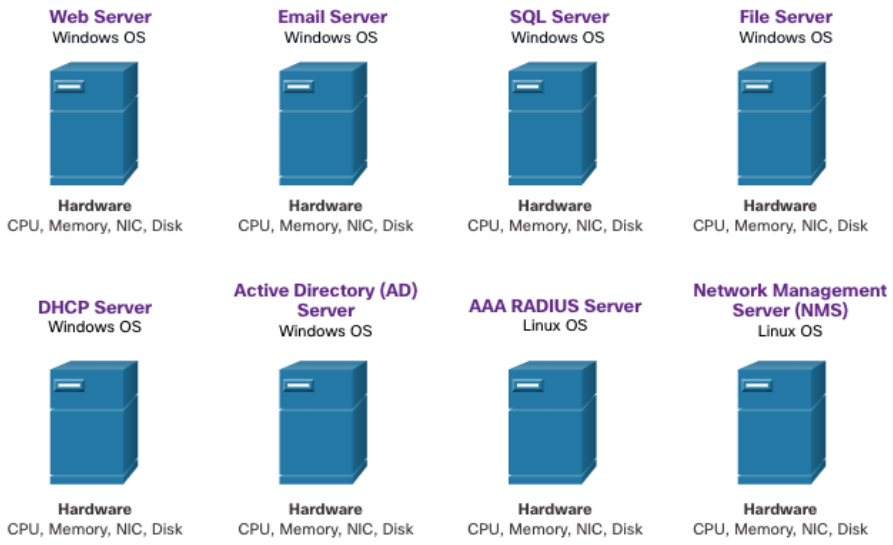


© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Dedicated Servers

Historically, enterprise servers consisted of a server OS, such as Windows Server or Linux Server, installed on specific hardware. All of a server's RAM, processing power, and hard drive space were dedicated to the service provided (e.g., Web, email services, etc.).

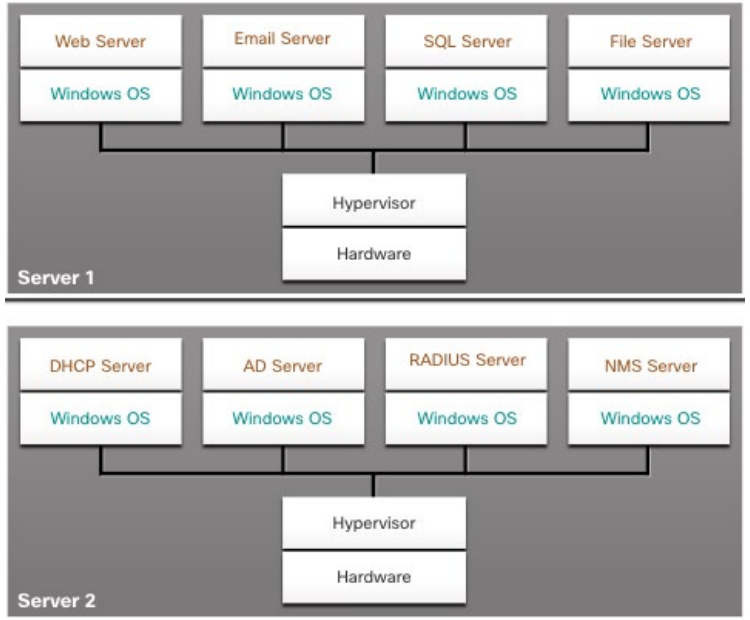
- When a component fails, the service that is provided by this server becomes unavailable. This is known as a single point of failure.
- Dedicated servers were generally underused. They often sat idle for long periods of time, waiting until there was a need to deliver the specific service they provide. These servers wasted energy and took up more space than was warranted by the amount of service provided. This is known as server sprawl.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Server Virtualization

- Server virtualization takes advantage of idle resources and consolidates the number of required servers. This also allows for multiple operating systems to exist on a single hardware platform.
- The use of virtualization normally includes redundancy to protect from a single point of failure.
- The hypervisor is a program, firmware, or hardware that adds an abstraction layer on top of the 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.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Advantages of Virtualization

One major advantage of virtualization is overall reduced cost:

- Less equipment is required
- Less energy is consumed
- Less space is required

These are additional benefits of virtualization:

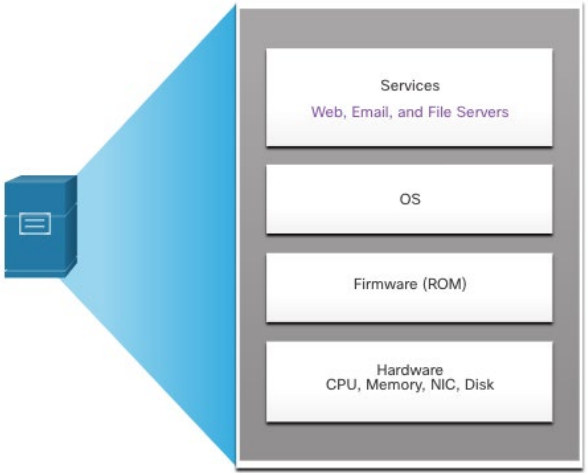
- Easier prototyping
- Faster server provisioning
- Increased server uptime
- Improved disaster recovery
- Legacy support

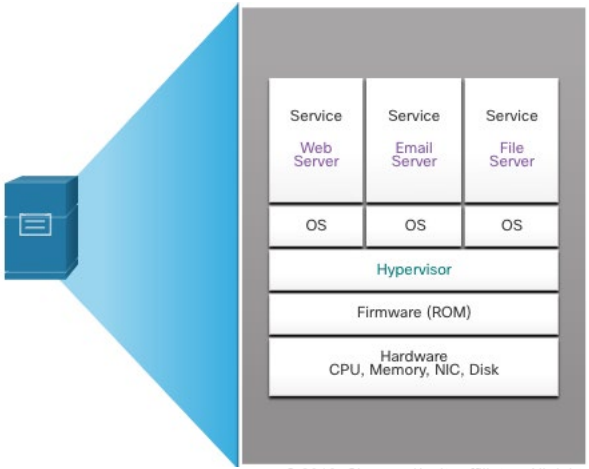
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Abstraction Layers

A computer system consists of the following abstraction layers: Services, OS, Firmware, and Hardware.

- At each of these layers of abstraction, some type of programming code is used as an interface between the layer below and the layer above.
- A hypervisor is installed between the firmware and the OS. The hypervisor can support multiple instances of OSs.

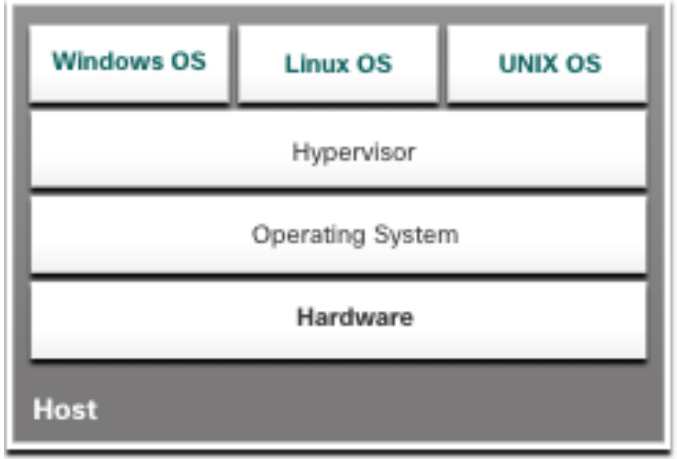




© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Type 2 Hypervisors

- A Type 2 hypervisor is software that creates and runs VM instances. The computer, on which a hypervisor is supporting one or more VMs, is a host machine. Type 2 hypervisors are also called hosted hypervisors.
- A big advantage of Type 2 hypervisors is that management console software is not required.



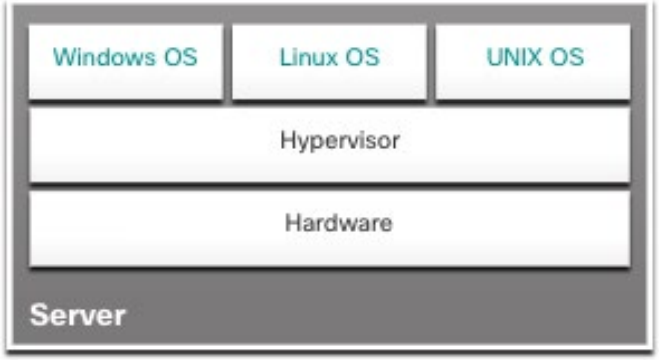
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

13.3 Virtual Network Infrastructure

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Type 1 Hypervisors

- Type 1 hypervisors are also called the “bare metal” approach because the hypervisor is installed directly on the hardware. Type 1 hypervisors are usually used on enterprise servers and data center networking devices.
- With Type 1 hypervisors, the hypervisor is installed directly on the server or networking hardware. Then, instances of an OS are installed on the hypervisor, as shown in the figure. Type 1 hypervisors have direct access to the hardware resources. Therefore, they are more efficient than hosted architectures. Type 1 hypervisors improve scalability, performance, and robustness.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

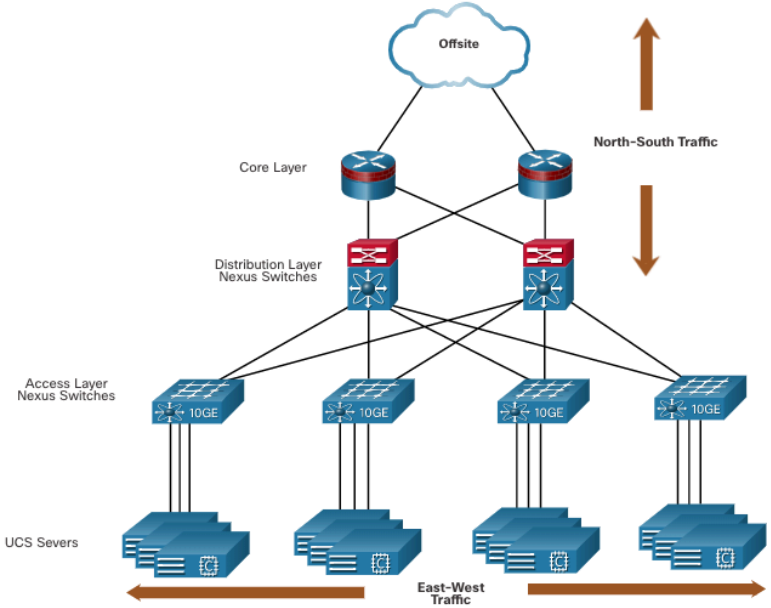
Installing a VM on a Hypervisor

- Type 1 hypervisors require a “management console” to manage the hypervisor. Management software is used to manage multiple servers using the same hypervisor. The management console can automatically consolidate servers and power on or off servers as required.
- The management console provides recovery from hardware failure. If a server component fails, the management console automatically moves the VM to another server. Cisco Unified Computing System (UCS) Manager controls multiple servers and manages resources for thousands of VMs.
- Some management consoles also allow server over allocation. Over allocation is when multiple OS instances are installed, but their memory allocation exceeds the total amount of memory that a server has. Over allocation is a common practice because all four OS instances rarely require the all their allocated resources at any one moment.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The Complexity of Network Virtualization

- Server virtualization hides server resources. This can create problems when using traditional network architectures.
- VMs are movable, and the network administrator must be able to add, drop, and change network resources and profiles to support their mobility. This process would be manual and time-consuming with traditional network switches.
- Traffic flows differ from the traditional client-server model. Typically, there is a considerable amount of traffic being exchanged between virtual servers (East-West traffic) that changes in location and intensity over time. North-South traffic is typically traffic destined for offsite locations such as another data center, other cloud providers, or the internet.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The Complexity of Network Virtualization (Cont.)

- Dynamic ever-changing traffic requires 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.
- The network infrastructure can also benefit from virtualization. Network functions can be virtualized. Each network device can be segmented into multiple virtual devices that operate as independent devices. Examples include subinterfaces, virtual interfaces, VLANs, and routing tables. Virtualized routing is called virtual routing and forwarding (VRF).

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

13.4 Software-Defined Networking

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Control Plane and Data Plane

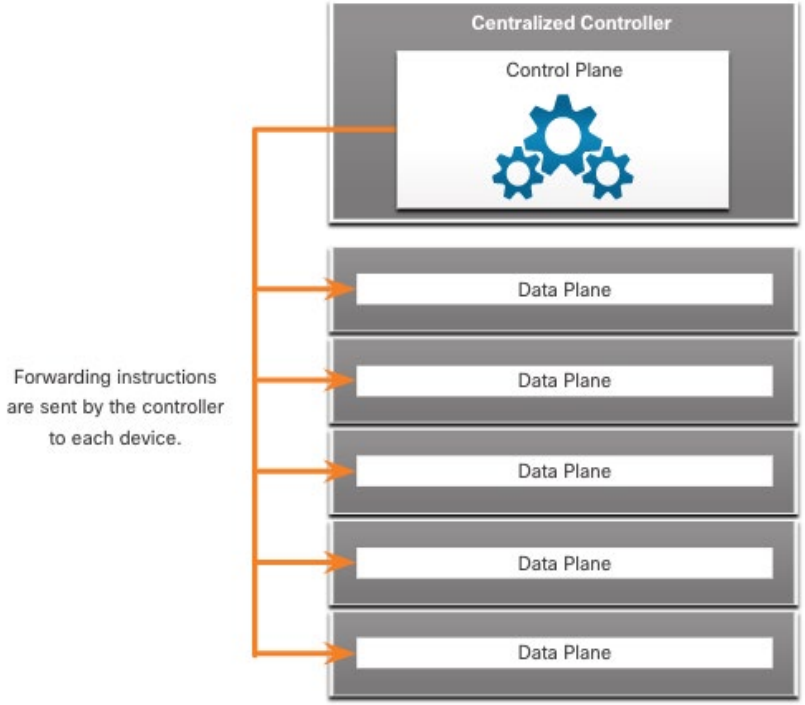
A network device contains the following planes:

- **Control plane** - This is typically regarded as the brains of a device. It is used to make forwarding decisions. The control plane contains Layer 2 and Layer 3 route forwarding mechanisms, such as routing protocol neighbor tables and topology tables, IPv4 and IPv6 routing tables, STP, and the ARP table. Information sent to the control plane is processed by the CPU.
- **Data plane** - Also called the forwarding plane, this plane is typically the switch fabric connecting the various network ports on a device. The data plane of each device is used to forward traffic flows. Routers and switches use information from the control plane to forward incoming traffic out the appropriate egress interface. Information in the data plane is typically processed by a special data plane processor without the CPU getting involved.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Control Plane and Data Plane (Cont.)

- 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.
- SDN is basically the separation of the control plane and data plane. 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.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Control Plane and Data Plane (Cont.)

- The **management plane** is responsible for managing a device through its connection to the network.
- Network administrators use applications such as Secure Shell (SSH), Trivial File Transfer Protocol (TFTP), Secure FTP, and Secure Hypertext Transfer Protocol (HTTPS) to access the management plane and configure a device.
- The management plane is how you have accessed and configured devices in your networking studies. In addition, protocols like Simple Network Management Protocol (SNMP), use the management plane.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Network Virtualization Technologies

Two major network architectures have been developed to support network virtualization:

- **Software-Defined Networking (SDN)** - A network architecture that virtualizes the network, offering a new approach to network administration and management that seeks to simplify and streamline the administration process.
- **Cisco Application Centric Infrastructure (ACI)** - A purpose-built hardware solution for integrating cloud computing and data center management.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Network Virtualization Technologies (Cont.)

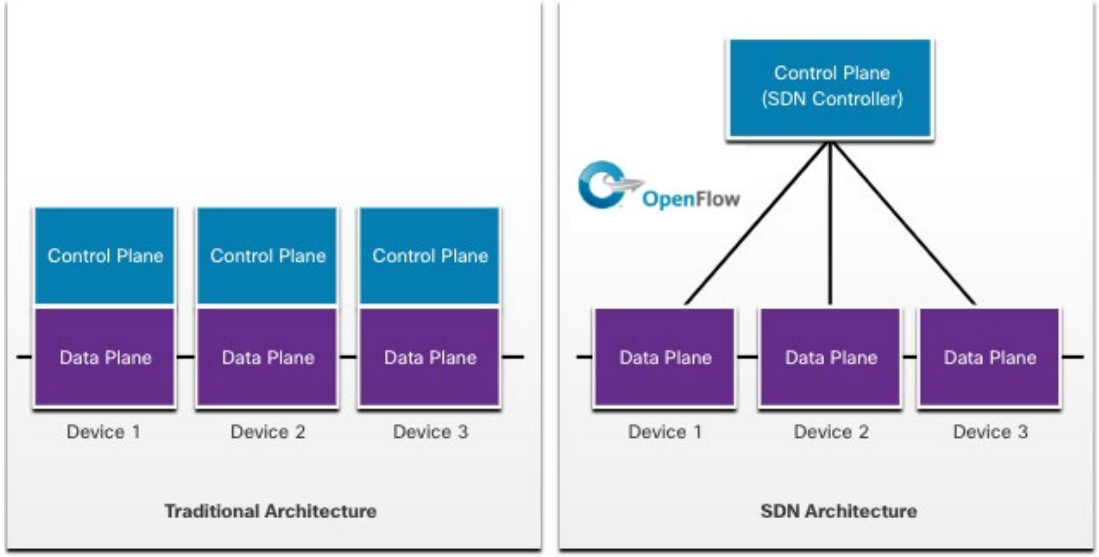
Components of SDN may include the following:

- **OpenFlow** - This approach was developed at Stanford University to manage traffic between routers, switches, wireless access points, and a controller. The OpenFlow protocol is a basic element in building SDN solutions.
- **OpenStack** - This approach is a virtualization and orchestration platform designed to build scalable cloud environments and provide an IaaS solution. OpenStack is often used with Cisco ACI. Orchestration in networking is the process of automating the provisioning of network components such as servers, storage, switches, routers, and applications.
- **Other components** - Other components include Interface to the Routing System (I2RS), Transparent Interconnection of Lots of Links (TRILL), Cisco FabricPath (FP), and IEEE 802.1aq Shortest Path Bridging (SPB).

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Traditional and SDN Architectures

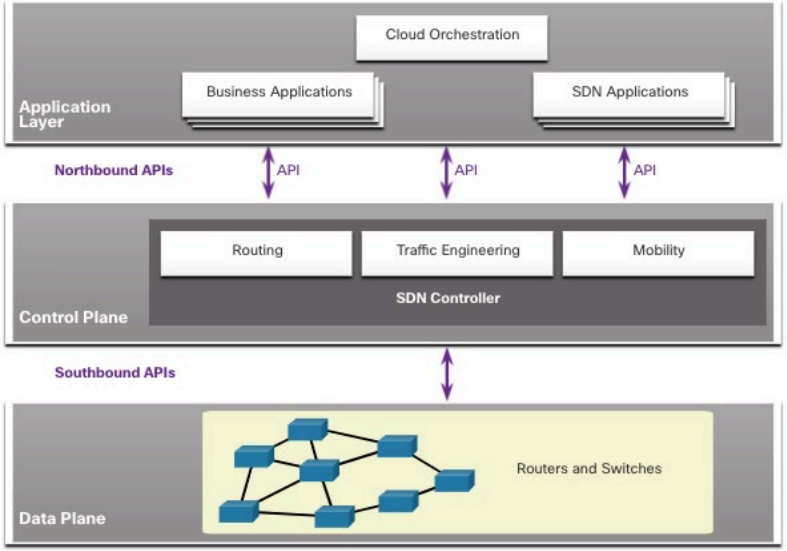
In a traditional router or switch architecture, the control plane and data plane functions occur in the same device. Routing decisions and packet forwarding are the responsibility of the device operating system. In SDN, management of the control plane is moved to a centralized SDN controller. The figure compares traditional and SDN architectures.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Traditional and SDN Architectures (Cont.)

- The SDN controller is a logical entity that enables network administrators to manage and dictate how the data plane of switches and routers should handle network traffic. It orchestrates, mediates, and facilitates communication between applications and network elements.
- The complete SDN framework is shown in the figure. Note the use of Application Programming Interfaces (APIs). An API is a standardized definition of the proper way for an application to request services from another application.
- The SDN controller uses northbound APIs to communicate with the upstream applications, helping network administrators shape traffic and deploy services. The SDN controller uses southbound APIs to define the behavior of the data planes on downstream switches and routers. OpenFlow is a widely implemented southbound API.



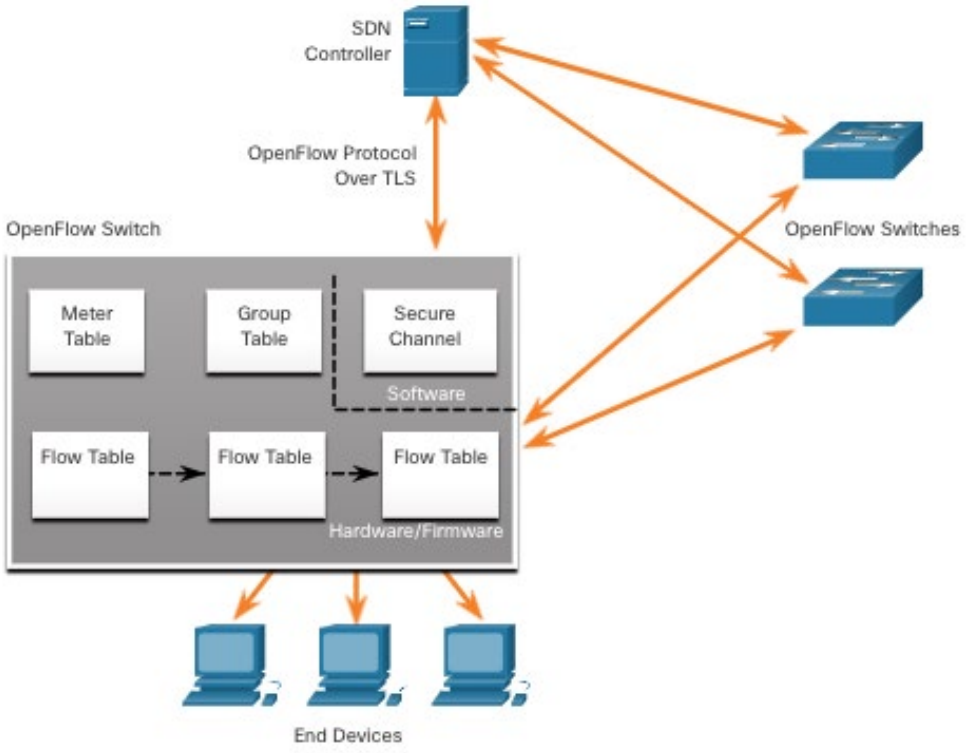
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

13.5 Controllers

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

SDN Controller and Operations

- The SDN controller defines the data flows between the centralized control plane and the data planes on individual routers and switches.
- Each flow traveling through the network must first get permission from the SDN controller, which verifies that the communication is permissible according to the network policy.
- All complex functions are performed by the controller. The controller populates flow tables. Switches manage the flow tables.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

SDN Controller and Operations (Cont.)

Within each switch, a series of tables implemented in hardware or firmware are used to manage the flows of packets through the switch. To the switch, a flow is a sequence of packets that matches a specific entry in a flow table.

The three table types shown in the previous figure are as follows:

- **Flow Table** - This table matches incoming packets to a particular flow and specifies the functions that are to be performed on the packets. There may be multiple flow tables that operate in a pipeline fashion.
- **Group Table** - A flow table may direct a flow to a Group Table, which may trigger a variety of actions that affect one or more flows.
- **Meter Table** - This table triggers a variety of performance-related actions on a flow including the ability to rate-limit the traffic.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Core Components of ACI

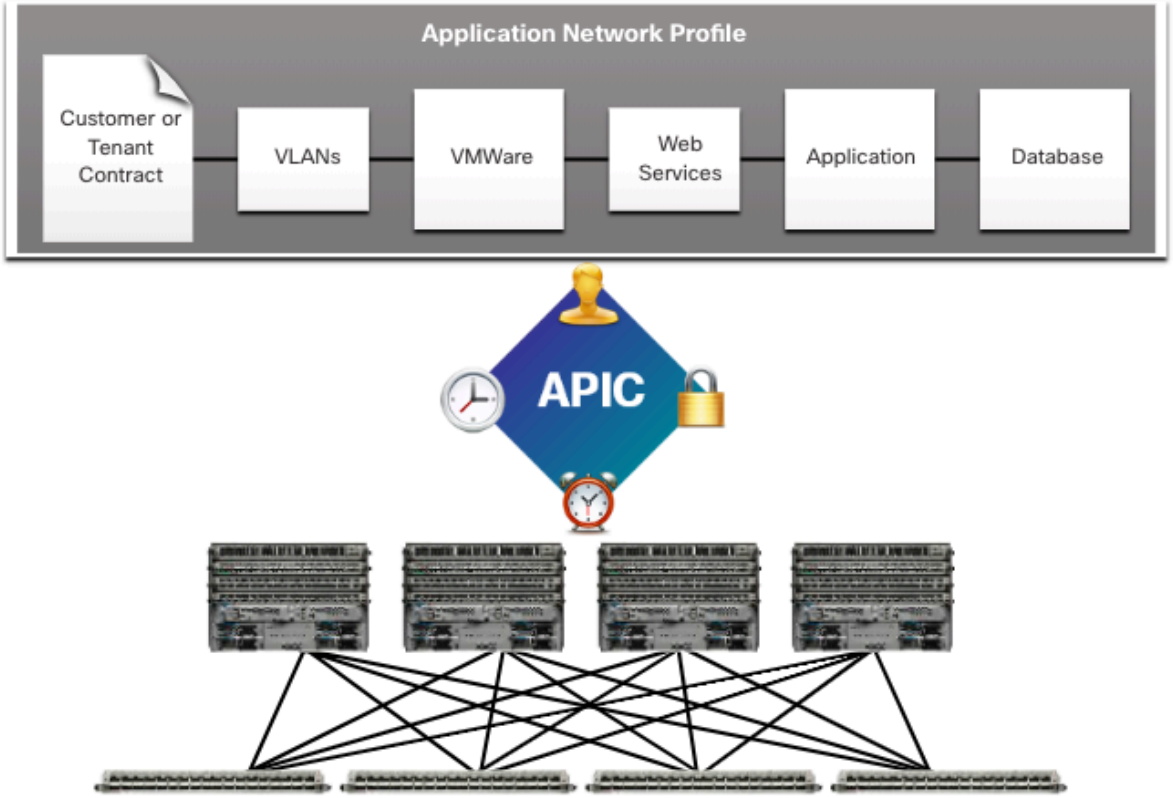
There are three core components of the ACI architecture:

- **Application Network Profile (ANP)** - An ANP is a collection of end-point groups (EPG), their connections, and the policies that define those connections.
- **Application Policy Infrastructure Controller (APIC)** - APIC is a centralized software controller that manages and operates a scalable ACI clustered fabric. It is designed for programmability and centralized management. It translates application policies into network programming.
- **Cisco Nexus 9000 Series switches** - These switches provide an application-aware switching fabric and work with an APIC to manage the virtual and physical network infrastructure.

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

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

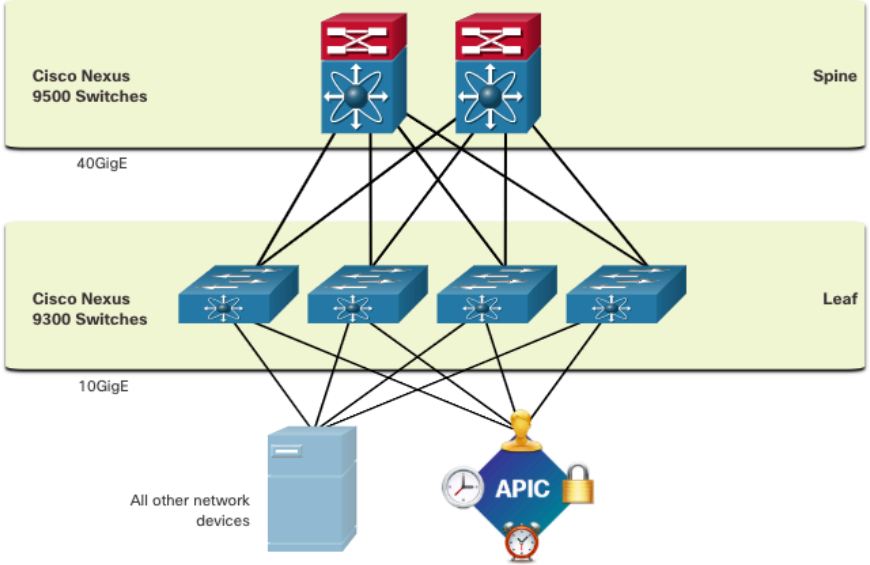
Core Components of ACI (Cont.)



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Spine-Leaf Topology

- The 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. The leaf switches attach to the spines, but they never attach to each other. Similarly, the spine switches only attach to the leaf and core switches (not shown). In this two-tier topology, everything is one hop from everything else.
- When compared to SDN, the APIC controller does not manipulate the data path directly. Instead, the APIC centralizes the policy definition and programs the leaf switches to forward traffic based on the defined policies.

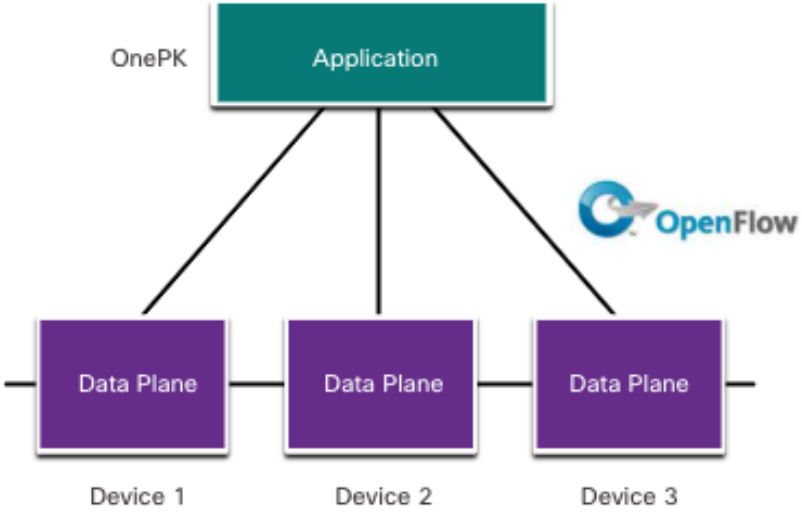


© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

SDN Types

The Cisco Application Policy Infrastructure Controller - Enterprise Module (APIC-EM) extends ACI aimed at enterprise and campus deployments. To better understand APIC-EM, it is helpful to take a broader look at the three types of SDN:

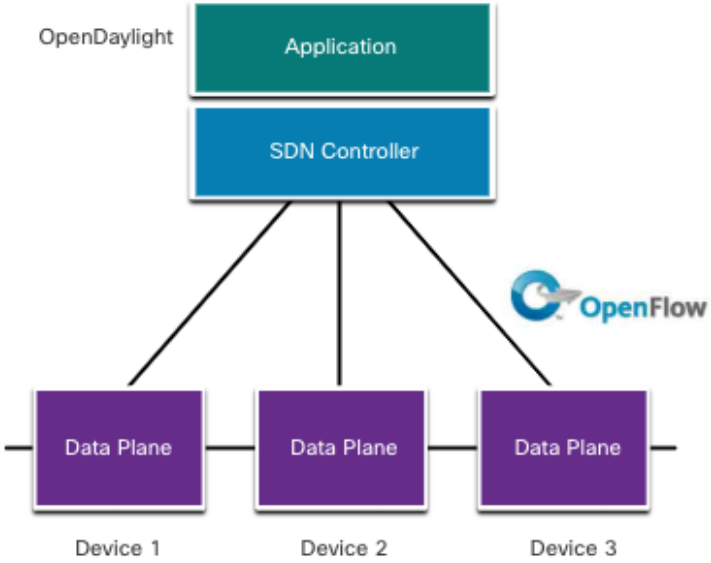
- **Device-based SDN:** Devices are programmable by applications running on the device itself or on a server in the network, as shown in the figure.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

SDN Types (Cont.)

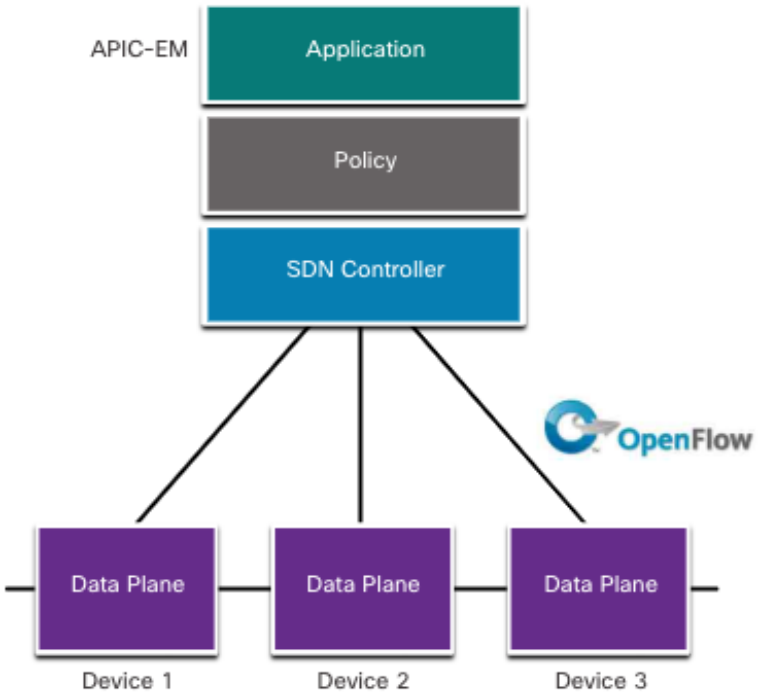
Controller-based SDN: Uses a centralized controller that has knowledge of all devices in the network, as shown in the figure. The applications can interface with the controller responsible for managing devices and manipulating traffic flows throughout the network. The Cisco Open SDN Controller is a commercial distribution of OpenDaylight.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

SDN Types (Cont.)

Policy-based SDN: Similar to controller-based SDN where a centralized controller has a view of all devices in the network, as shown in the figure. Policy-based SDN includes an additional Policy layer that operates at a higher level of abstraction. It uses built-in applications that automate advanced configuration tasks via a guided workflow and user-friendly GUI. No programming skills are required. Cisco APIC-EM is an example of this type of SDN.

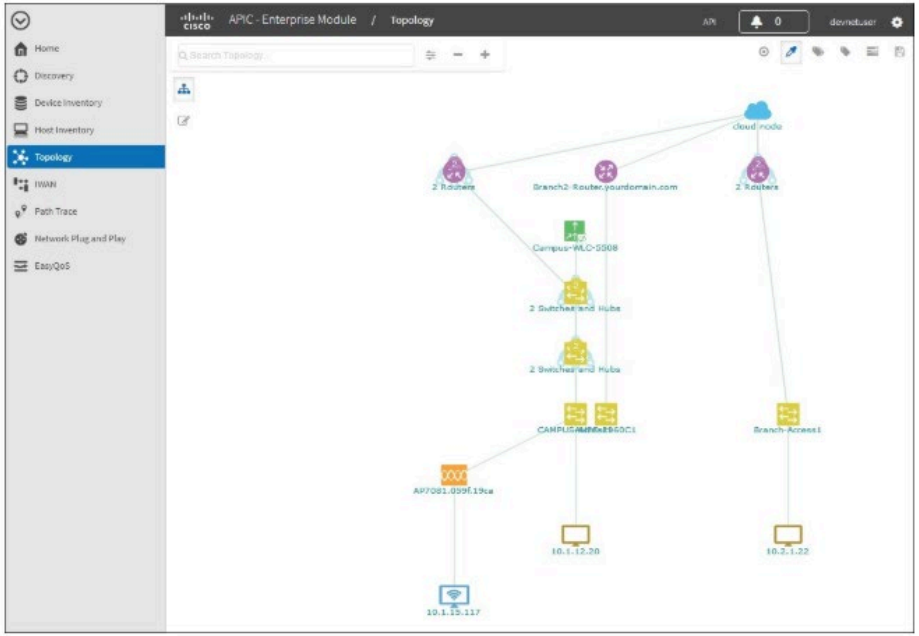


© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

APIC-EM Features

Cisco APIC-EM provides a single interface for network management including:

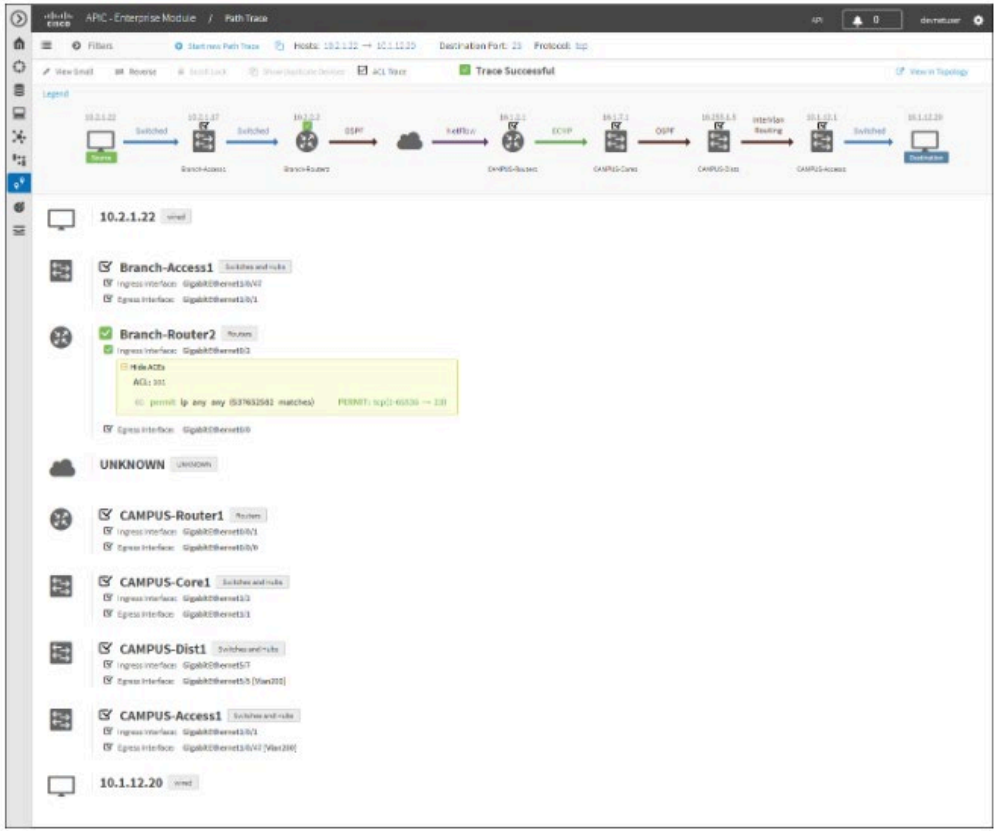
- Discovering and accessing device and host inventories.
- Viewing the topology (as shown in the figure).
- Tracing a path between end points.
- Setting policies.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

APIC-EM Path Trace

The APIC-EM Path Trace tool allows the administrator to easily visualize traffic flows and discover any conflicting, duplicate, or shadowed ACL entries. This tool examines specific ACLs on the path between two end nodes, displaying any potential issues. You can see where any ACLs along the path either permitted or denied your traffic, as shown in the figure. Notice how Branch-Router2 is permit all traffic. The network administrator can now make adjustments, if necessary, to better filter traffic.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

CISCO