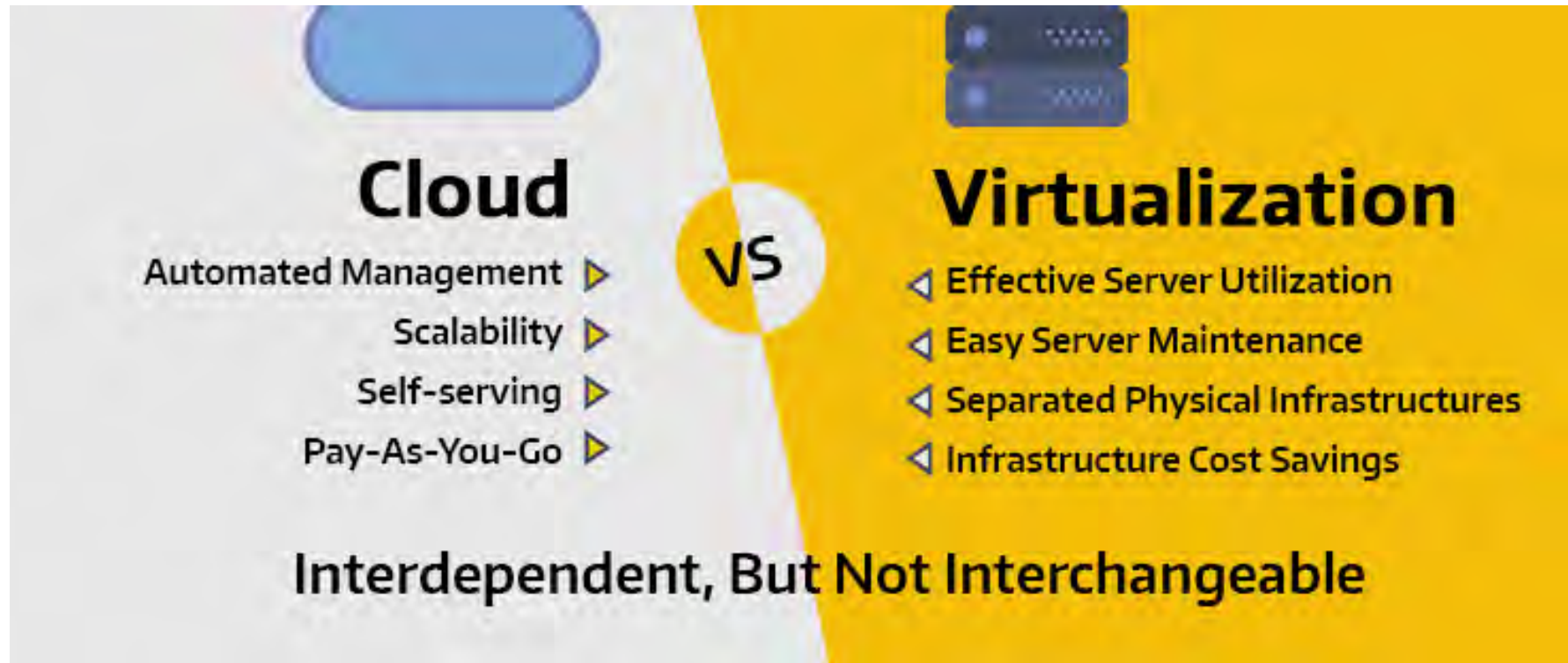


# CH7: Cloud and Virtualization Computing



# Implementing Client Virtualization and Cloud Computing

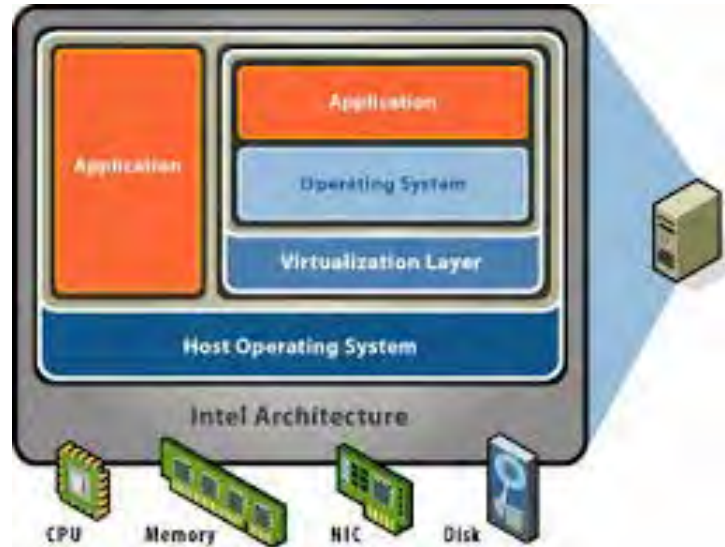


Configure Client-Side  
Virtualization



Cloud Computing Concepts

# Topic A: Configure Client-Side Virtualization

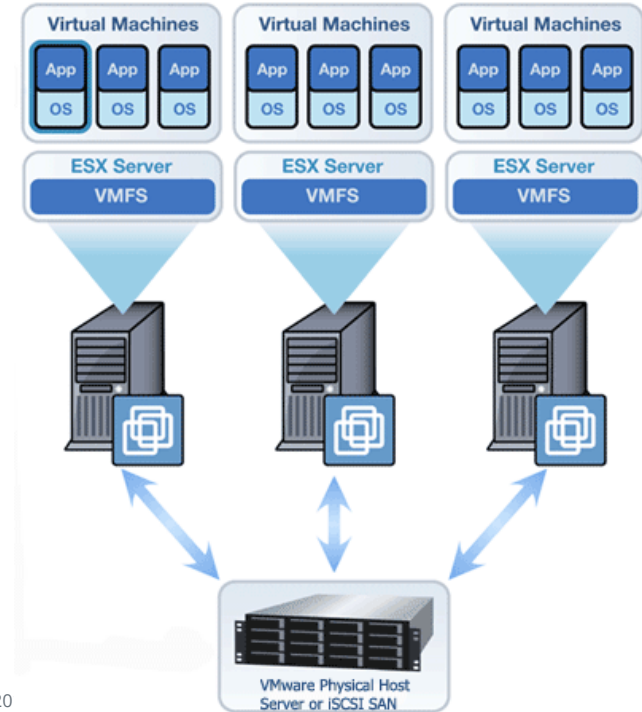


# Virtualization

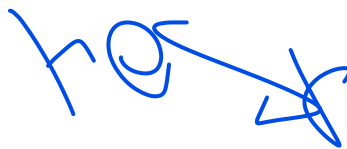


**Virtualization:** Software allowing a host computer to run multiple guest operating systems known as virtual machines.

- Virtual platform requires:
  - Computer(s)
  - Hypervisor or Virtual Machine Monitor (VMM)
  - Guest operating system or Virtual Machines (VMs)

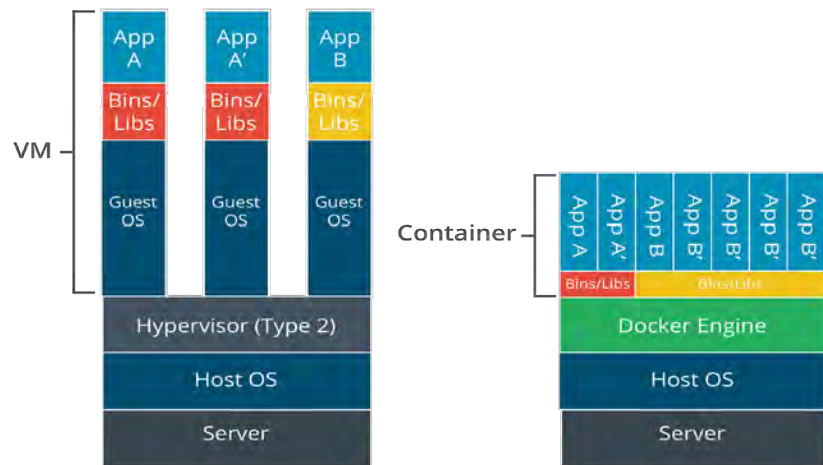


# Uses for Virtualization



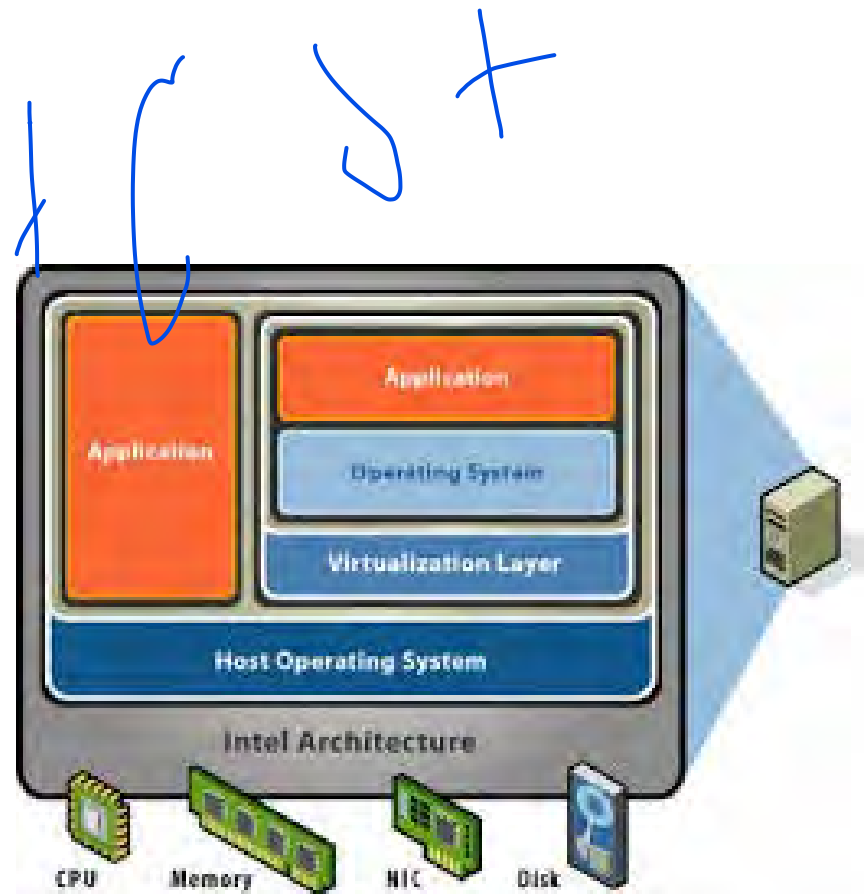
- Client-side virtualization
  - Sandboxes, install legacy software applications and operating systems, test software across different platforms, training, ...
- Server-side virtualization
  - Better hardware utilization and resource flexibility
- Application virtualization
  - Install software to server and stream to clients
- Container virtualization
  - Run apps within an isolated workspace

Container vs. VMs

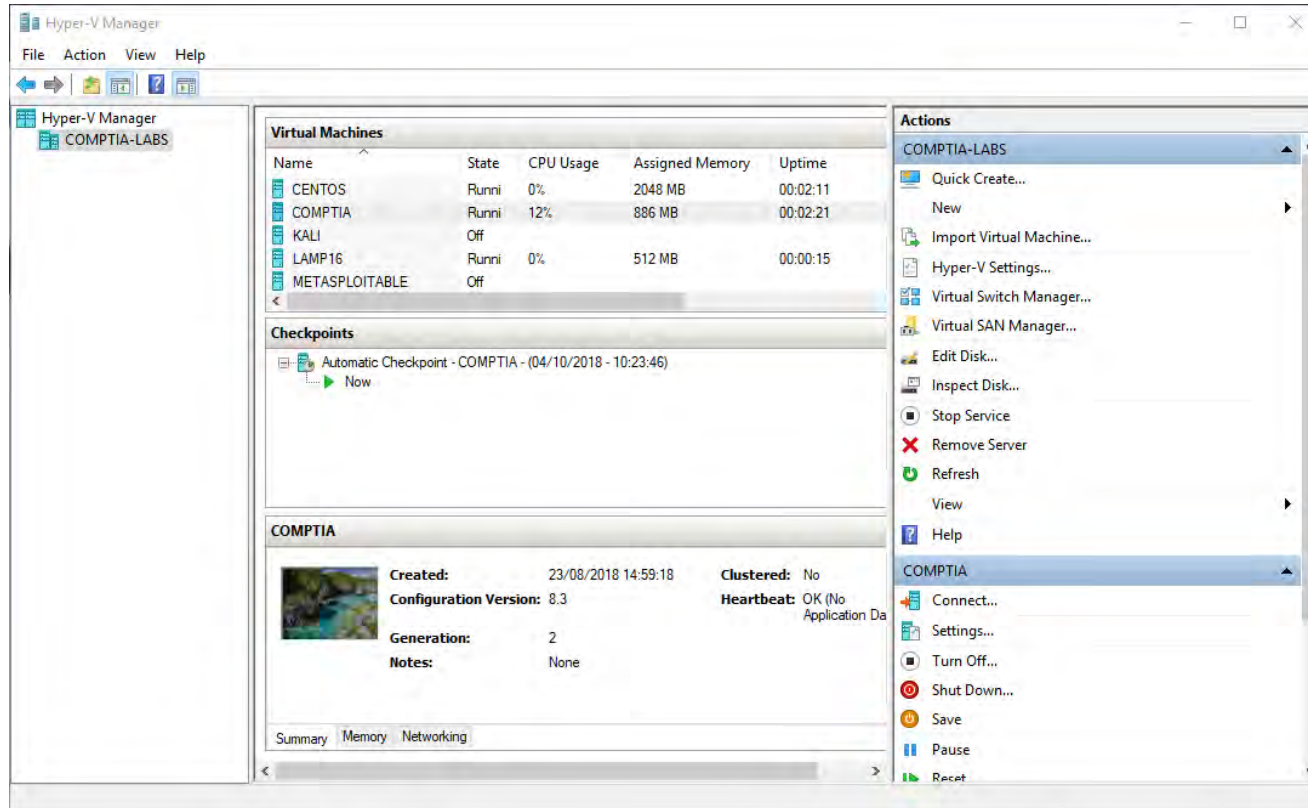


# Hypervisors

- Each VM runs in protected space
- View from inside the VM is a CPU and memory
- Hard disk is an image file
- Components such as network adapter are emulated
- Main functions of hypervisors
  - Emulation
  - Guest OS support
  - Assigning resources to each guest OS
  - Configuring networking
  - Configuring security



# Hypervisors

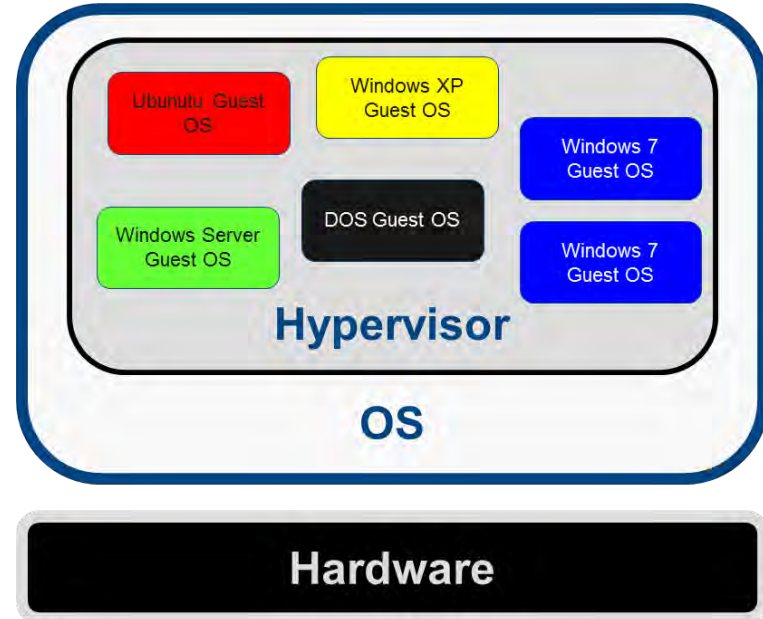


# Hypervisors



**Type 2 hypervisor:** A host-based hypervisor in which you install the host operating system first, then install the hypervisor.

- Examples:
  - VMware Workstation
  - Oracle Virtual Box
  - Parallels Workstation



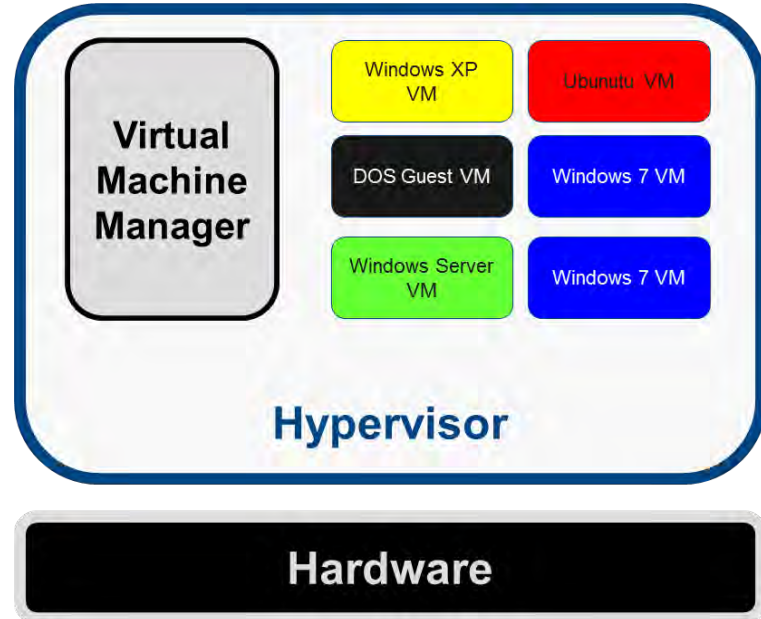


# Hypervisors)



**Type 1 hypervisor:** A bare metal hypervisor in which you install directly on the server's hardware.

- Examples:
  - VMware ESX Server
  - Microsoft Hyper-V
  - Citrix XEN Server
  - Linux KVM



# Hypervisors

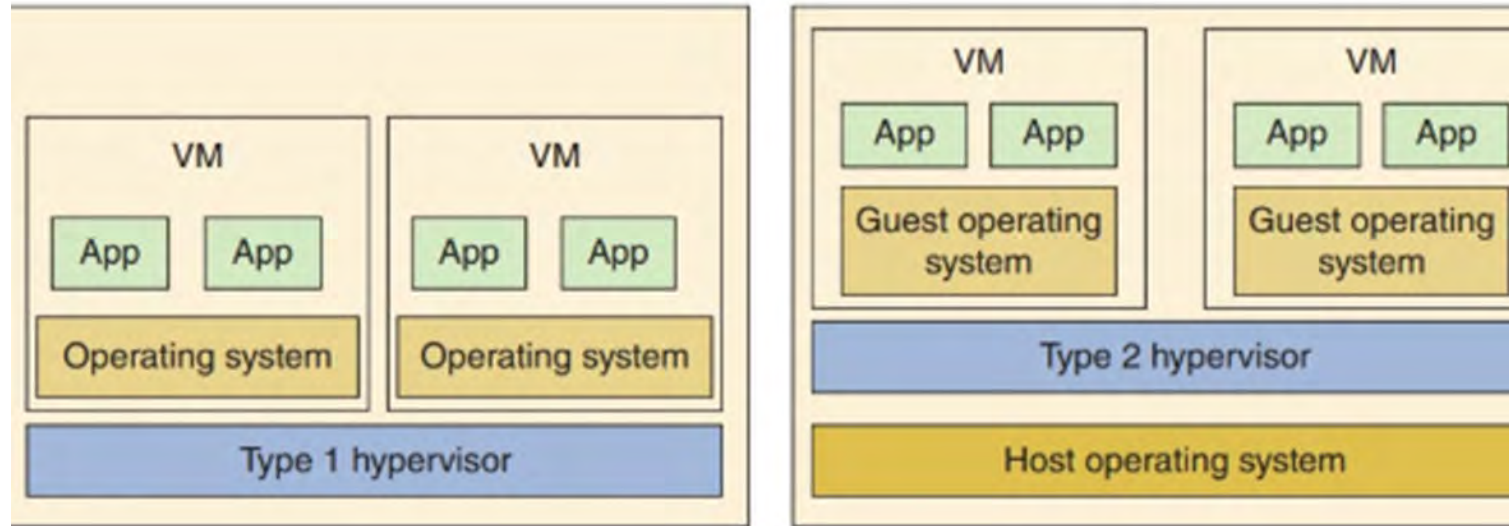
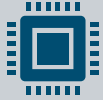


Figure 10-2 Type 1 and Type 2 hypervisors

# Processor Support and Resource Requirements

- CPU with built-in instruction sets to facilitate virtualization
  - Intel: VT-x
  - AMD: AMD-v
- SLAT **Second-level address translation** (SLAT) is a hardware virtualization technology that reduces hypervisor overhead
  - Intel: EPT
  - AMD: RVI
- Multiple CPU resources
  - SMP
  - Multiple physical processors
  - Multi-core

# Processor Support and Resource Requirements



Each guest OS requires memory above that required by the host.



Each guest OS requires hard disk space for the VM image.



Most hypervisors allow guest VMs to use host adapters and peripherals.

# Virtual Networks



Multiple VMs can communicate with each other using standard networking protocols.



Guest OS emulates standard network adapter hardware.

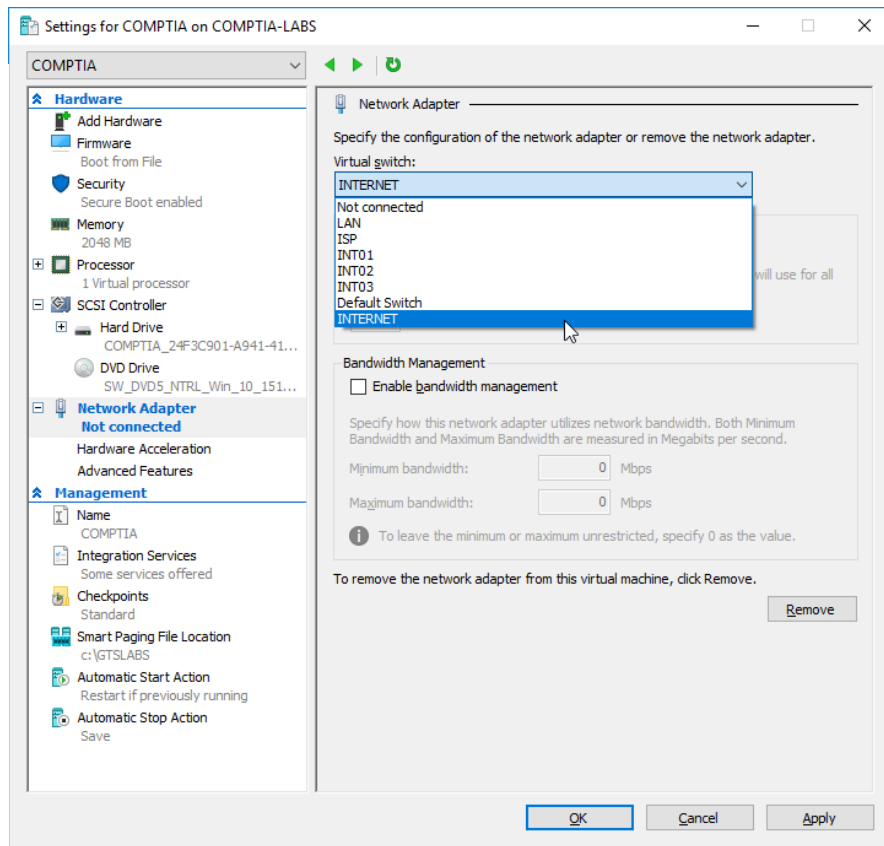
Can often have multiple adapters.  
Configurable just like a physical adapter.



Hypervisor implements network connectivity via virtual switches.

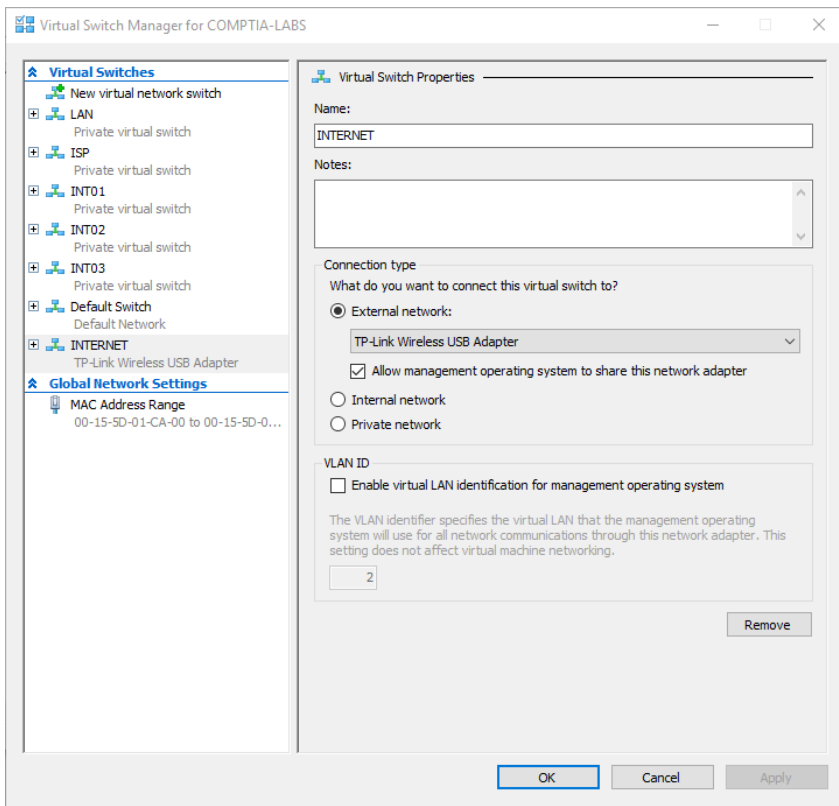
Function like Ethernet switches.  
Implemented in software.  
Connectivity between virtual adapters and virtual switches configured in hypervisor.

# Virtual Networks



# Virtual Networks

- Can configure connectivity between host physical NIC and virtual switches.
  - Provides a bridge between host platform and physical network switches.
- Allows frames to pass between:
  - Physical and virtual machines.
  - Virtual machines and the host.



# Virtual Machines



Client and Server OSs can be virtualized



Some hypervisors have limited support for certain OSs



Many purposes for deploying a virtual platform



Client-side virtualization

Deployed to desktop-type machines



Server-side virtualization



# Client-side virtualization



**Client-side virtualization:** Any solution designed to run on desktops or workstations in which the user interacts with the virtualization host directly.



Virtual labs



Support legacy  
software  
applications



Development  
environment



Training

# Client-side virtualization



**Server-side virtualization:** A solution in which one or more virtual servers are created on a physical server in which each virtual server acts like it was a separate computer.

**Server consolidation:** Using virtual servers, make more efficient use of system resources and hardware since most servers' capacity is not fully utilized.

- Better hardware utilization:
  - Typical server hardware resource utilization of 10%.
  - Implies 8-9 additional server instances could obtain the same performance.

# Security Requirements



**Rogue VM:** A virtual machine that has been installed without authorization.

**VM sprawl:** The uncontrolled development of more and more virtual machines.

## Guest OS Security

- Each guest OS must be patched and protected against malware
- Running security software on each guest OS can cause performance issues.
- Rogue VMs and VM sprawl are major security concerns.
  - System management software can detect rogue VMs.
  - VMs should conform to an application template.
  - Rogue developers often install backdoors and logic bombs.

# Security Requirements



**MTBF:** The rating on a device or component that predicts the expected time between failures.

**Denial of Service (DoS):** A network attack that aims to disrupt a service, usually by overloading it.

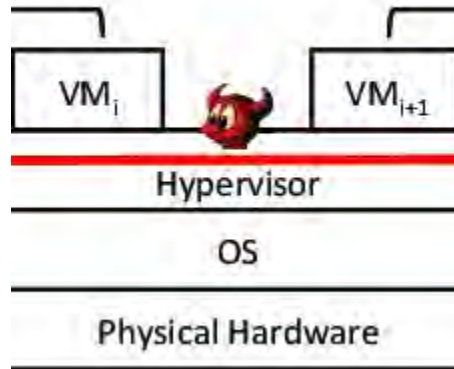
## Host Security

- If **host** is **compromised**, **so are guest OSs**.
- Host hardware failures are a single point of failure.
- DOS attack on host or hypervisor causes more damage than to a single server.
  - Most hypervisors support disk snapshots to revert to saved image.
  - Snapshots can be misused to perform DoS attacks.

# Security Requirements



**VM escaping:** Malware running on a guest OS jumping to another guest or to the host.



## Hypervisor Security

- Hypervisor provides another attack surface
- Few attacks have been detected so far
- Keep hypervisor up-to-date with patches to help prevent VM escapes

# Discussing Client-Side Virtualization Configuration

- What might you need to install to a guest OS to make full use of a hypervisor's features?
- **ANSWER:**
  - The drivers for the emulated hardware (often referred to as an extensions, additions, or integration components).



# Discussing Client-Side Virtualization Configuration

- What is a Type 2 hypervisor?

Get wrong

- **ANSWER:**

- Hypervisor software that must be installed to a host OS. A Type 1 (or bare metal) hypervisor is installed directly on the host PC.



# Discussing Client-Side Virtualization Configuration

- True or false? VMs can be networked together by using a virtual switch, which is implemented in software by the hypervisor.
- **ANSWER:**
  - True.





# Discussing Client-Side Virtualization Configuration

- What is a guest OS?
- **ANSWER:**
  - An OS installed on a virtual machine running within the virtual environment.



# Activity 7-1: Discussing Client-Side Virtualization Configuration

- What system resources are most important on a system designed to host multiple virtual machines?
- **ANSWER:**
  - The CPU must support virtualization extensions (and ideally be multi-processor or multicore), and there must be plenty of **system memory** and disk space.

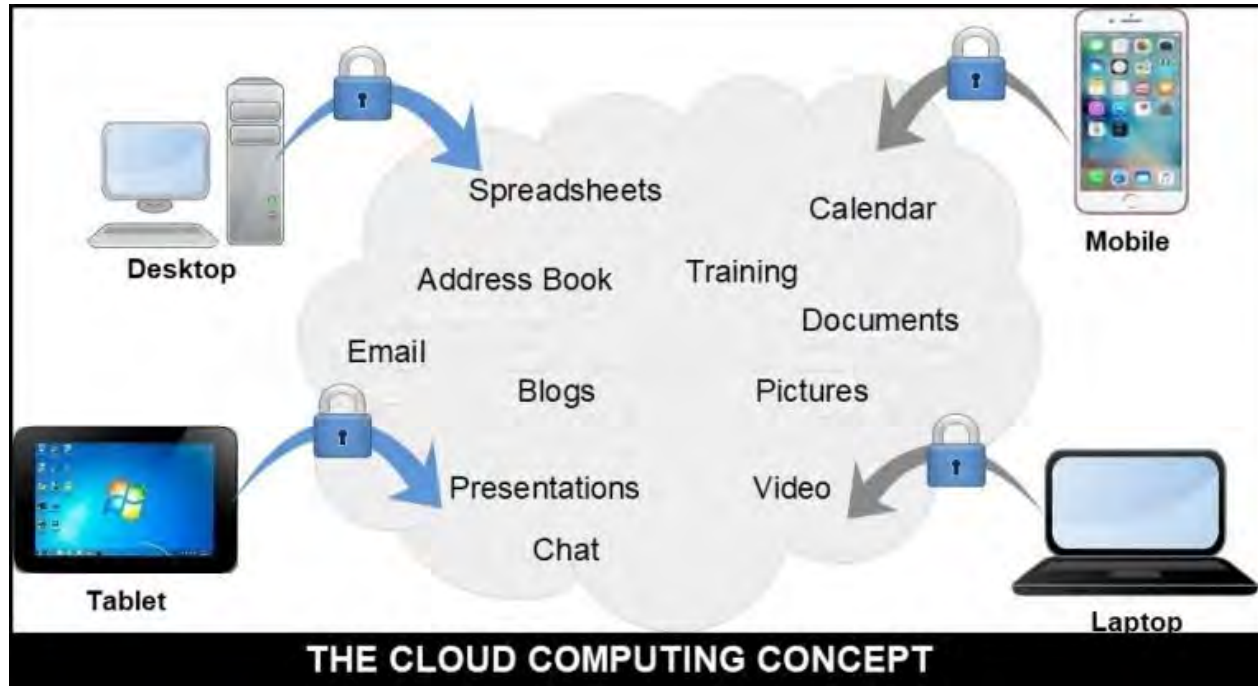


# Discussing Client-Side Virtualization Configuration

- If users have access to virtualization tools, what network security controls might be required?
- **ANSWER:**
  - A VM needs to be subject to network access control and authorization, like any physical computer device.
  - The VMs need to be checked to ensure they are not running malware, for instance.



# Topic B: Cloud Computing Concepts



# Cloud Computing



**Cloud:** are the features that distinguish a cloud provisioning model from on-premises or hosted client/server network architecture.

- NIST definition for cloud computing:  
Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services)

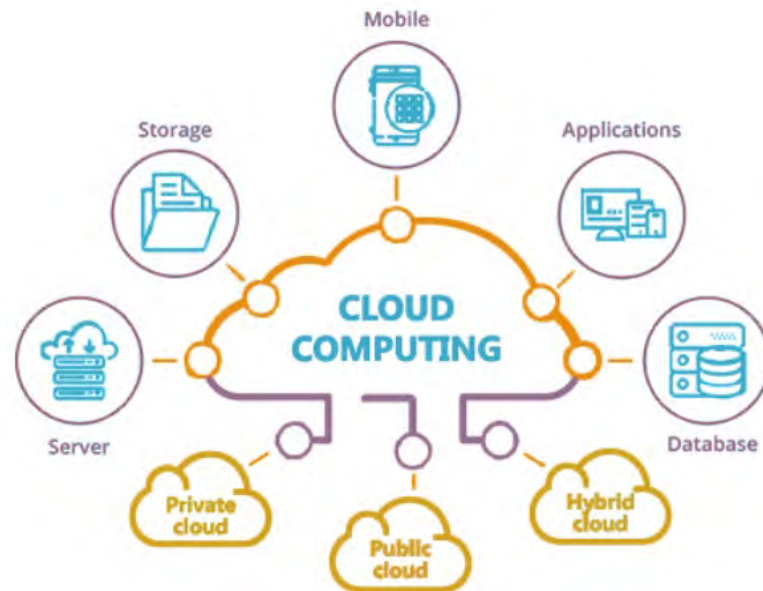
That can be rapidly provisioned and released with minimal management effort or service provider interaction.

(<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>, section 2.)

# Cloud Computing

## 5 components of cloud computing

- Resource allocation through:
- Rapid elasticity
- Resource pooling.
- On-demand self-service.
- Measured service



# Benefits of Cloud Computing



**Rapid elasticity:** refers to the system's ability to handle changes to demand in real time.

**Measured service:** A provider's ability to control and bill a customer's use of resources.

- Rapid elasticity
- On-demand and pay-per-use
- Measured service
- Resource pooling
- Flexibility

# Common Cloud Models

*in progress*

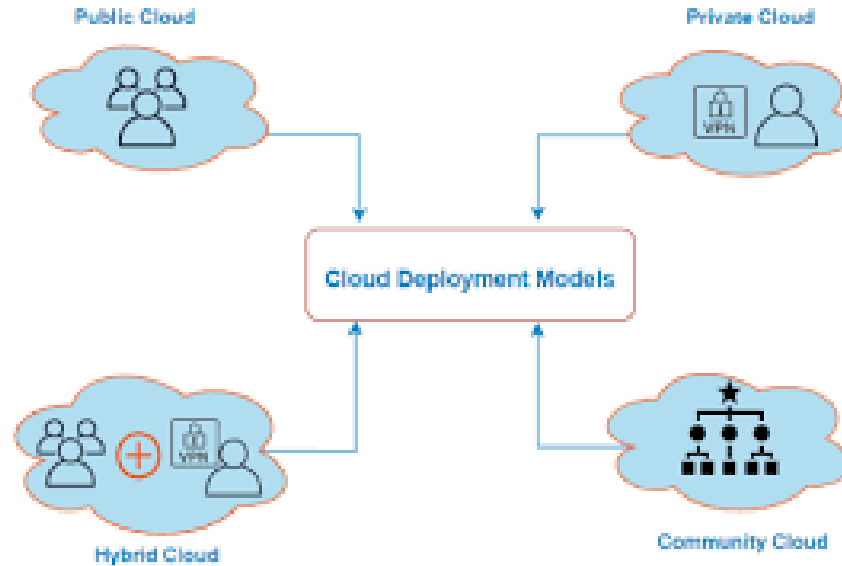
Public or multi-tenant

Hosted private

Private

Community

Hybrid





# Internal and External Shared Resources

- All networks share pool of resources
- File servers provide disk storage resources to clients
  - Shared folders
- Servers use shared disk storage
  - SANs
- Mix of virtualization and hybrid cloud solutions
  - Allows shared resources to be provisioned using:
    - Internally owned assets
    - Externally provisioned assets

# Cloud Service Options

Test



**IaaS:** A service that enables a consumer to outsource computing equipment purchases and running their own data center.

**SaaS:** A service that enables a service provider to make applications available over the Internet.

**PaaS:** A service that enables consumers to rent fully configured systems that are set up for specific purposes.

# Cloud Service Options



**IaaS: Infrastructure**

**SaaS: Software**

**PaaS: Platform**

## The best cloud computing services:

**Microsoft Azure.** The best cloud services platform. ...

**Amazon Web Services.** The most popular cloud computing service. ...

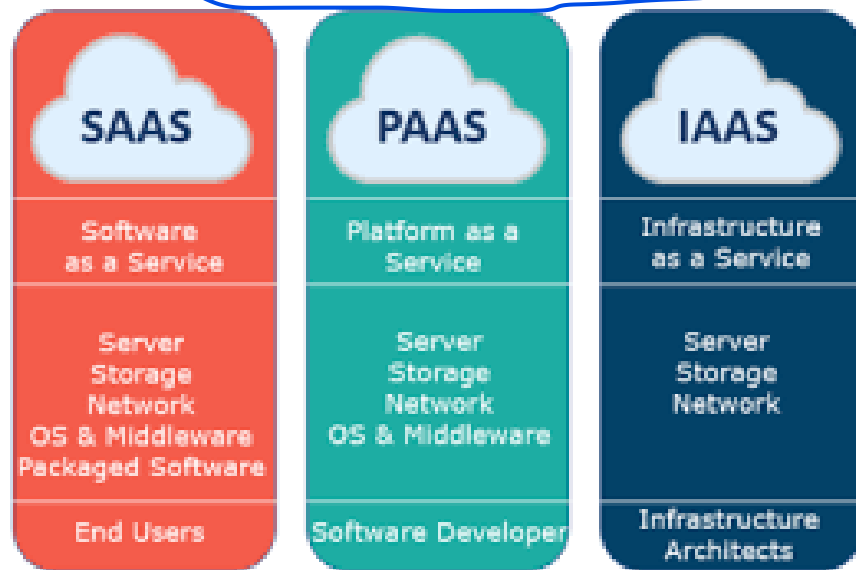
**Google Cloud.** Google's powerful cloud computing alternative. ...

**IBM Cloud.** Reasonably priced cloud services from one of the tech masters. ...

**Oracle Cloud Infrastructure.** ...

**CloudLinux.**

after picking up the type of cloud we pick what we want it to do



# Virtual Desktops



**VDI:** Using a VM as a means of provisioning corporate desktops.

**VDE:** The virtual desktop environment or workspace.

- Desktop computers are replaced by low-spec, low-power thin client computers.
- The thin client boots a minimal OS, allowing the user to log on to a VM stored on the company server infrastructure.
- All application processing and data storage in the VDE or workspace is performed by the server.

# Virtual Desktops

- All data is stored on the server, so it is easier to back up, and the desktop VMs are easier to support and troubleshoot
- VDIs are better locked against unsecure user practices.
- The main disadvantage is that in the event of a failure in the server or network infrastructure, users have no local processing ability.
- Virtual NIC

# Cloud-Based Applications



Application virtualization:

- Rather than run the whole client desktop as a virtual platform. The client accesses a particular application hosted on a server or streams the application from the server.

Virtual application streaming:

- Just enough of an application is installed on the end user device for the system to recognize that the application.

# Cloud-Based Applications



- Off-site email applications
- Cloud file storage
- Virtual application streaming
- Client platforms

## Benefits of cloud apps

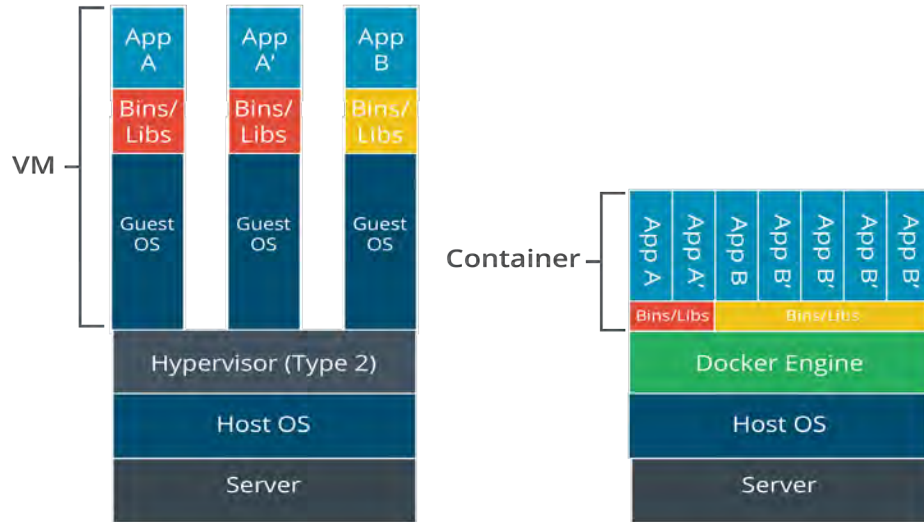


# Container Virtualization



**Container virtualization:** Enforces resource separation at the operating system level with each user having a separate instance to run in.

## Container vs. VMs





# Software-Defined Networking (SDN)

Networking devices have different functional planes of operation:

- Data, control & Management planes

- Split the functions into separate logical units will extend the functionality and management of a single device.

Perfectly built for cloud operations.

Application layer / Management plane

- Configure and manage the device
- SSH, browser, API

Control layer / Control plane

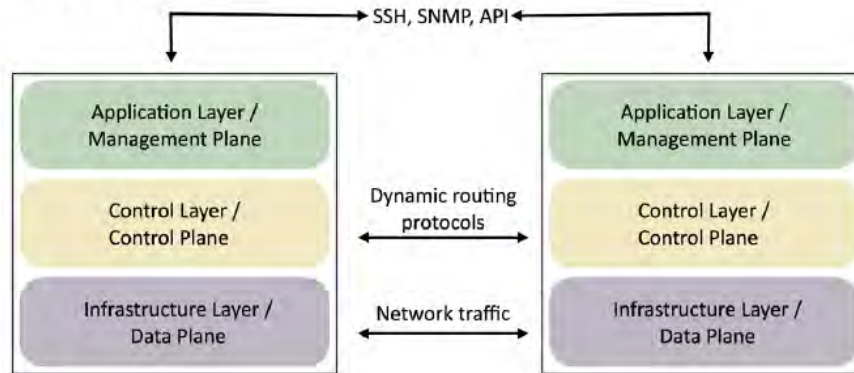
- Manages the actions of the Data plane
- Routing tables, session tables, NAT
- Dynamic routing protocol updates

Infrastructure layer / Data plane

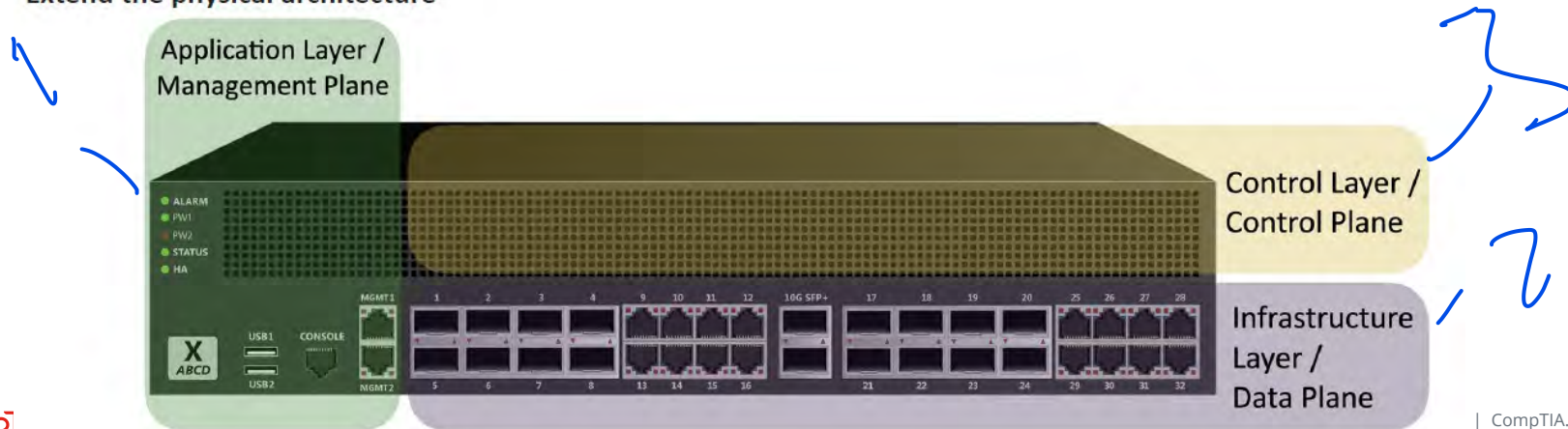
- Process the network frames, packets
- Forwarding, trunking, encrypting, NAT

# Software-Defined Networking (SDN)

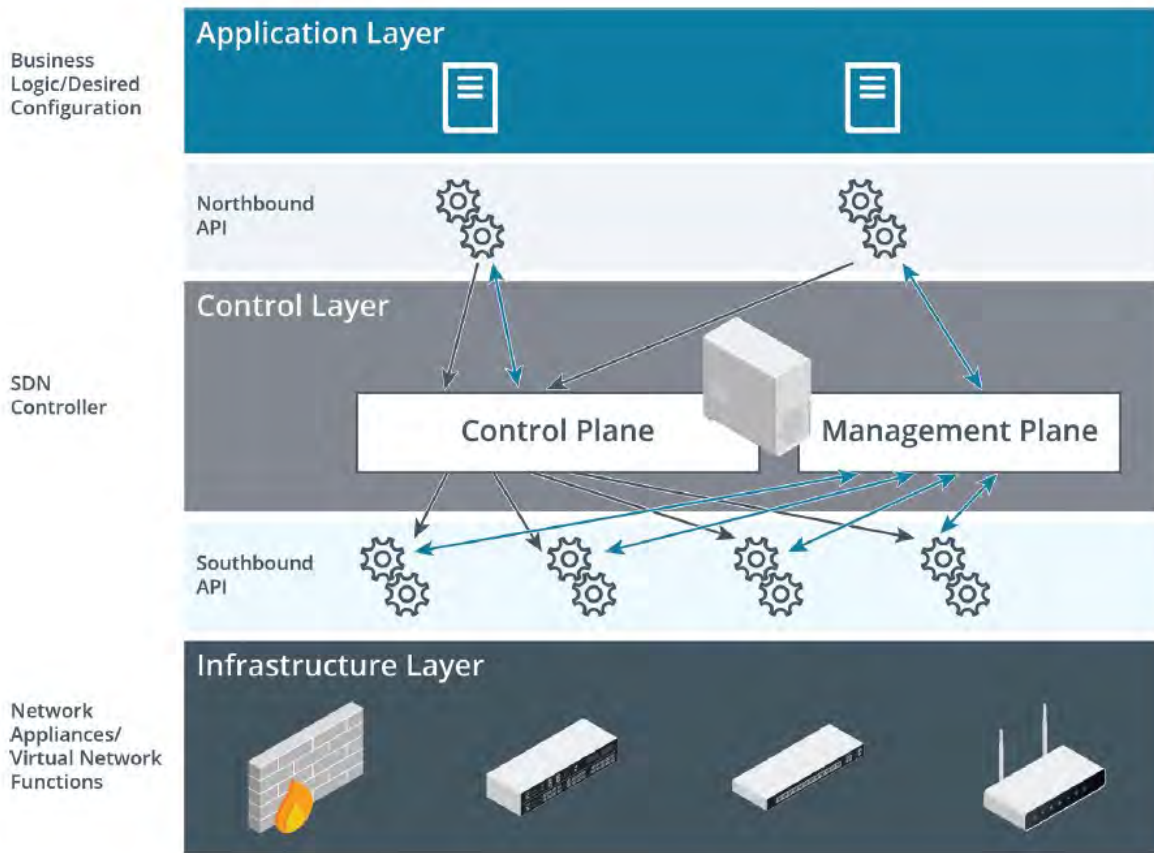
SDN data flows



Extend the physical architecture



# Software-Defined Networking (SDN)



# Discussing Cloud Computing Concepts

- A cloud service should exhibit rapid elasticity, allow users to access resources on-demand, and pay on a per-use basis. What type of service should the provider run to enable these features?
- **ANSWER:**
  - A measured service with the resources to cope with changing demands.



# Discussing Cloud Computing Concepts

- Which type of cloud would your organization be likely to use?
- **ANSWER:**
  - private cloud solution as the most secure.
  - community cloud solution as the least secure.



# Discussing Cloud Computing Concepts

- How do the five components of cloud computing defined by the NIST work together to provide users with cloud computing services?

- **ANSWER:**

- Resource allocation through:
- Rapid elasticity
- Resource pooling.
- On-demand self-service.
- Measured service.

*info*



# Discussing Cloud Computing Concepts

- When users connect to the network, they use a basic hardware terminal to access a desktop hosted on a virtualization server. What type of infrastructure is being deployed?
- **ANSWER:**
  - Virtual Desktop Infrastructure (VDI).

