CCNA 3 v7.0 Curriculum: Module 13 – Network Virtualization

itexamanswers.net/ccna-3-v7-0-curriculum-module-13-network-virtualization.html

April 16, 2020

13.0. Introduction

13.0.1. Why should I take this module?

Welcome to Network Virtualization!

Imagine you live in a two-bedroom house. You use the second bedroom for storage. The second bedroom is packed full of boxes, but you still have more to place in storage! You could consider building an addition on your house. It would be a costly endeavor and you may not need that much space forever. You decide to rent a storage unit for the overflow.

Similar to a storage unit, network virtualization and cloud services can provide a business with options other than adding servers into their own data center. In addition to storage, it offers other advantages. Get started with this module to learn more about what virtualization and cloud services can do!

13.0.2. What will I learn to do in this module?

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.

13.1. Cloud Computing

13.1.1 Video – Cloud and Virtualization

Click Play for an overview of cloud computing and virtualization.

13.1.2. Cloud Overview

In the previous video, an overview of cloud computing was explained. Cloud computing involves large numbers of computers connected through a network that can be physically located anywhere. Providers rely heavily on virtualization to deliver their cloud computing services. Cloud computing can reduce operational costs by using resources more efficiently. 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

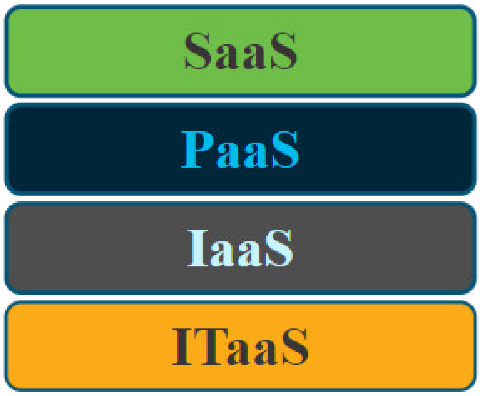
Cloud computing, with its "pay-as-you-go" model, allows organizations to treat computing and storage expenses more as a utility rather than investing in infrastructure. Capital expenditures are transformed into operating expenditures.

13.1.3. Cloud Services

Cloud services are available in a variety of options, tailored to meet customer requirements. 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, such as email, communication, and Office 365 that are delivered over the internet. The user does not manage any aspect of the cloud services except for limited user-specific application settings. The user only needs to provide their data.
- **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. These users are typically programmers and may have control over the configuration settings of the cloud provider's application hosting environment.
- **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. Using this cloud service allows IT managers to deploy and run software code, which can include operating systems and applications.

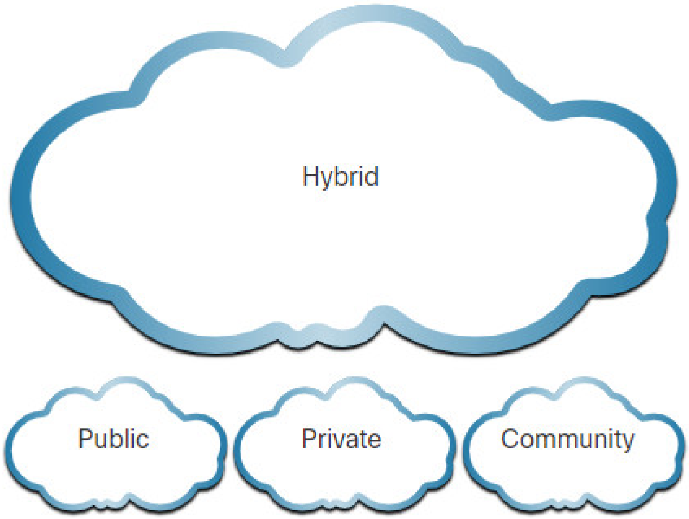
Cloud service providers have extended this model to also provide IT support for each of the cloud computing services (ITaaS), as shown in the figure. For businesses, ITaaS can extend the capability of the network without requiring investment in new infrastructure, training new personnel, or licensing new software. These services are available on demand and delivered economically to any device anywhere in the world without compromising security or function.



13.1.4. Cloud Models

There are four primary cloud models, as shown in the figure.

- **Public clouds** – Cloud-based applications and services offered in a public cloud are 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. The public cloud uses the internet to provide services.
- **Private clouds** – Cloud-based applications and services offered in a private cloud 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** – 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. Individuals on a hybrid cloud would be able to have degrees of access to various services based on user access rights.
- **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.



13.1.5. Cloud Computing versus Data Center

The terms data center and cloud computing are often used incorrectly. 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.
- **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.

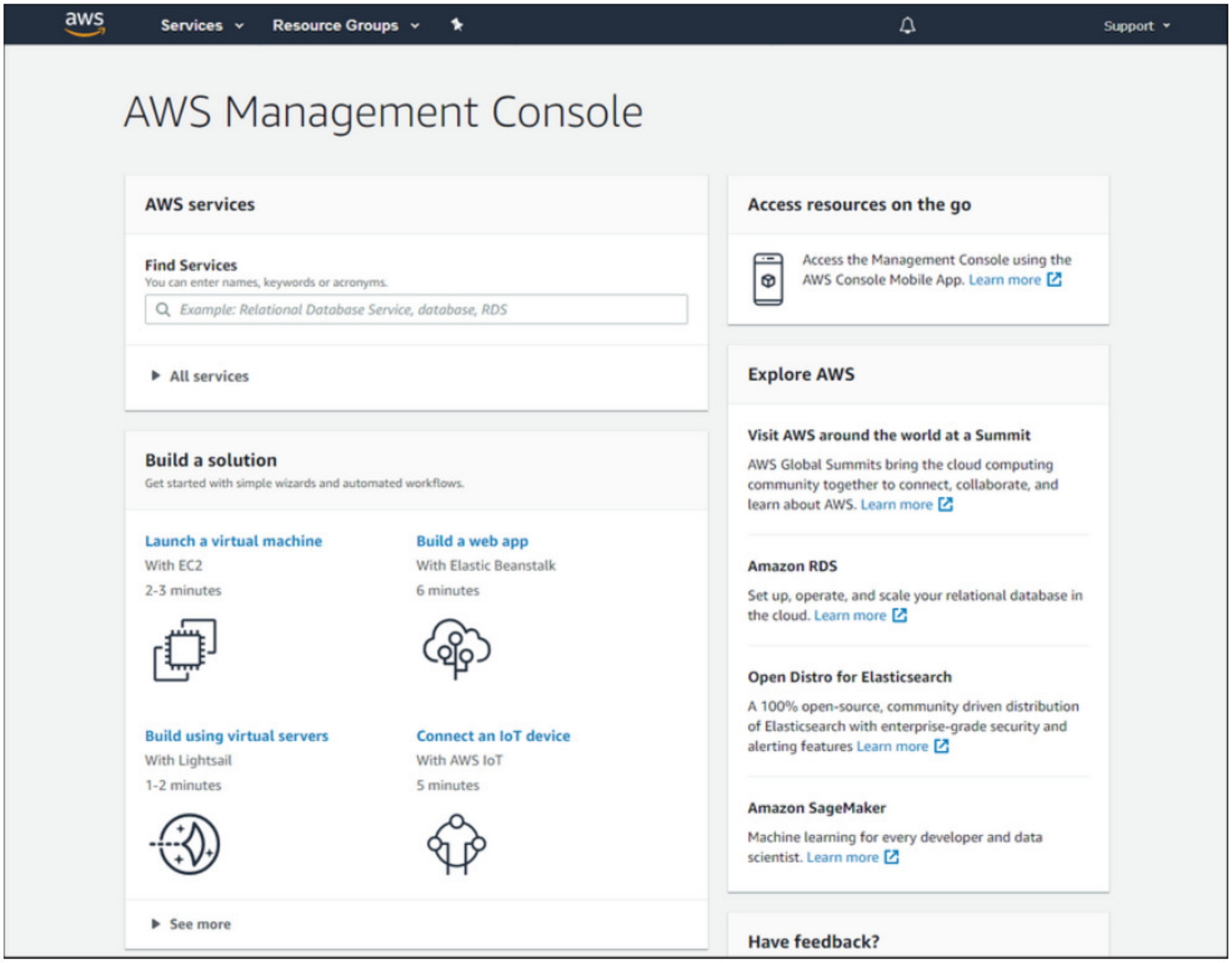
A data center can occupy one room of a building, one or more floors, or an entire building. Data centers are typically very expensive to build and maintain. For this reason, only large organizations use privately built data centers to house their data and provide services to users. Smaller organizations that cannot afford to maintain their own private data center can reduce the overall cost of ownership by leasing server and storage services from a larger data center organization in the cloud.

13.2. Virtualization

13.2.1. Cloud Computing and Virtualization

In the previous topic, you learned about cloud services and cloud models. This topic will explain 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. For example, Amazon Web Services (AWS) provides a simple way for customers to dynamically provision the compute resources they need. These virtualized instances of servers are created on demand. As shown in the figure, the network administrator can deploy a variety of services from the AWS Management Console including virtual machines, web applications, virtual servers, and connections to IoT devices.



AWS Management Console

AWS services

Find Services
You can enter names, keywords or acronyms.
Example: Relational Database Service, database, RDS

▸ All services

Build a solution
Get started with simple wizards and automated workflows.

Launch a virtual machine
With EC2
2-3 minutes

Build a web app
With Elastic Beanstalk
6 minutes

Build using virtual servers
With Lightsail
1-2 minutes

Connect an IoT device
With AWS IoT
5 minutes

▸ See more

Access resources on the go

Access the Management Console using the AWS Console Mobile App. Learn more

Explore AWS

Visit AWS around the world at a Summit
AWS Global Summits bring the cloud computing community together to connect, collaborate, and learn about AWS. Learn more

Amazon RDS
Set up, operate, and scale your relational database in the cloud. Learn more

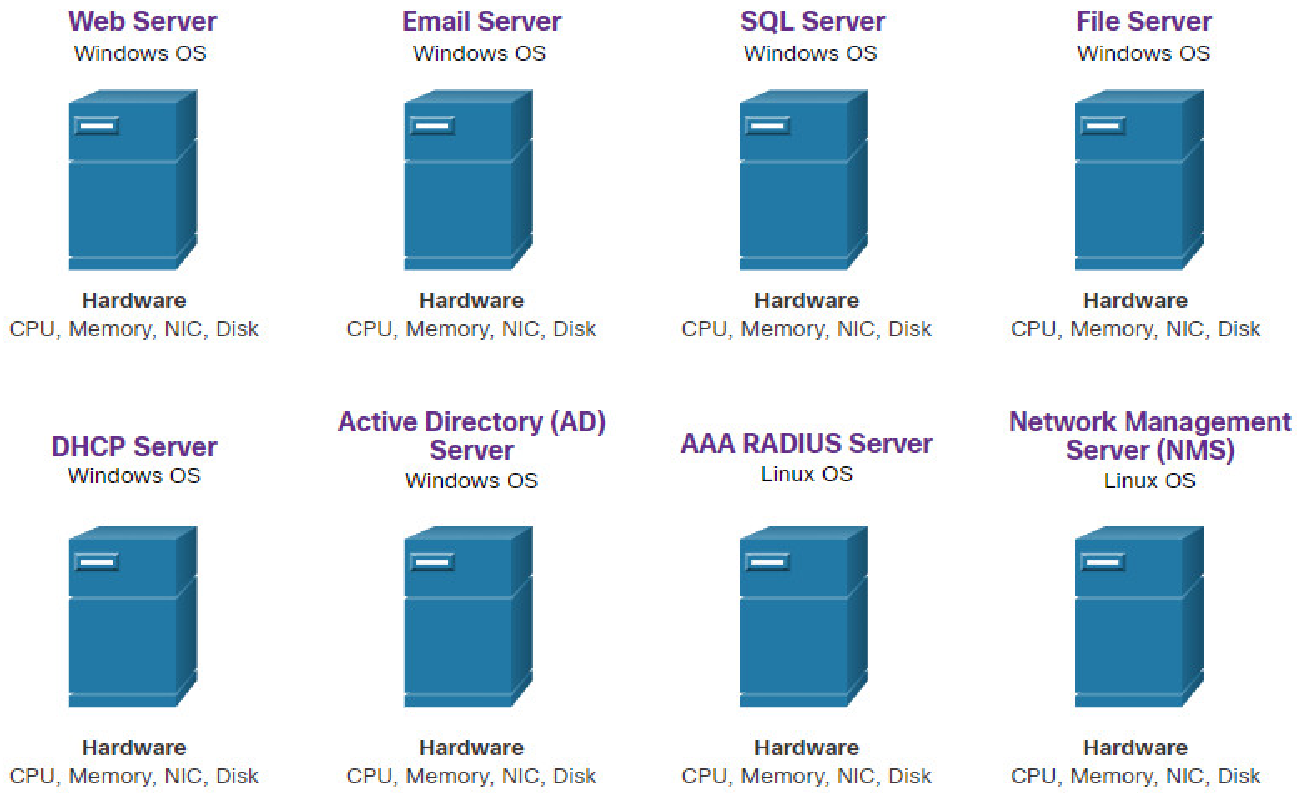
Open Distro for Elasticsearch
A 100% open-source, community driven distribution of Elasticsearch with enterprise-grade security and alerting features Learn more

Amazon SageMaker
Machine learning for every developer and data scientist. Learn more

Have feedback?

13.2.2. Dedicated Servers

To fully appreciate virtualization, it is first necessary to understand some of the history of server technology. Historically, enterprise servers consisted of a server OS, such as Windows Server or Linux Server, installed on specific hardware, as shown in the figure. All of a server's RAM, processing power, and hard drive space were dedicated to the service provided (e.g., Web, email services, etc.).

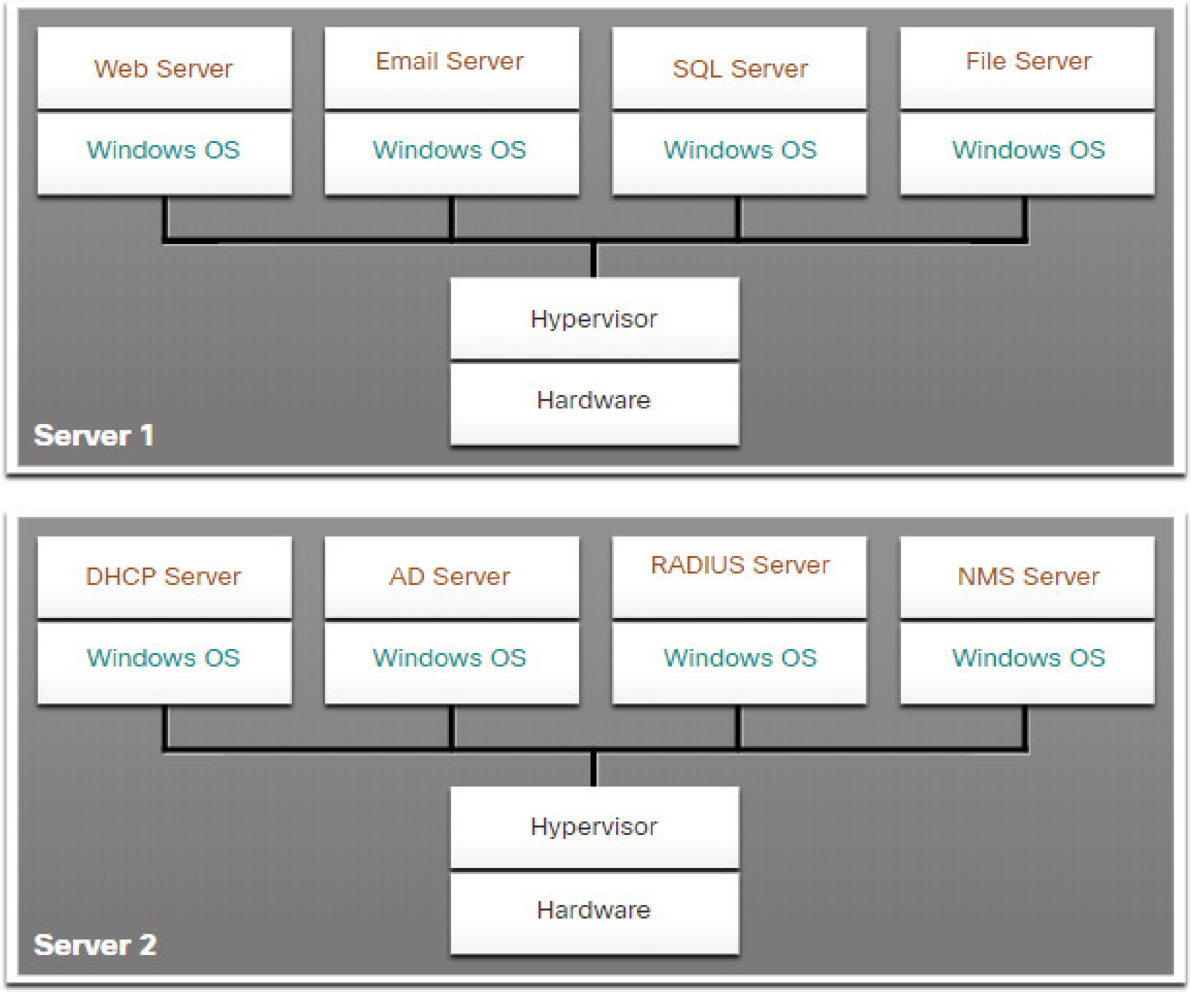


The major problem with this configuration is that when a component fails, the service that is provided by this server becomes unavailable. This is known as a single point of failure. Another problem was that dedicated servers were underused. Dedicated servers often sat idle for long periods of time, 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.

13.2.3. 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.

For example, 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.



The use of virtualization normally includes redundancy to protect from a single point of failure. Redundancy can be implemented in different ways. If the hypervisor fails, the VM can be restarted on another hypervisor. Also, the same VM can run on two hypervisors concurrently, copying the RAM and CPU instructions between them. If one hypervisor fails, the VM continues running on the other hypervisor. The services running on the VMs are also virtual and can be dynamically installed or uninstalled, as needed.

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. Each of these virtual machines runs a complete and separate operating system. With virtualization, enterprises can now consolidate the number of servers they require. For example, it is not uncommon for 100 physical servers to be consolidated as virtual machines on top of 10 physical servers that are using hypervisors.

13.2.4. Advantages of Virtualization

One major advantage of virtualization is overall reduced cost:

- **Less equipment is required** – Virtualization enables server consolidation, which requires fewer physical servers, fewer networking devices, and less supporting infrastructure. It also means lower maintenance costs.
- **Less energy is consumed** – Consolidating servers lowers the monthly power and cooling costs. Reduced consumption helps enterprises to achieve a smaller carbon footprint.
- **Less space is required** – Server consolidation with virtualization reduces the overall footprint of the data center. Fewer servers, network devices, and racks reduce the amount of required floor space.

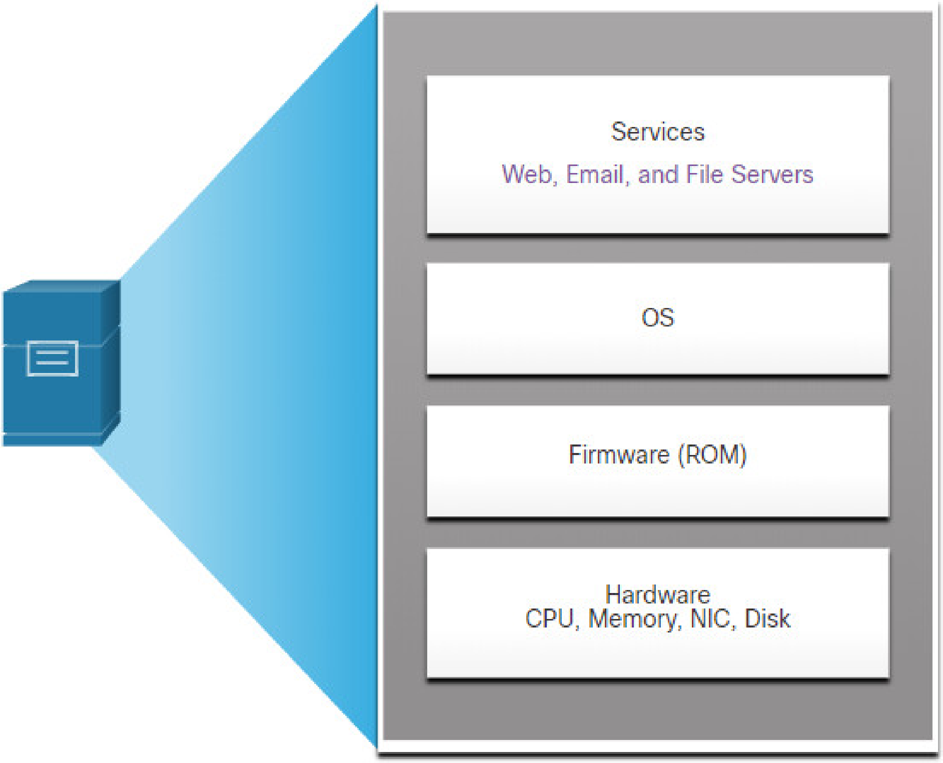
These are additional benefits of virtualization:

- **Easier prototyping** – Self-contained labs, operating on isolated networks, can be rapidly created for testing and prototyping network deployments. If a mistake is made, an administrator can simply revert to a previous version. The testing environments can be online, but isolated from end users. When testing is completed, the servers and systems can be deployed to end users.
- **Faster server provisioning** – Creating a virtual server is far faster than provisioning a physical server.
- **Increased server uptime** – Most server virtualization platforms now offer advanced redundant fault tolerance features, such as live migration, storage migration, high availability, and distributed resource scheduling.
- **Improved disaster recovery** – Virtualization offers advanced business continuity solutions. It provides hardware abstraction capability so that the recovery site no longer needs to have hardware that is identical to the hardware in the production environment. Most enterprise server virtualization platforms also have software that can help test and automate the failover before a disaster does happen.
- **Legacy support** – Virtualization can extend the life of OSs and applications providing more time for organizations to migrate to newer solutions.

13.2.5. Abstraction Layers

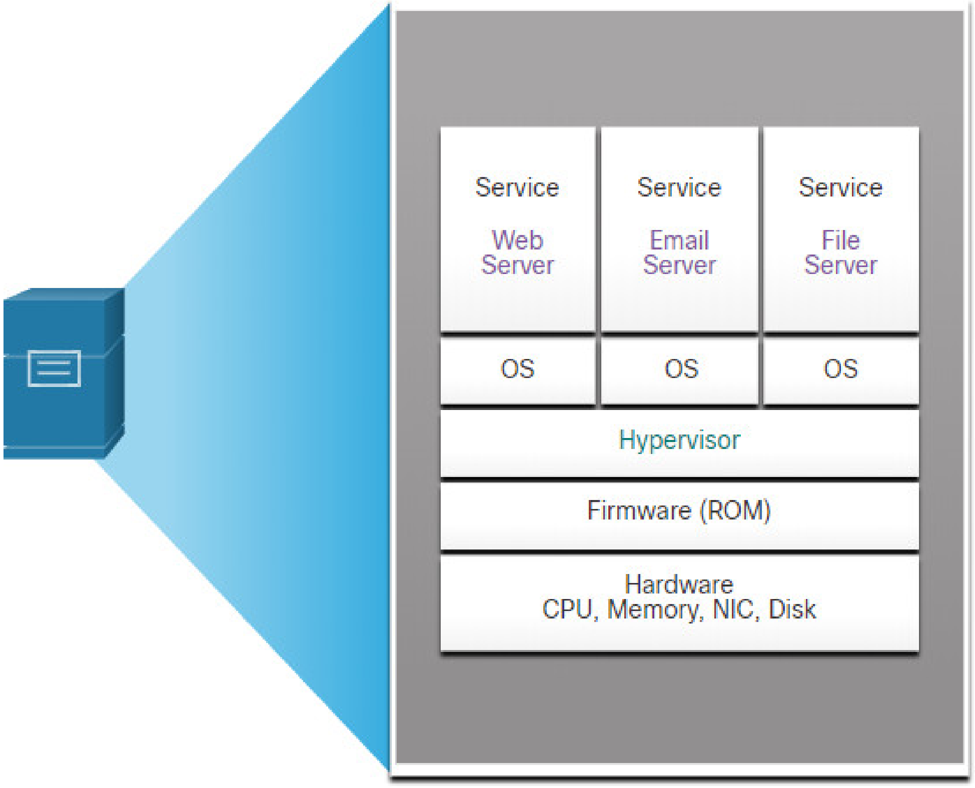
To help explain how virtualization works, it helps to use layers of abstraction in computer architectures. A computer system consists of the following abstraction layers, as illustrated in the figure:

- Services
- OS
- Firmware
- Hardware



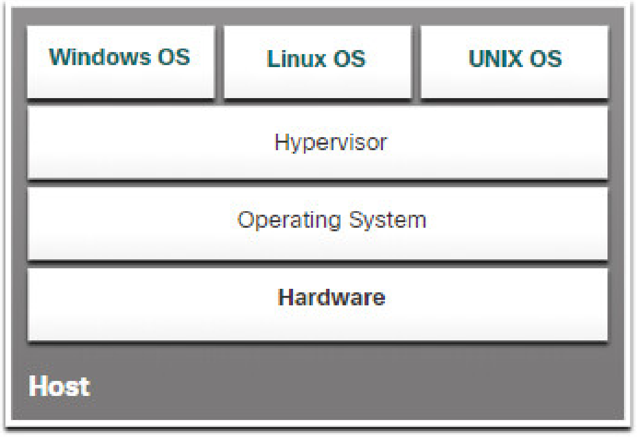
At each of these layers of abstraction, some type of programming code is used as an interface between the layer below and the layer above. For example, the C programming language is often used to program the firmware that accesses the hardware.

An example of virtualization is shown in the figure. A hypervisor is installed between the firmware and the OS. The hypervisor can support multiple instances of OSs.



13.2.6. 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. This is because the hypervisor is installed on top of the existing OS, such as macOS, Windows, or Linux. Then, one or more additional OS instances are installed on top of the hypervisor, as shown in the figure.



A big advantage of Type 2 hypervisors is that management console software is not required.

Type 2 hypervisors are very popular with consumers and for organizations experimenting with virtualization. Common Type 2 hypervisors include:

- Virtual PC
- VMware Workstation
- Oracle VM VirtualBox
- VMware Fusion
- Mac OS X Parallels

Many of these Type 2 hypervisors are free. However, some hypervisors offer more advanced features for a fee.

Note: It is important to make sure that the host machine is robust enough to install and run the VMs, so that it does not run out of resources.

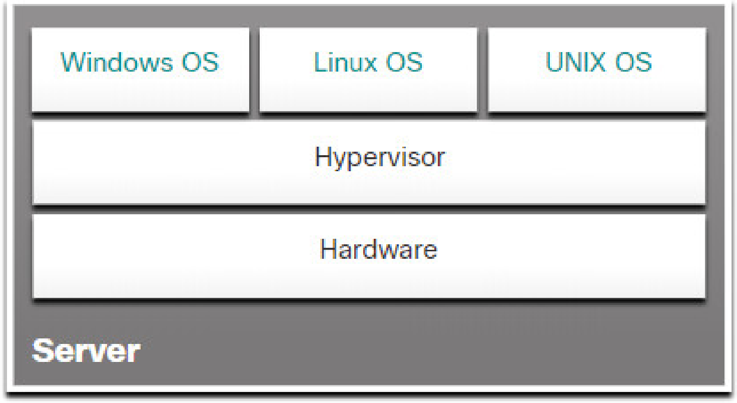
13.3. Virtual Network Infrastructure

13.3.1. Type 1 Hypervisors

In the previous topic, you learned about virtualization. This topic will cover the virtual network infrastructure.

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.

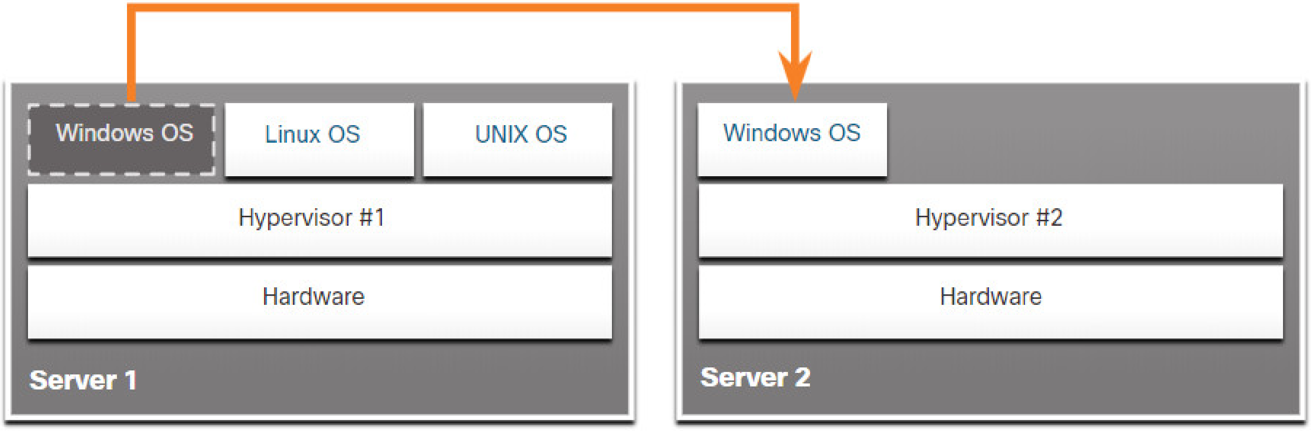
With Type 1 hypervisors, the hypervisor is installed directly on the server or networking hardware. Then, instances of an OS are installed on the hypervisor, as shown in the figure. Type 1 hypervisors have direct access to the hardware resources. Therefore, they are more efficient than hosted architectures. Type 1 hypervisors improve scalability, performance, and robustness.



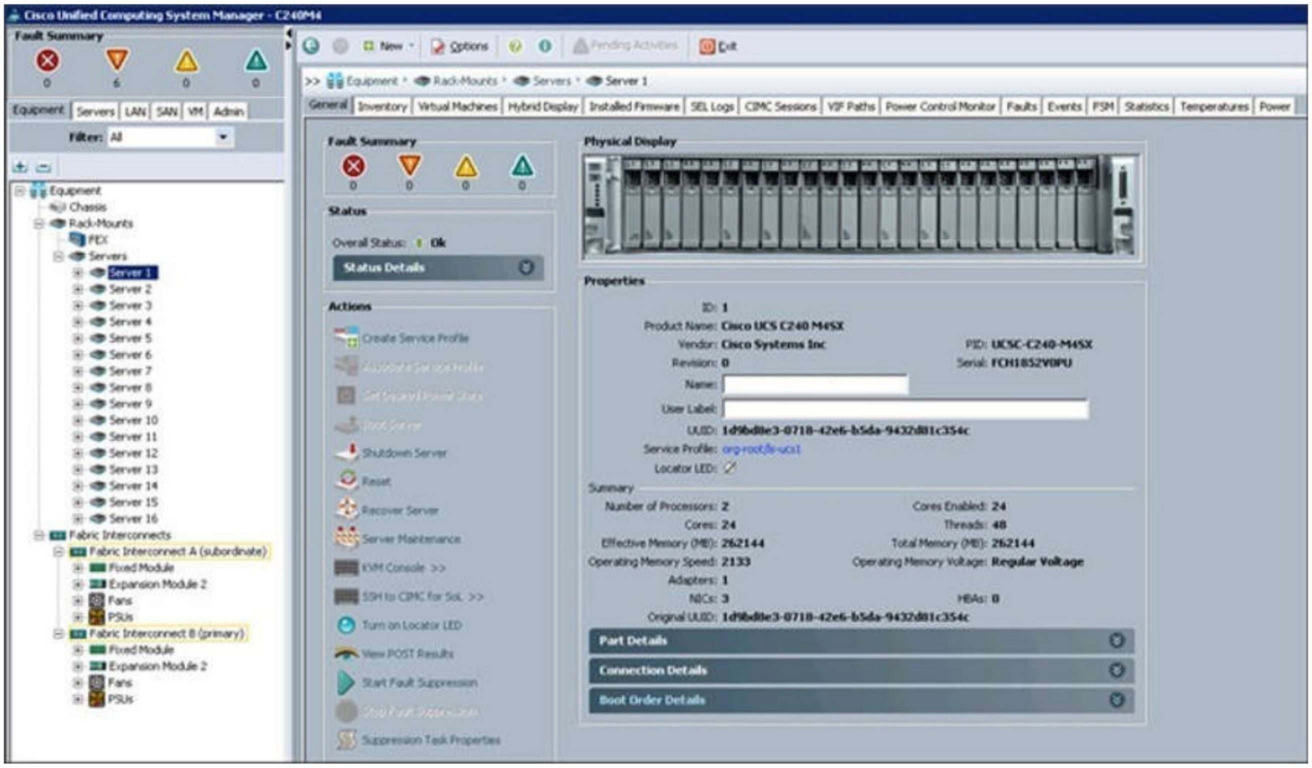
13.3.2. Installing a VM on a Hypervisor

When a Type 1 hypervisor is installed, and the server is rebooted, only basic information is displayed, such as the OS version, the amount of RAM, and the IP address. An OS instance cannot be created from this screen. 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.

For example, assume that Server1 in the figure becomes low on resources. To make more resources available, the network administrator uses the management console to move the Windows instance to the hypervisor on Server2. The management console can also be programmed with thresholds that will trigger the move automatically.



The management console provides recovery from hardware failure. If a server component fails, the management console automatically moves the VM to another server. The management console for the Cisco Unified Computing System (UCS) Manager is shown in the figure. Cisco UCS Manager controls multiple servers and manages resources for thousands of VMs.



Overall Status: Ok

ID: 1
Product Name: Cisco UCS C240 M4SX
Vendor: Cisco Systems Inc
PID: UCSC-C240-M4SX
Revision: 0
Serial: FCH1852V0PU
Name:
User Label:
UUID: 1d9bd8e3-0718-42e6-b5da-9432d81c354c
Service Profile: org-root/ls-ucs1
Locator LED:

Number of Processors: 2
Cores Enabled: 24
Cores: 24
Threads: 48
Effective Memory (MB): 262144
Total Memory (MB): 262144
Operating Memory Speed: 2133
Operating Memory Voltage: Regular Voltage
Adapters: 1
NICs: 3
HBAs: 0
Original UUID: 1d9bd8e3-0718-42e6-b5da-9432d81c354c

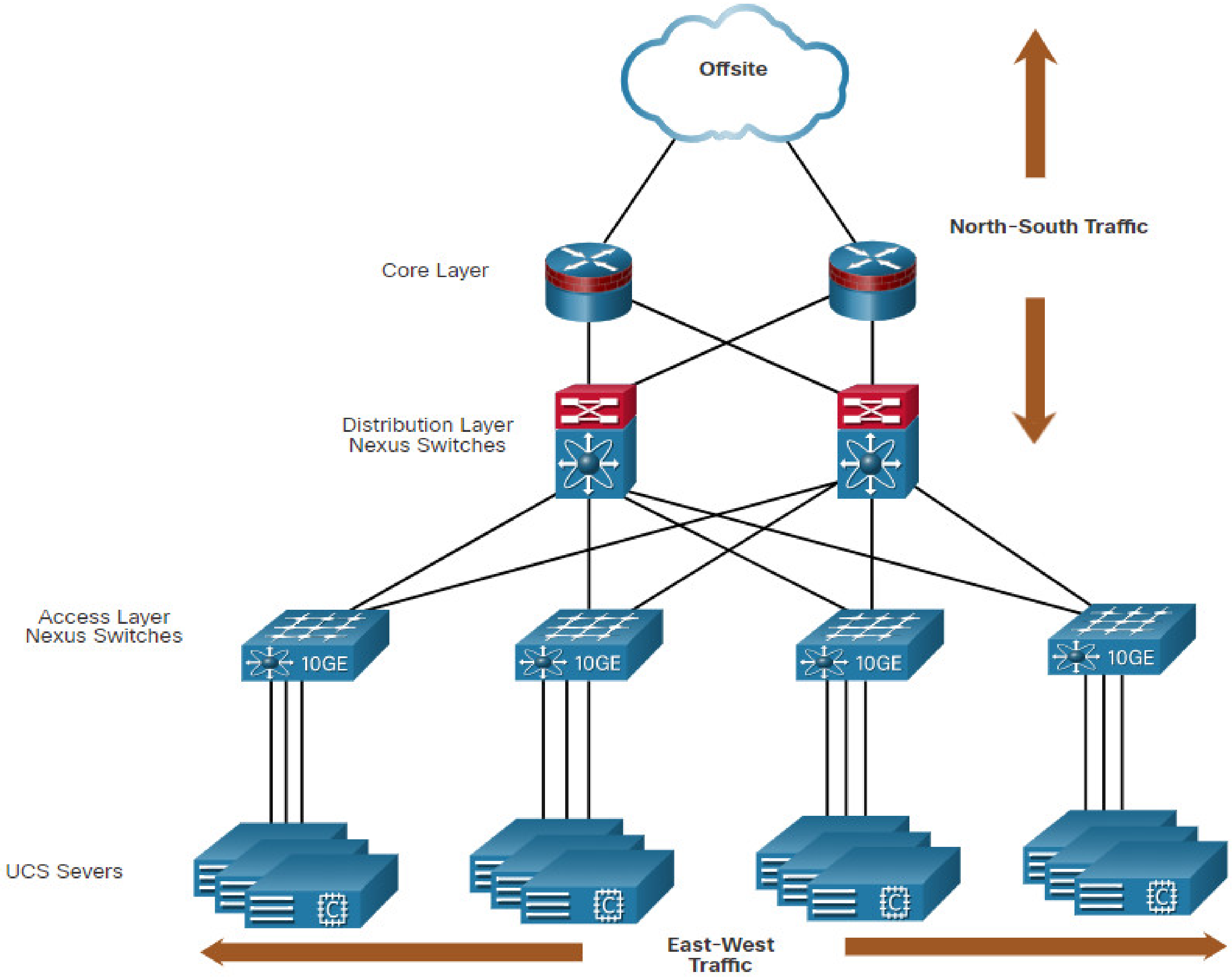
Some management consoles also allow server over allocation. Over allocation is when multiple OS instances are installed, but their memory allocation exceeds the total amount of memory that a server has. For example, a server has 16 GB of RAM, but the administrator creates four OS instances with 10 GB of RAM allocated to each. This type of over allocation is a common practice because all four OS instances rarely require the full 10 GB of RAM at any one moment.

13.3.3. The Complexity of Network Virtualization

Server virtualization hides server resources, such as the number and identity of physical servers, processors, and OSs 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 would be manual and time-consuming 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, such as the UCS servers shown in the figure. These flows are called East-West traffic and can change in location and intensity over time. North-South traffic occurs between the distribution and core layers and is typically traffic destined for offsite locations such as another data center, other cloud providers, or the internet.



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).

How is the network virtualized? The answer is found in how a networking device operates using a data plane and a control plane, as discussed in the next topic.

13.4. Software-Defined Networking

13.4.1 Video – Software-Defined Networking

Click Play to view a video on network programming, software-defined networking (SDN), and controllers.

13.4.2. Control Plane and Data Plane

The previous topic explained virtual network infrastructure. This topic will cover Software-Defined Networking (SDN). SDN was explained in the previous video. We will cover more details here.

A network device contains the following planes:

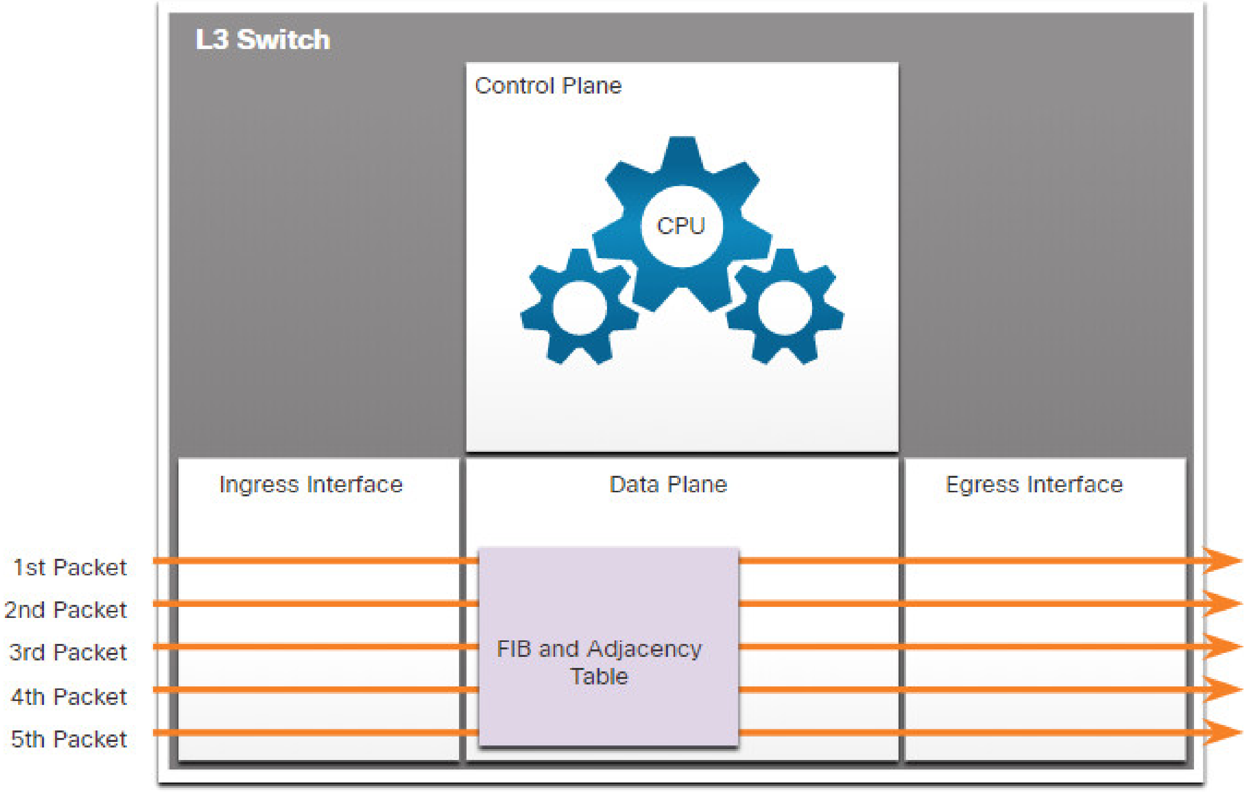
- **Control plane** – This is typically regarded as the brains of a device. It is used to make forwarding decisions. The control plane contains Layer 2 and Layer 3 route forwarding mechanisms, such as routing protocol neighbor tables and topology tables, IPv4 and IPv6 routing tables, STP, and the ARP 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.

Click each button for an illustration and explanation of the difference between the operation of localized control on a Layer 3 switch and a centralized controller in SDN

- Layer 3 Switch and CEF
- SDN and Central Controller

Layer 3 Switch and CEF
The figure illustrates how Cisco Express Forwarding (CEF) uses the control plane and data plane to process packets.

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. In CEF, the control plane's routing table pre-populates the CEF Forwarding Information Base (FIB) table in the data plane. The control plane's ARP table pre-populates the adjacency table. Packets are then forwarded directly by the data plane based on the information contained in the FIB and adjacency table, without needing to consult the information in the control plane.



Management Plane

Not shown in the figures is the management plane, which 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.

13.4.3. Network Virtualization Technologies

Over a decade ago, VMware developed a virtualizing technology that enabled a host OS to support one or more client OSs. Most virtualization technologies are now based on this technology. The transformation of dedicated servers to virtualized servers has been embraced and is rapidly being implemented in data center and enterprise networks.

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

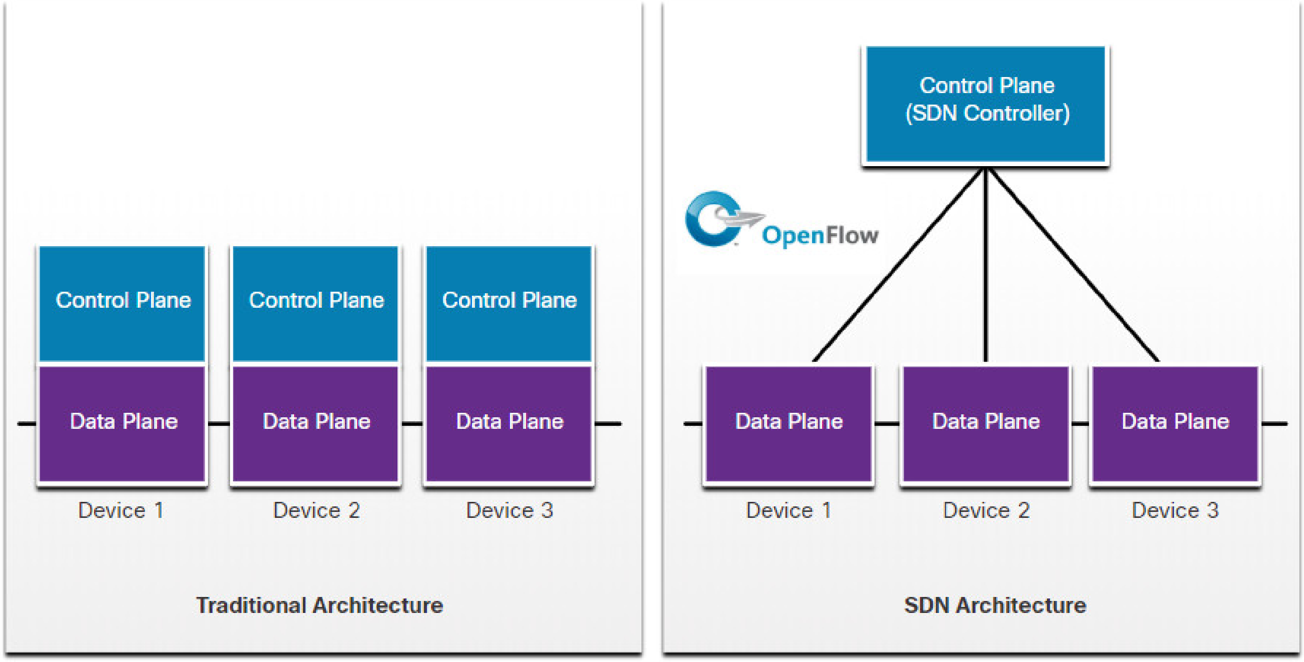
- **Software-Defined Networking (SDN)** – A network architecture that virtualizes the network, offering a new approach to network administration and management that seeks to simplify and streamline the administration process.
- **Cisco Application Centric Infrastructure (ACI)** – A purpose-built hardware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

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. Search for OpenFlow and the Open Networking Foundation for more information.
- **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. Search for OpenStack for more information.
- **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).

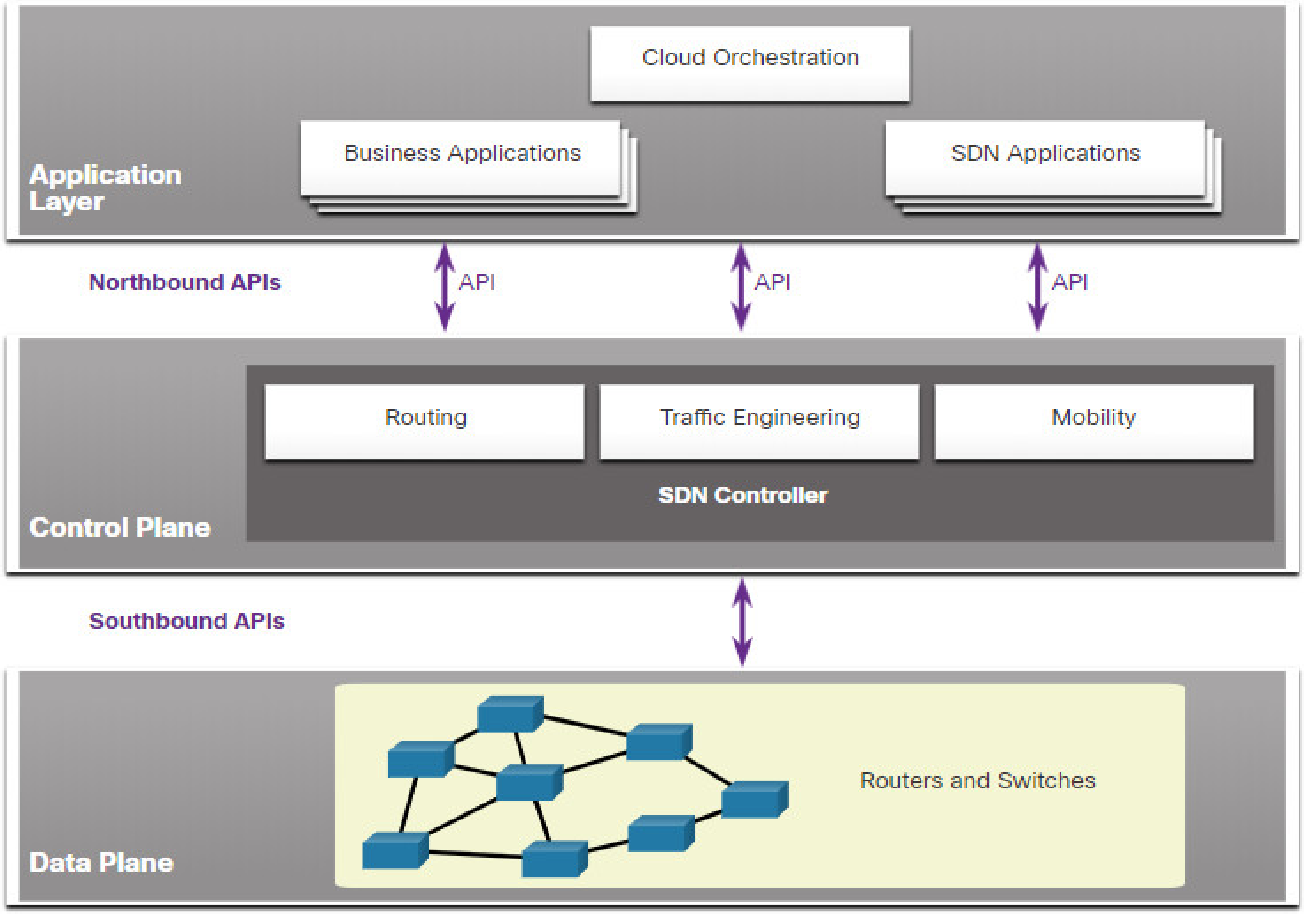
13.4.4. Traditional and SDN Architectures

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.



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) within the SDN framework. An API is a set of standardized requests that define the proper way for an application to request services from another application. 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 data planes on downstream switches and routers. OpenFlow is the original and widely implemented southbound API.



13.5. Controllers

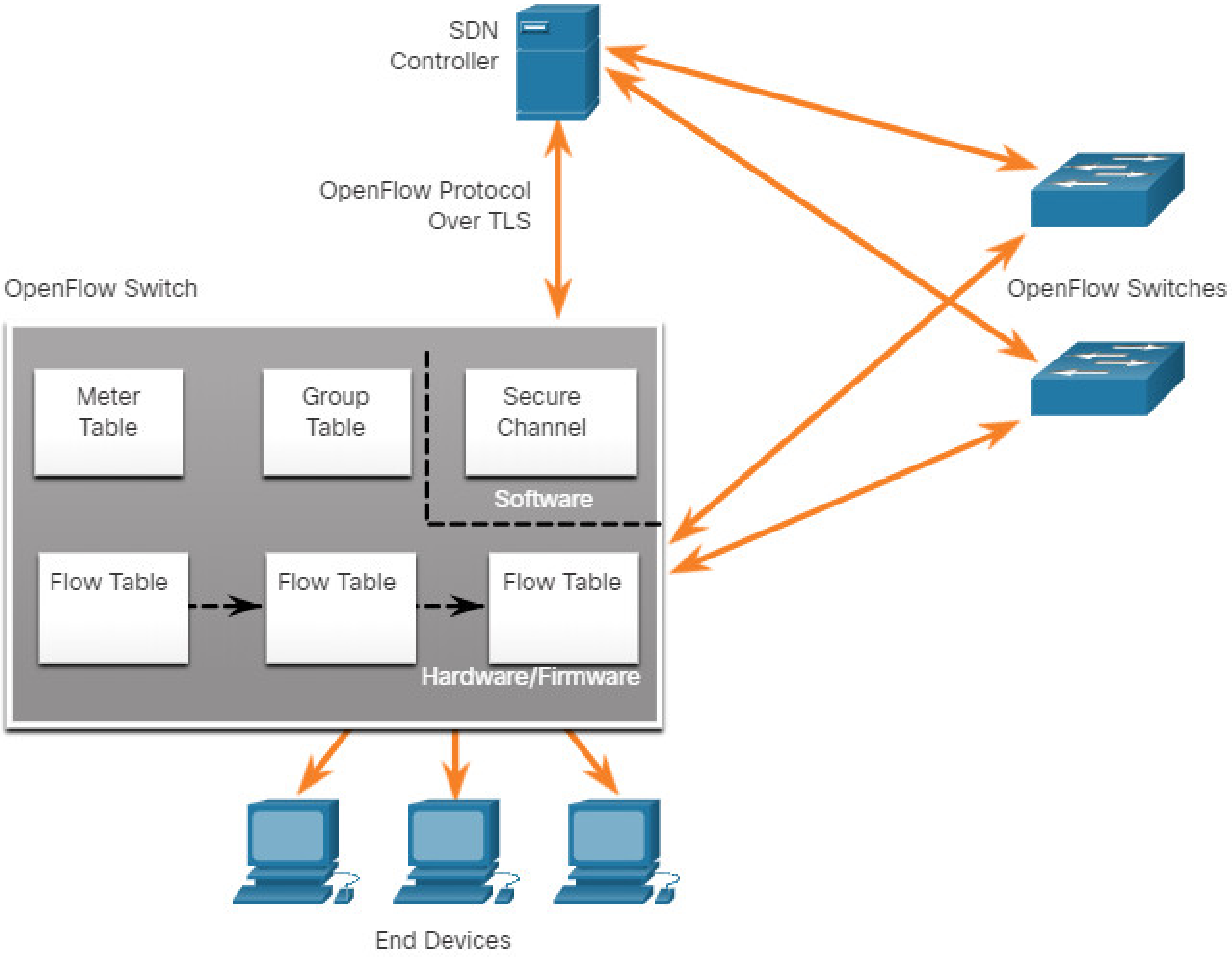
13.5.1. SDN Controller and Operations

The previous topic covered SDN. This topic will explain controllers.

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. If the controller allows a flow, it computes a route for the flow to take and adds an entry for that flow in each of the switches along the path.

All complex functions are performed by the controller. The controller populates flow tables. Switches manage the flow tables. In the figure, an SDN controller communicates with OpenFlow-compatible switches using the OpenFlow protocol. This protocol uses Transport Layer Security (TLS) to securely send control plane communications over the network. Each OpenFlow switch connects to other OpenFlow switches. They can also connect to end-user devices that are part of a packet flow.



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 tables 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.

13.5.2 Video – Cisco ACI

Very few organizations actually have the desire or skill to program the network using SDN tools. However, the majority of organizations want to automate the network, accelerate application deployments, and align their IT infrastructures to better meet business requirements. Cisco developed the Application Centric Infrastructure (ACI) to meet these objectives in more advanced and innovative ways than earlier SDN approaches.

Cisco ACI is a hardware solution for integrating cloud computing and data center management. At a high level, the policy element of the network is removed from the data plane. This simplifies the way data center networks are created.

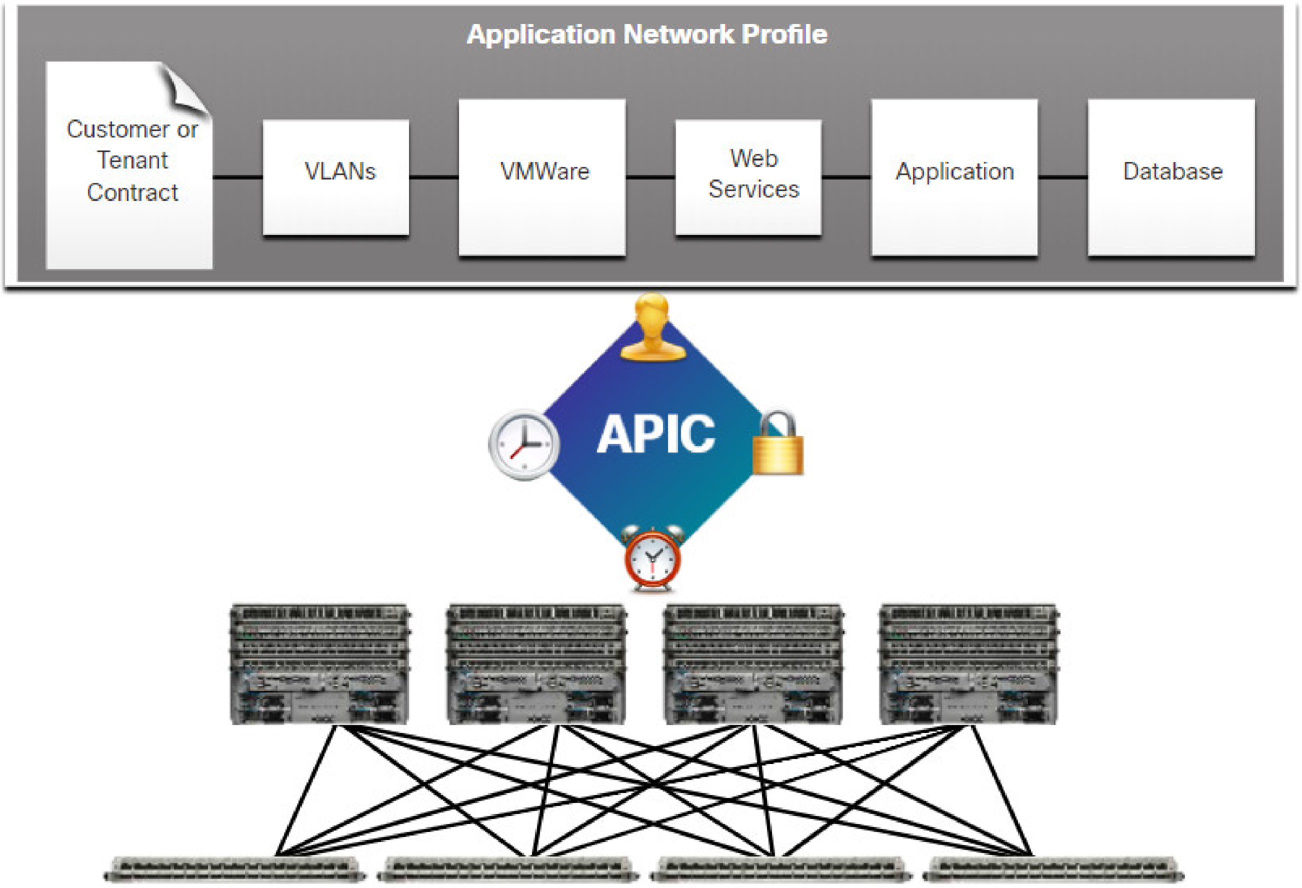
Click Play to view a video about the evolution of SDN and ACI.

13.5.3. Core Components of ACI

These are the 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. The EPGs shown in the figure, such as VLANs, web services, and applications, are just examples. An ANP is often much more complex.
- **Application Policy Infrastructure Controller (APIC)** – The APIC is considered to be the brains of the ACI architecture. 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, as shown in the figure

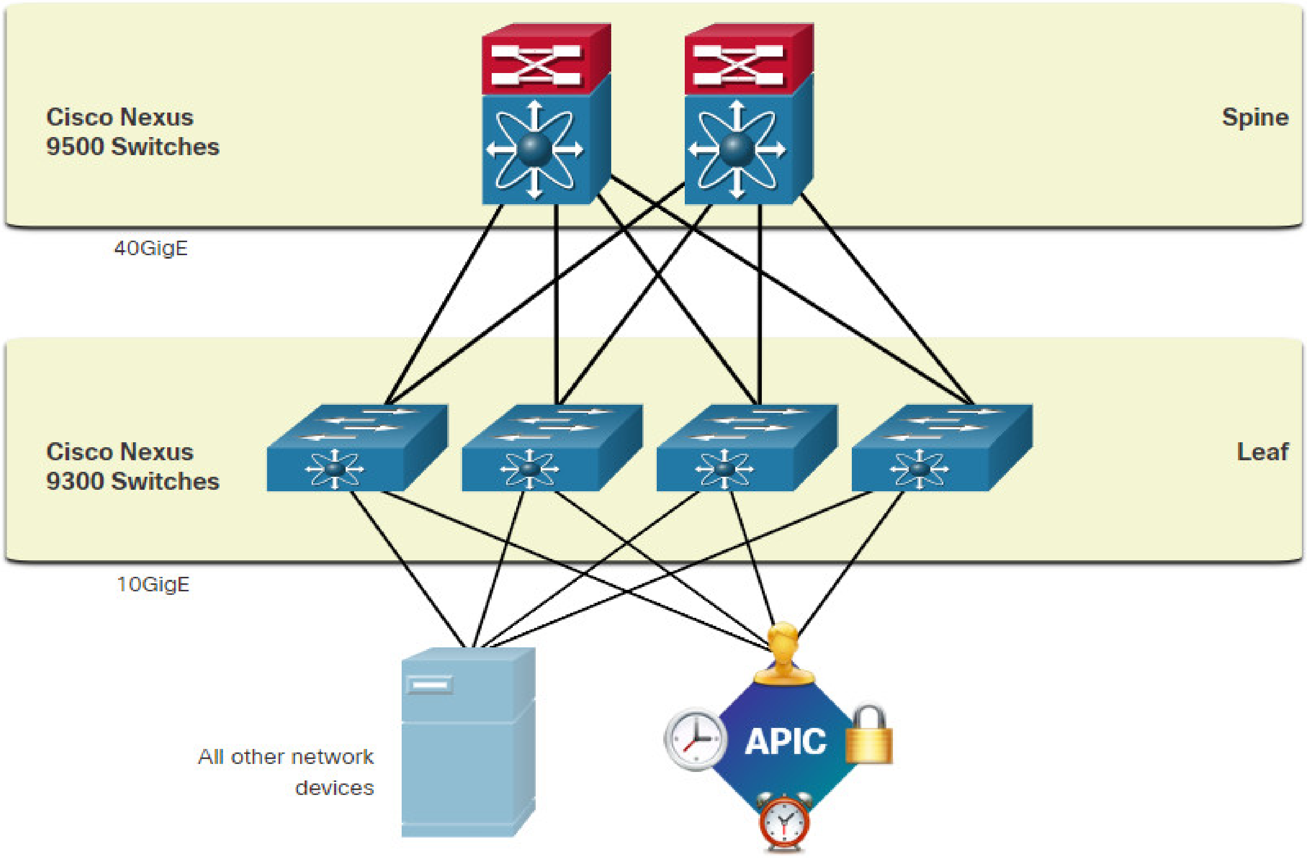


13.5.4. Spine-Leaf Topology

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 always 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.

The 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. Instead, the APIC centralizes the policy definition and programs the leaf switches to forward traffic based on the defined policies.

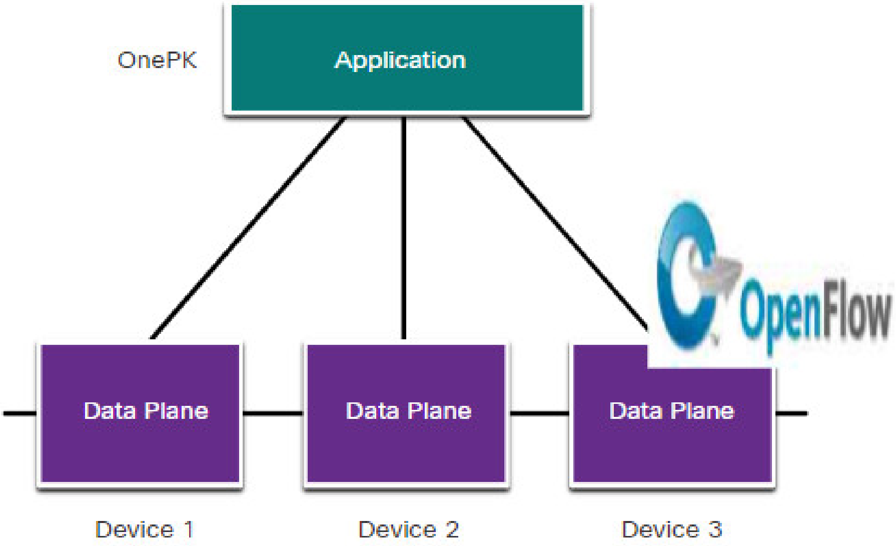


13.5.5. SDN Types

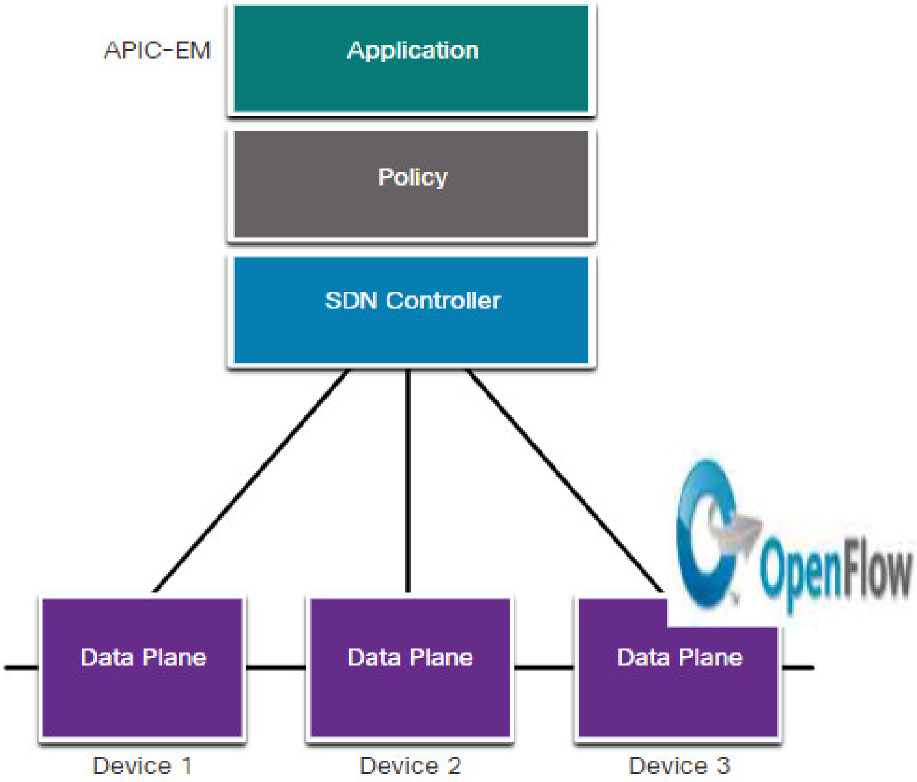
The Cisco Application Policy Infrastructure Controller – Enterprise Module (APIC-EM) extends ACI aimed at enterprise and campus deployments. To better understand APIC-EM, it is helpful to take a broader look at the three types of SDN.

Click each SDN type to for more information.

Device-based SDN
In this type of SDN, the devices are programmable by applications running on the device itself or on a server in the network, as shown in the figure. Cisco OnePK is an example of a device-based SDN. It enables programmers to build applications using C, and Java with Python, to integrate and interact with Cisco devices.



Policy-based SDN
This type of SDN is 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.

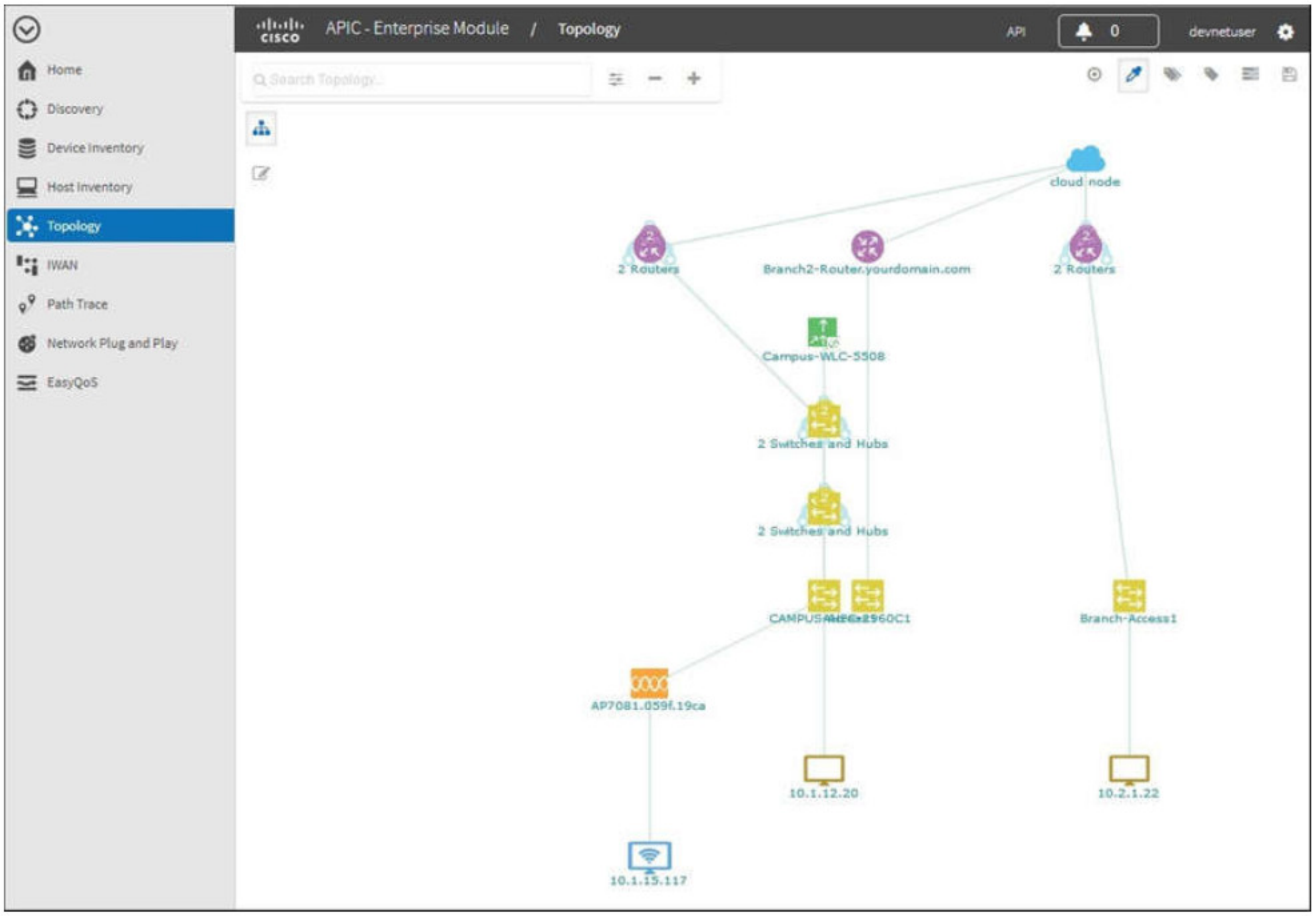


13.5.6. APIC-EM Features

Each type of SDN has its own features and advantages. Policy-based SDN is the most robust, providing for a simple mechanism to control and manage policies across the entire network.

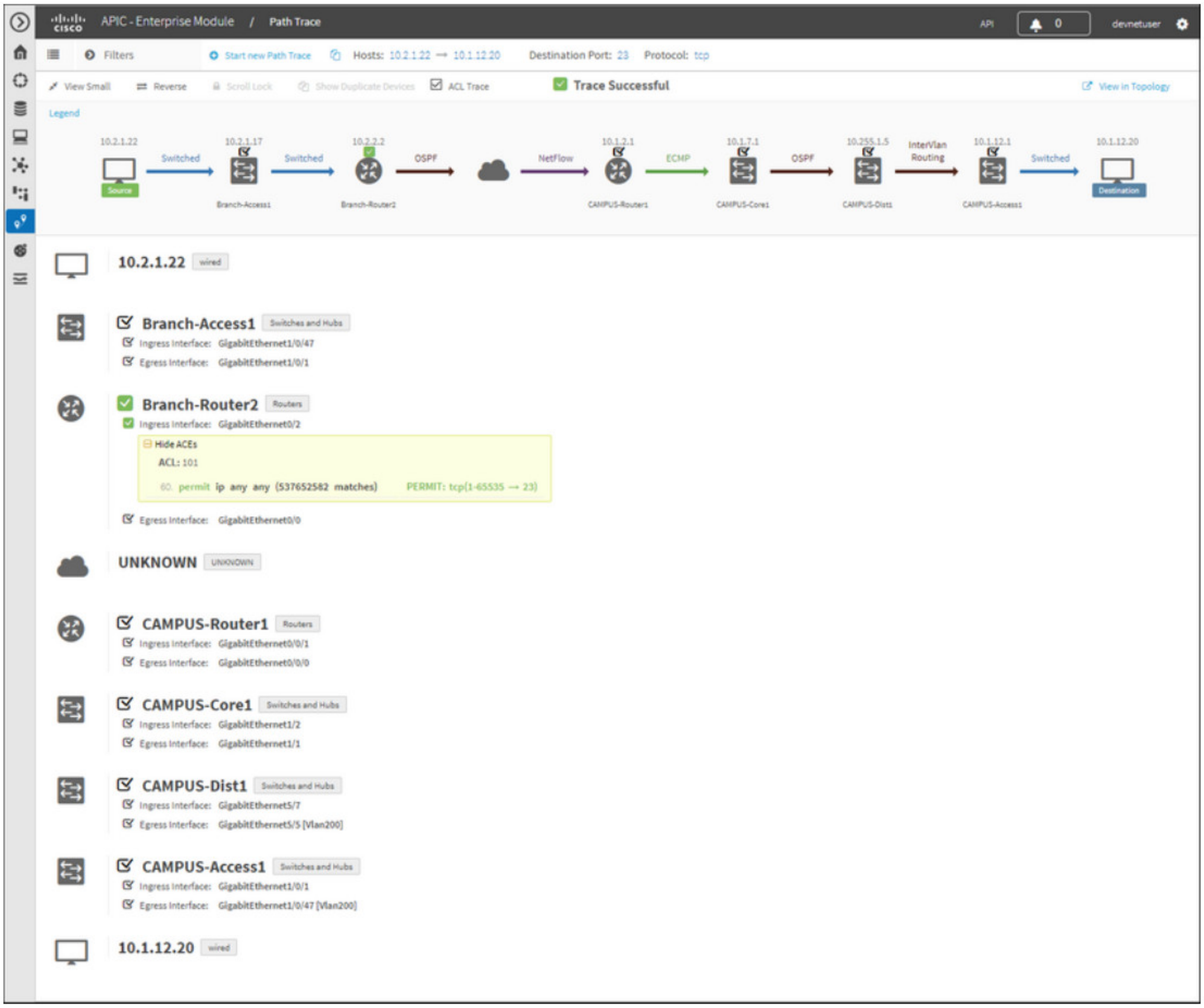
Cisco APIC-EM is an example of policy-based SDN. Cisco APIC-EM provides a single interface for network management including:

- discovering and accessing device and host inventories,
- viewing the topology (as shown in the figure),
- tracing a path between end points, and
- setting policies.



13.5.7. 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.



10.2.1.22 wired

☑ **Branch-Access1** Switches and Hubs
☑ Ingress Interface: GigabitEthernet1/0/47
☑ Egress Interface: GigabitEthernet1/0/1

☑ **Branch-Router2** Routers
☑ Ingress Interface: GigabitEthernet0/2
⊟ Hide ACEs
ACL: 101
60. permit ip any any (537652582 matches) PERMIT: tcp(1-65535 → 23)
☑ Egress Interface: GigabitEthernet0/0

UNKNOWN UNKNOWN

☑ **CAMPUS-Router1** Routers
☑ Ingress Interface: GigabitEthernet0/0/1
☑ Egress Interface: GigabitEthernet0/0/0

☑ **CAMPUS-Core1** Switches and Hubs
☑ Ingress Interface: GigabitEthernet1/2
☑ Egress Interface: GigabitEthernet1/1

☑ **CAMPUS-Dist1** Switches and Hubs
☑ Ingress Interface: GigabitEthernet5/7
☑ Egress Interface: GigabitEthernet5/5 [Vlan200]

☑ **CAMPUS-Access1** Switches and Hubs
☑ Ingress Interface: GigabitEthernet1/0/1
☑ Egress Interface: GigabitEthernet1/0/47 [Vlan200]

10.1.12.20 wired

13.6. Module Practice and Quiz

13.6.1. Lab – Install Linux in a Virtual Machine and Explore the GUI

In this lab, you will install a Linux OS in a virtual machine using a desktop virtualization application, such as VirtualBox. After completing the installation, you will explore the GUI interface.

13.6.1 Lab – Install Linux in a Virtual Machine and Explore the GUI

13.6.2. What did I learn in this module?

Cloud Computing

Cloud computing involves large numbers of computers connected through a network that can be physically located anywhere. Cloud computing can reduce operational costs by using resources more efficiently. Cloud computing addresses a variety of data management issues:

- It enables access to organizational data anywhere and at any time.
- It streamlines the organization's IT operations by subscribing only to needed services.
- It eliminates or reduces the need for onsite IT equipment, maintenance, and management.
- It reduces cost for equipment, energy, physical plant requirements, personnel training needs.
- It enables rapid responses to increasing data volume requirements.

The three main cloud computing services defined by the National Institute of Standards and Technology (NIST) are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). With SaaS, the cloud provider is responsible for access to applications and services, such as email, communication, and Office 365 that are delivered over the internet. With PaaS, the cloud provider is responsible for providing users access to the development tools and services used to deliver the applications. With IaaS, the cloud provider is responsible for giving IT managers access to the network equipment, virtualized network services, and supporting network infrastructure. The four types of clouds are public, private, hybrid, and community. Cloud-based applications and services offered in a public cloud are made available to the general population. Cloud-based applications and services offered in a private cloud are intended for a specific organization or entity, such as the government. 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. A community cloud is created for exclusive use by a specific community.

Virtualization

The terms "cloud computing" and "virtualization" are often used interchangeably; however, they mean different things. Virtualization is the foundation of cloud computing. Virtualization separates the operating system (OS) from the hardware. 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. When a component fails, the service that is provided by this server becomes unavailable. This is known as a single point of failure. Another problem with dedicated servers is that they often sat idle for long periods of time, waiting until there was a need to deliver the specific service they provide. This wastes energy and resources (server sprawl). Virtualization reduces costs because less equipment is required, less energy is consumed, and less space is required. It provides for easier prototyping, faster server provisioning, increased server uptime, improved disaster recovery, and legacy support. A computer system consists of the following abstraction layers: services, OS, firmware, and hardware. With Type 1 hypervisors, the hypervisor is installed directly on the server or networking hardware. A Type 2 hypervisor is software that creates and runs VM instances. It can be installed on top of the OS or can be installed between the firmware and the OS. A Type 2 hypervisor is software that creates and runs VM instances.

Virtual Network Infrastructure

Type 1 hypervisors are also called the “bare metal” approach because the hypervisor is installed directly on the hardware. Type 1 hypervisors have direct access to the hardware resources and are more efficient than hosted architectures. They improve scalability, performance, and robustness. 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. Some management consoles also allow server over allocation. Server virtualization hides server resources, such as the number and identity of physical servers, processors, and OSs from server users. This practice can create problems if the data center is using traditional network architectures. 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. These flows are called East-West traffic and can change in location and intensity over time. North-South traffic occurs between the distribution and core layers and is typically traffic destined for offsite locations such as another data center, other cloud providers, or the internet.

Software-Defined Networking

Two major network architectures have been developed to support network virtualization: Software-Defined Networking (SDN) and Cisco Application Centric Infrastructure (ACI). SDN is an approach to networking where the network is software programmable remotely. Components of SDN may include OpenFlow, OpenStack, and other components. 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. A network device contains a control plane and a data plane. The control plane is 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. The data plane, also called the forwarding 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. Cisco Express Forwarding (CEF) uses the control plane and data plane to process packets. 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. 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. Protocols like Simple Network Management Protocol (SNMP) use the management plane.

Controllers

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. 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. If the controller allows a flow, it computes a route for the flow to take and adds an entry for that flow in each of the switches along the path. The controller populates flow tables. Switches manage the flow tables. A flow 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. A flow table may direct a flow to a group table, which may trigger a variety of actions that affect one or more flows. A meter table triggers a variety of performance-related actions on a flow including the ability to rate-limit the traffic. Cisco developed the Application Centric Infrastructure (ACI) which is a more advanced and innovative way than earlier SDN approaches. Cisco ACI is a hardware solution for integrating cloud computing and data center management. At a high level, the policy element of the network is removed from the data plane. This simplifies the way data center networks are created. The three core components of the ACI architecture are Application Network Profile (ANP), Application Policy Infrastructure Controller (APIC), and Cisco Nexus 9000 Series switches. The Cisco ACI fabric is composed of the APIC and the Cisco Nexus 9000 series switches using two-tier spine-leaf topology. 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. There are three types of SDN. Device-based SDN is when the devices are programmable by applications running on the device itself or on a server in the network. Controller-based SDN uses a centralized controller that has knowledge of all devices in the network. Policy based SDN is similar to controller-based SDN where a centralized controller has a view of all devices in the network. Policy-based SDN includes an additional Policy layer that operates at a higher level of abstraction. Policy-based SDN is the most robust, providing for a simple mechanism to control and manage policies across the entire network. Cisco APIC-EM is an example of policy-based SDN. Cisco APIC-EM provides a single interface for network management including discovering and accessing device and host inventories, viewing the topology, tracing a path between end points, and setting policies. 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.

13.6.3 Module Quiz – Network Virtualization

Download Slide Powerpoint (PPT)

CCNA 3 v7.0 Curriculum: Module 13 - Network Virtualization.pptx

1 file(s)   1.97 MB

Download

Tags:ccna 3 v7 modules