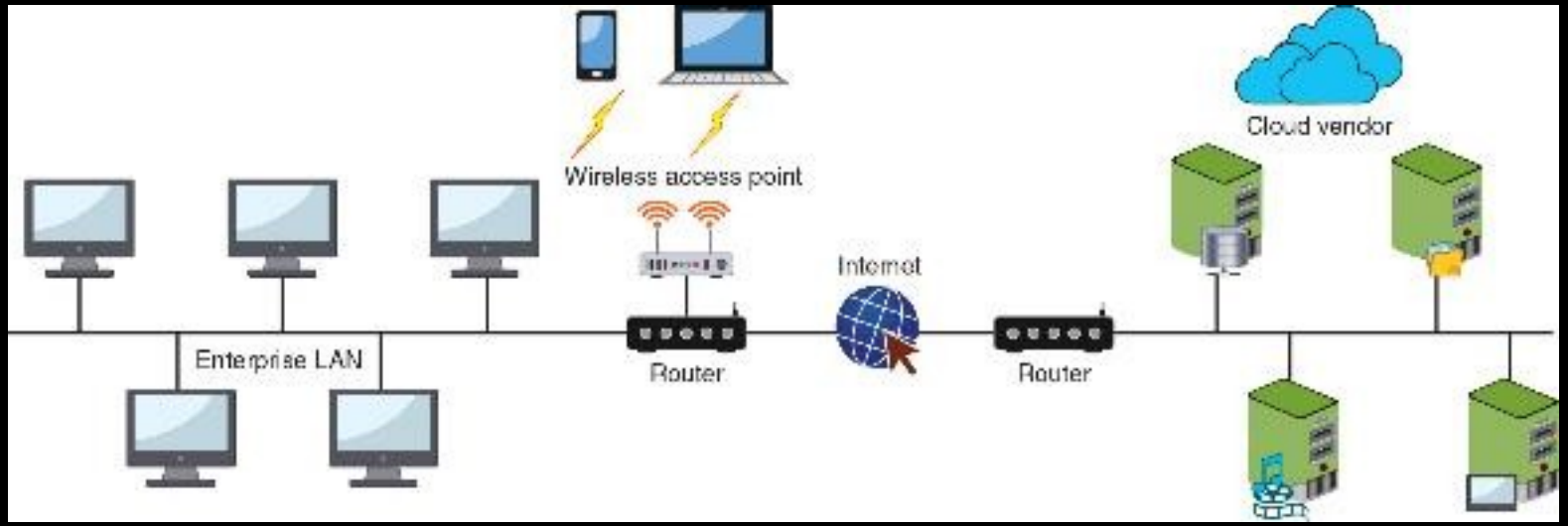
Chapter 11: Cloud and Virtualization Security

Introduction to Cloud Computing

- **Cloud computing** is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources
  - Entities that offer cloud computing are called **cloud service providers**
- Cloud computing cost savings is due to the following factors:
  - Elasticity and scalability
  - Pay-per-use
  - On demand
  - Resiliency

Cloud Computing



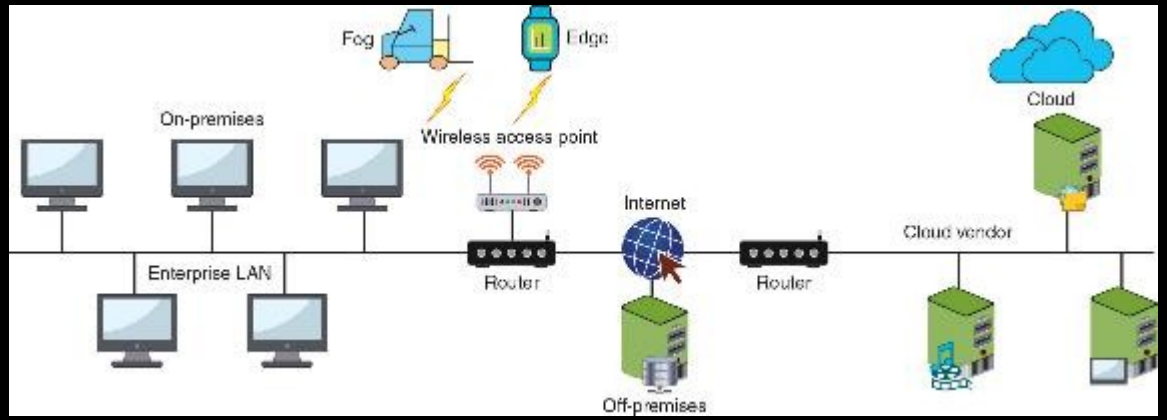
Introduction to Cloud Computing

Characteristic	Explanation
On-demand self-service	The consumer can make changes, such as increasing or decreasing computing resources, without requiring any human interaction from the service provider
Universal client support	Virtually any networked devices (desktop, laptop, smartphone, tablet, etc.) can access cloud computing resources
Invisible resource pooling	The physical and virtual computing resources are pooled together to serve multiple, simultaneous consumers that are dynamically assigned or reassigned based on the consumer's needs; the customer has little or no control or knowledge of the physical location of the resources
Immediate elasticity	Computing resources can be increased or decreased quickly to meet demands
Metered services	Fees are based on the computing resources used

Types of Clouds

- A **public cloud** is one in which the services and infrastructure are offered to all users with access provided remotely through the Internet
- A **community cloud** is a cloud that is open only to specific organizations that have common concerns
- A **private cloud** is created and maintained on a private network
- A **hybrid cloud** is a combination of public and private clouds

Cloud Locations



Instead of using a centralized model, cloud computing takes place in several different locations (a **decentralized** model)

Cloud Locations

Location	Description	Example
On-premises	Computing resources located on the campus of the organization (“on-prem”)	Desktop computer, local area network, data center
Off-premises	A computing resource hosted and supported by a third party	Remote backup facility
Fog	A decentralized computing infrastructure in which data, compute capabilities, storage, and applications are located between the data source and the cloud	Automated guided vehicles on an industrial shop floor
Edge	Computing that is performed at or very near to the source of data instead of relying on the cloud or on-prem for processing	Internet of Things device
Cloud	A remote facility for computing	Artificial intelligence processing engine

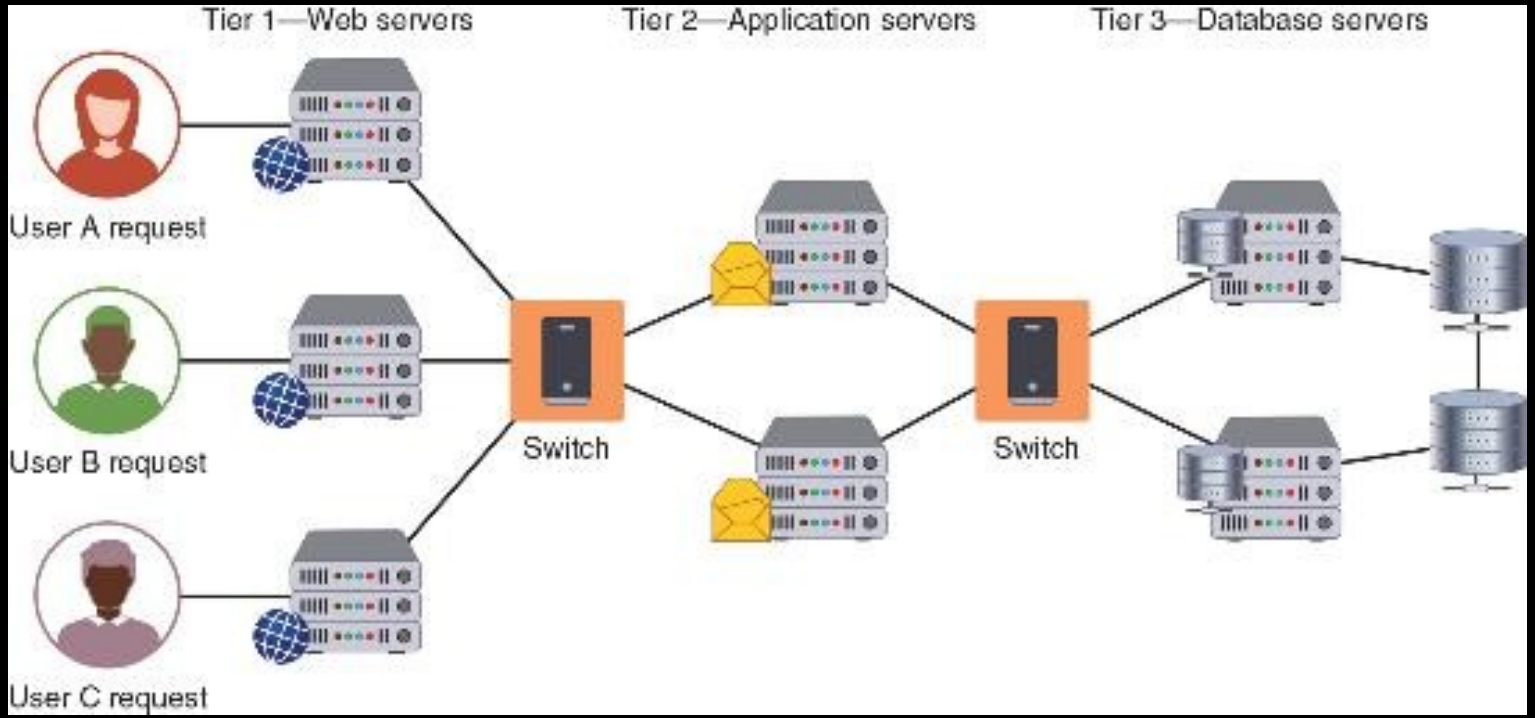
Cloud Architecture

- A **thin client** is a computer that runs from resources stored on a central cloud server instead of a localized hard drive
- A **transit gateway** is an Amazon Web Services (AWS) technology that allows organizations to connect all existing virtual private clouds (VPCs), physical data centers, remote offices, and remote gateways into a single managed source
- A **serverless infrastructure** is one in which the capacity planning, installation, setup, and management are all invisible to the user because they are handled by the cloud provider

Cloud Models

- **Software as a Service (SaaS) –** the vendor provides access to the vendor's software applications running on a cloud infrastructure
- **Platform as a Service (PaaS)** – consumers install and run their own specialized applications on the cloud computing network
- **Infrastructure as a Service (IaaS) –** the vendor allows customers to deploy and run their own software, including OSs and applications
- **Anything as a Service (XaaS) –** a broad category of subscription services related to cloud computing

Three-Tier Architecture



Cloud Management

- Cloud management can be conducted by the local organization performing the work itself or by contracting with a third-party management service provider
- **Services integration** attempts to achieve a “boundary-less” approach
  - It involves integrating all users across the enterprise who are using cloud computing

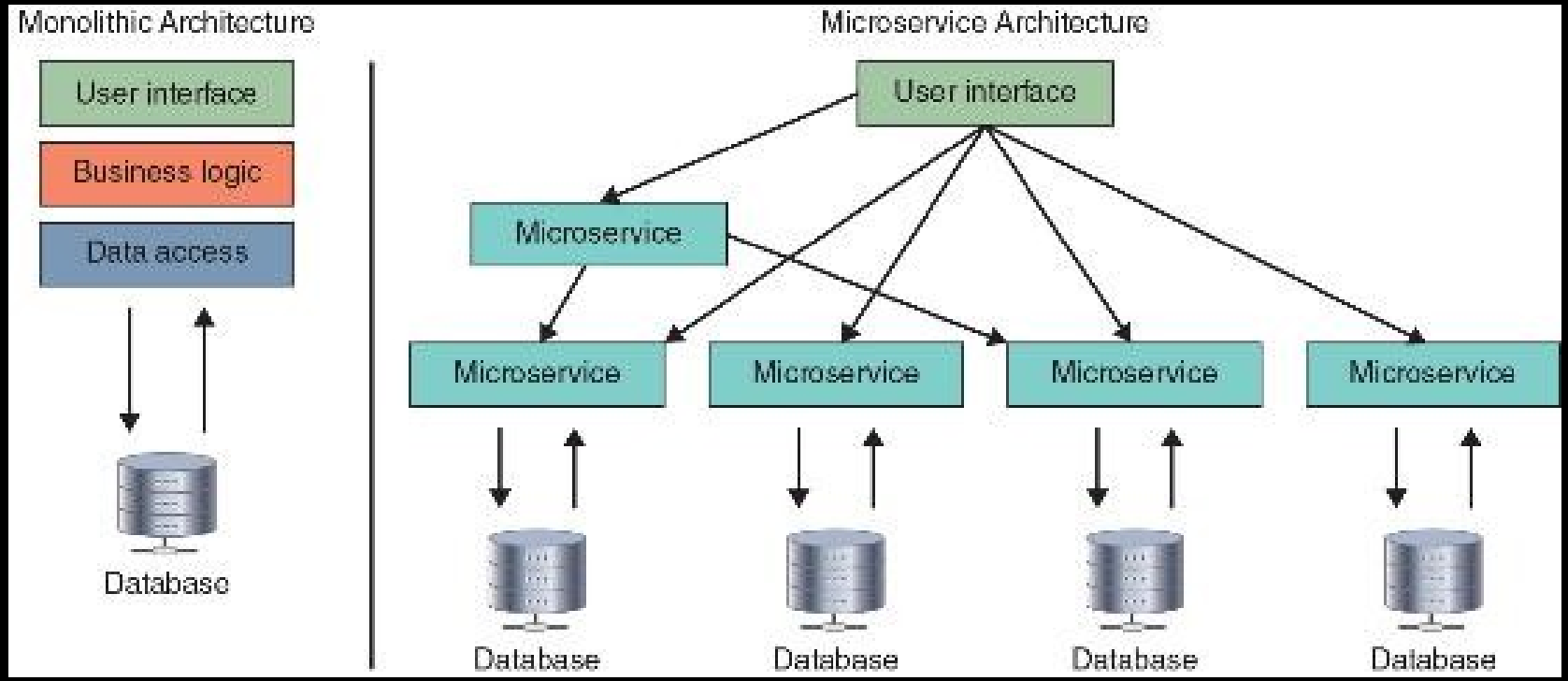
Cloud Management

- When managing cloud computing locally, it is important to have written resource policies in place
- A managed service provider (MSP) delivers services through ongoing and regular support as well as active administration of those resources
- An MSP can manage on the customer’s premises, in the MSP’s own data center, in a third-party data center, or in a cloud computing environment
- A managed security service provider (MSSP) can assist with or fully assume cybersecurity defenses

Cloud-Native Microservices

- Traditional application design is often called “monolithic” because the entire program is developed as a single entity
- The solution to monolithic application design is to divide it into smaller entities
  - Each entity is a specialized part of the code (known as **microservices**)
- A microservice architecture has smaller and more specialized elements, each of which manages its own database, generates its own logs, and handles user authentication (performed by microservices APIs)

Monolithic vs Microservices



Question

- Ash has been given a project to manage the development of a new company app. He wants to use a cloud model to facilitate the development and deployment. Which cloud model should he likely choose?

Answer

- Ash has been given a project to manage the development of a new company app. He wants to use a cloud model to facilitate the development and deployment. Which cloud model should he likely choose?
- Platform as a Service (PaaS) provides a software platform on which the enterprise or users can build their own applications and then host them on the PaaS provider’s infrastructure. The software platform can be used as a development framework to build and debug the app and then deploy it.

Cloud-Based Security

- Virtual security devices can provide protection in a cloud computing environment
- A cloud firewall is virtual software that functions in a similar manner to a physical security appliance by examining traffic into and out of the cloud
- A **secure web gateway** (**SWG**) examines both incoming and outgoing traffic and performs basic URL and monitoring web applications
  - A SWG also analyzes received traffic, performs data loss prevention (DLP), and provides alerts to a monitoring device like a SIEM appliance

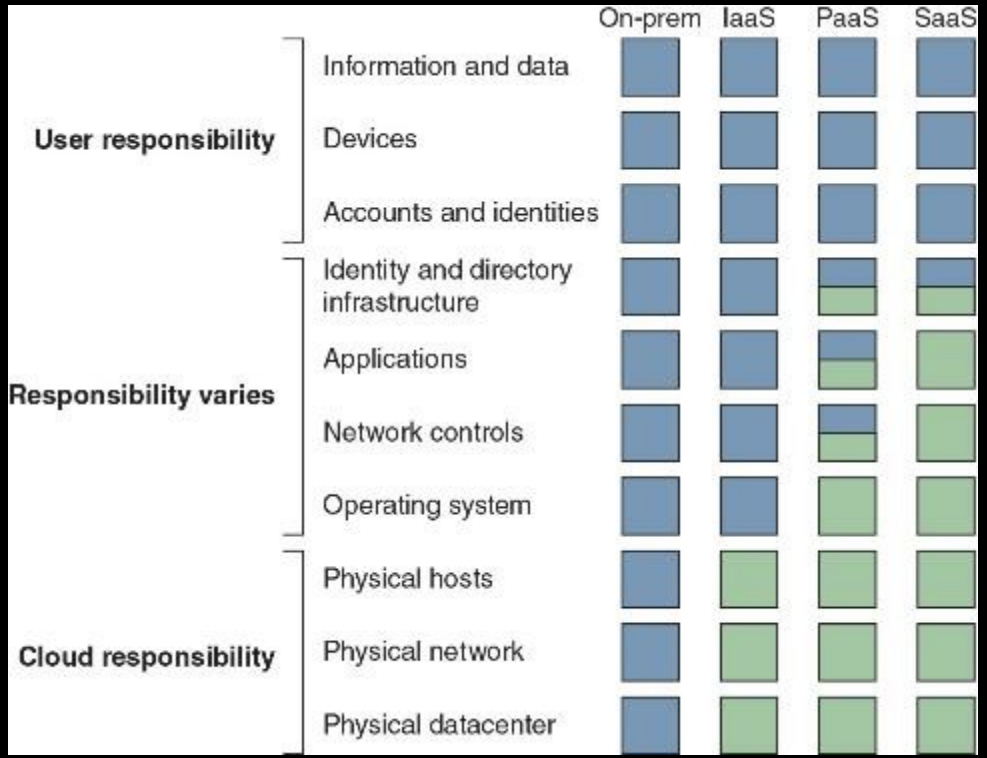
Cloud-Based Security

- A **cloud access security broker** (**CASB**) is a set of software tools or services that resides between an enterprise's on-prem infrastructure and the cloud provider's infrastructure
- CASB acts as a "gatekeeper", ensuring that the security policies of the enterprise extend to its data in the cloud
- A **secure access service edge** (**SASE**) is the convergence of several security services into a single, cloud-delivered service model
  - Various technologies that make up SASE include SWG, CASB, zero-trust architecture (ZTA), and WAN technologies

Cloud Vulnerabilities

Security issue	Description
Unauthorized access to data	Improper cloud security configurations can result in data being left exposed
Lack of visibility	Organizations have limited or no visibility into the security mechanisms of the cloud provider and thus cannot verify the effectiveness of security controls
Insecure APIs	While APIs help cloud customers customize their PaaS by providing data recognition, access, and effective encryption, threat actors can exploit a vulnerable API
Compliance regulations	Maintaining compliance requires that an organization know where their data is, who can access it, and how it is protected, but this can be difficult in an opaque cloud system where the transparency is lacking
System vulnerabilities	A cloud infrastructure is prone to system vulnerabilities due to complex networks and multiple third-party platforms

Responsibility Matrix



There needs to be clear understanding of who is responsible for each security element

Cloud Vulnerabilities

- Physical networks use the Open Source Interconnection (OSI) seven-layer model to illustrate network functionality
- With cloud computing, the OSI model is no longer as useful
- The lack of a conceptual model like the OSI model makes selecting and managing security virtual devices more challenging
  - Different cloud-based conceptual models are starting to be proposed
  - However, no single model has been widely adapted

Cloud Security Controls

- Securing cloud computing involves using controls such as the following:
  - **Conducting audits –** a **cloud security audit** is an independent examination of cloud service controls
  - **Use Regions and Zones –** reliability and resiliency are achieved through duplicating processes across one or more geographical areas (called **high availability across zones**)
  - **Secrets management –** enables strong security and improved management of a microservices-based architecture, allowing the entire cloud infrastructure to remain flexible and scalable without sacrificing security

Cloud Security Controls

- Hybrid clouds have special security challenges (called **hybrid cloud considerations**) due to their nature of spanning both public and private spaces

Cloud Security Controls

- Best practices of hybrid clouds include the following:
  - Encrypt sensitive data and data traffic between two clouds and inspect all encrypted traffic
  - Monitor and audit configurations and use automation, rather than manual management
  - Run regular scans to identify weak points
  - Secure all endpoints
  - Enforce zero-trust security

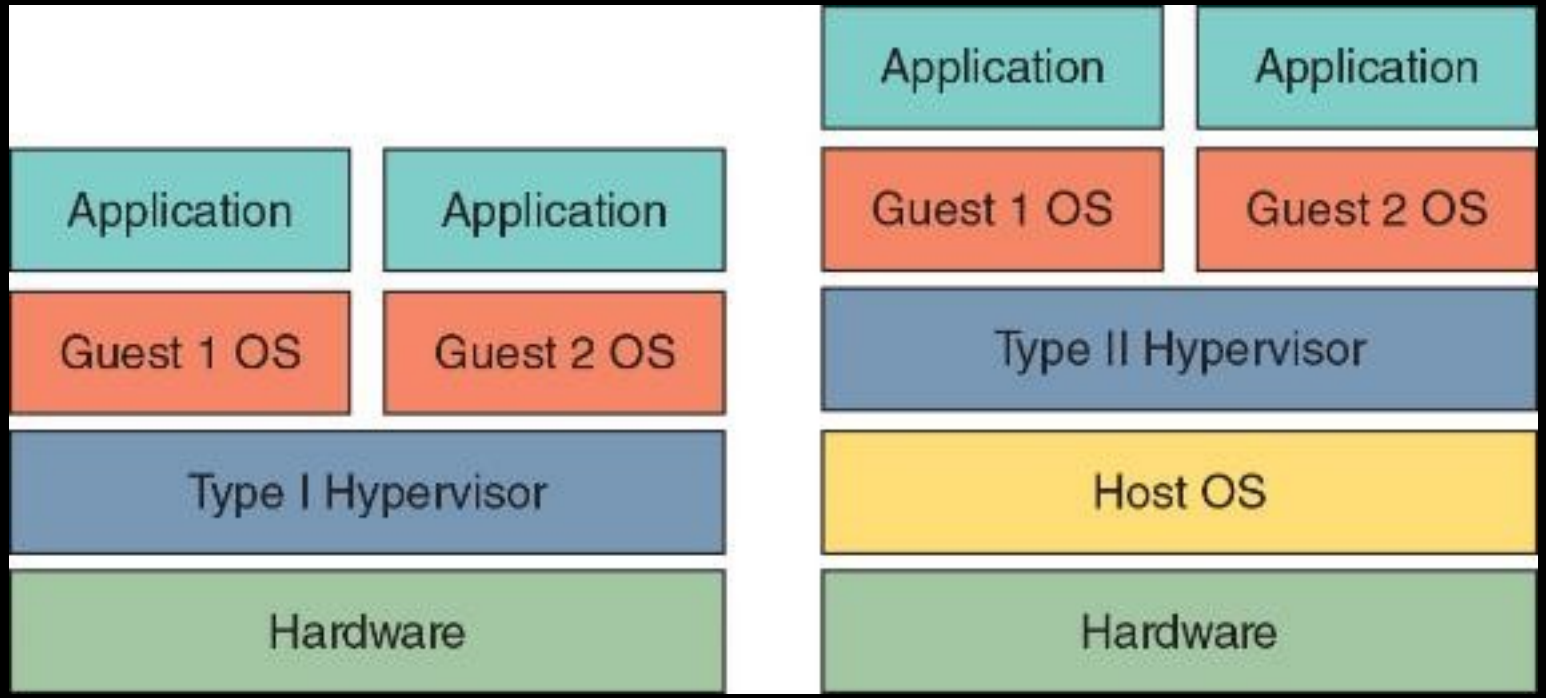
Defining Virtualization

- **Virtualization** is a means of managing and presenting computer resources without regard to physical layout or location
- Host virtualization is a type of virtualization in which an entire operating system environment is simulated
- A **virtual machine** (**VM**) is a simulated software-based emulation of a computer
- The “host system” runs a VM monitor program that supports one or more “guest systems”

Defining Virtualization

- Virtualization is used to consolidate multiple physical servers into VMs that can run on a single physical computer
- The VM monitor program is called a **hypervisor**, which manages the VM operating systems
- There are two types of hypervisors:
  - **Type I** – run directly on the computer's hardware instead of the underlying OS
  - **Type II** – run on the host OS, much like an application

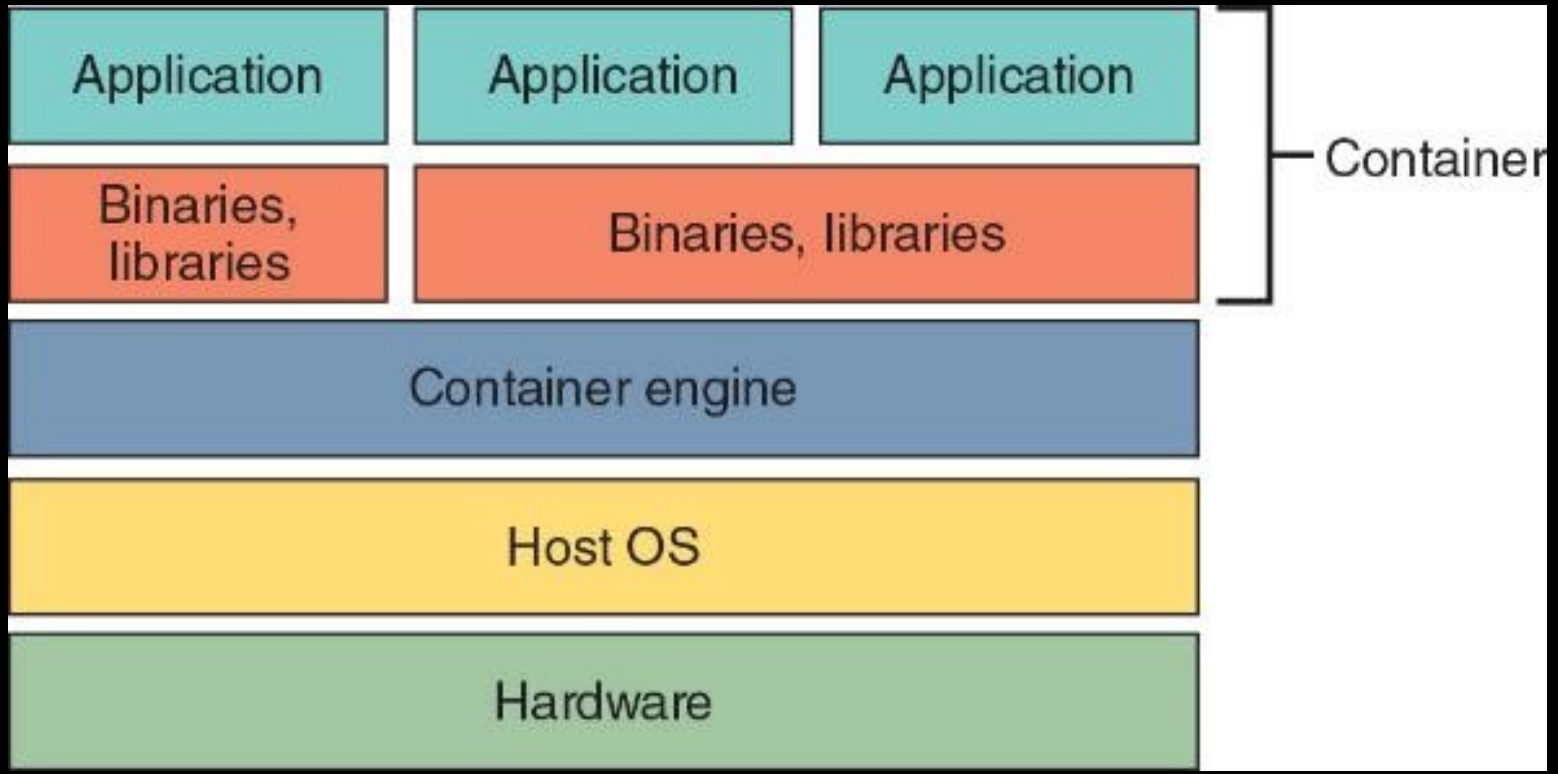
Type I and Type II Hypervisors



Defining Virtualization

- A **container** holds only the necessary OS components that are needed for that specific application to run
  - It reduces the necessary hard drive storage space and RAM needed
  - It allows for containers to start more quickly because the OS does not have to be started
- A common application of virtualization is **virtual desktop infrastructure** (**VDI**), which is the process of running a user desktop inside a remote VM that resides on a server

Containers


Application
Application
Application
Binaries, libraries
Binaries, libraries
Container
Container engine
Host OS
Hardware

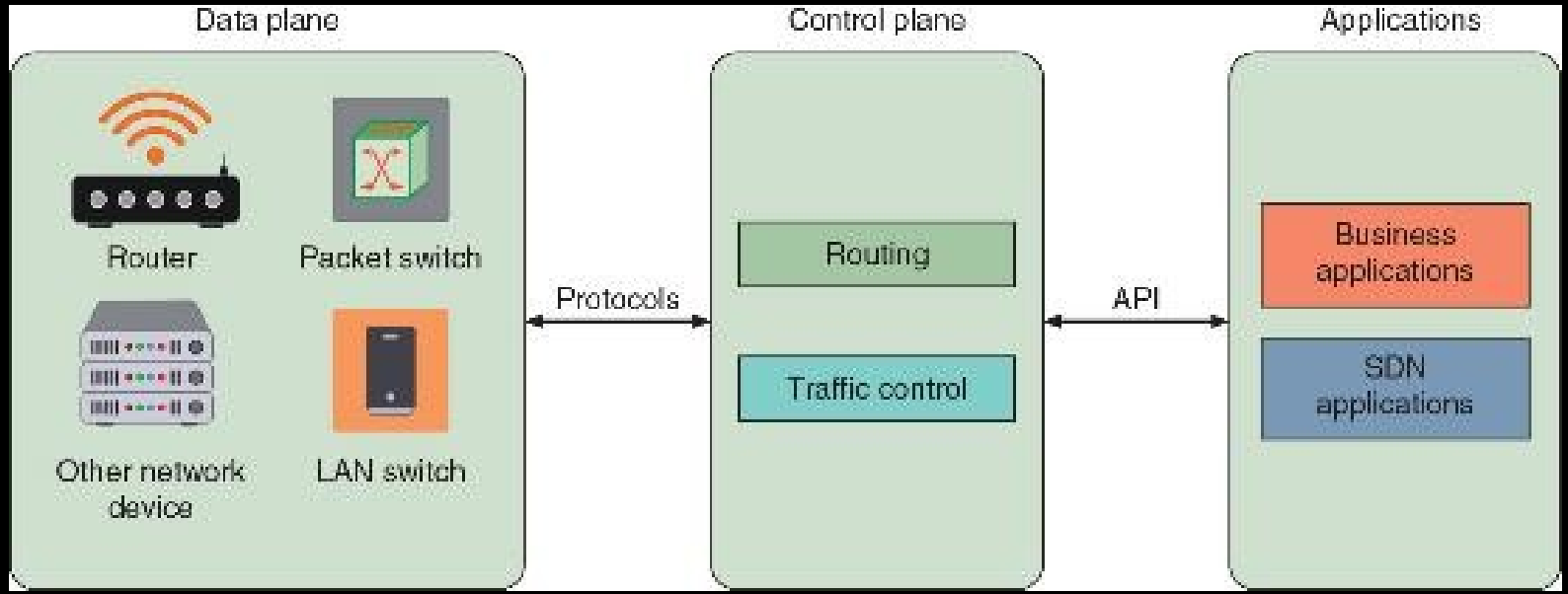
Advantages of Virtualization

- New virtual server machines can be made available (host availability), and resources can easily be expanded or contracted as needed (host elasticity)
- Virtualization can reduce costs
  - Fewer physical computers must be purchased and maintained
- It can provide uninterrupted server access to users
  - Virtualization supports live migration, which allows a virtual machine to be moved to a different physical computer with no impact to users

Infrastructure as Code

- A **software-defined network** (**SDN**) virtualizes parts of the physical network so that it can be more quickly and easily reconfigured
  - This is accomplished by separating the control plane from the data plane
- If traffic needs to flow through the network:
  - It receives permission from the SDN controller, which verifies the communication is permitted by the network policy of the enterprise
  - Once approved, the SDN controller computes a route for the flow to take and adds an entry for that flow in each of the switches along the path

Software-Defined Network



Infrastructure as Code

- A **software-defined wide area network** (**SD-WAN**) is a virtualized service that connects and extends enterprise WAN networks over large geographical distances
- SD-WAN is designed to solve challenges associated with a traditional WAN, such as integrating connectivity between the service provider and the organization

Infrastructure as Code

- A **software-defined visibility** (**SDV**) is a framework that allows users to create programs in which critical security functions can be automated
- SDV allows network administrators to automate multiple functions in a network infrastructure including:
  - Dynamic response to detected threat patterns
  - Adjustments to traffic mode configurations for in-line security tools
  - Additional IT operations-management functions and capabilities

Security Concerns for Virtualization

- Security-related advantages of virtualization include:
  - Test latest security updates by downloading on a virtual machine before installing on production computers
  - A snapshot of a particular state of a virtual machine can be saved for later use
  - Testing the existing security configuration *(*security control testing*)* can be performed using a simulated network environment
  - VMs can promote security segregation and isolation

Security Concerns for Virtualization

- Security-related advantages of virtualization include (continued):
  - A suspicious program can be loaded into an isolated virtual machine and executed *(*sandboxing*)*
  - If the program is malware, only the virtual machine will be impacted

Security Concerns for Virtualization

- Security concerns for virtualized environments include:
  - Not all hypervisors have the necessary security controls to keep out attackers
  - Existing security tools were designed for single physical servers
  - VMs must be protected from both outside networks and other VMs on the same physical computer
  - VMs may be able to “break out” from the contained environment and directly interact with the host OS (called **VM escape**)
  - It is important to have virtual machine escape protection

Virtual Machine Manager