CCNP ENCOR Cram Notes

II. Virtualization

Virtualization technology is the process of creating a virtual version of something, such as hardware, software, storage devices, and network resources. Virtualization technology allows multiple virtual instances of resources to be created and used simultaneously on the same physical infrastructure, enabling greater flexibility, scalability, and cost-effectiveness.

There are several types of virtualization technology, including:

1. Server virtualization: This involves dividing a physical server into multiple virtual machines (VMs) that can run different operating systems and applications independently.

2. Network virtualization: This involves creating virtual networks on top of a physical network infrastructure to provide greater flexibility and agility in managing network resources.

3. Storage virtualization: This involves pooling physical storage resources from multiple devices and presenting them as a single virtual storage device.

4. Desktop virtualization: This involves running multiple desktop operating systems on a single physical device, allowing users to access their desktop environments from anywhere.

Virtualization technology has many benefits, including reducing hardware and maintenance costs, improving resource utilization, increasing flexibility and scalability, and enhancing disaster recovery capabilities. It is widely used in data centers, cloud computing, and other IT infrastructure environments to optimize resource utilization and improve efficiency.

1. Describe device virtualization technologies

1.1. Hypervisor type 1 and 2

A hypervisor is a software process that abstracts the hardware layer from the operating systems allowing multiple virtual machines to run simultaneously.

A Hypervisor also known as Virtual Machine Monitor (VMM) can be a piece of software, firmware or hardware that gives an impression to the guest machines(virtual machines) as if they were operating on a physical hardware. It allows multiple operating system to share a single host and its hardware. The hypervisor manages requests by virtual machines to access to

the hardware resources (RAM, CPU, NIC etc) acting as an independent machine.

Hypervisor is mainly divided into two types namely

Type 1/Native/Bare Metal Hypervisor
Type 2/Hosted Hypervisor

Type 1 Hypervisor

This is also known as Bare Metal or Embedded or Native Hypervisor. It works directly on the hardware of the host and can monitor operating systems that run above the hypervisor.
It is completely independent from the Operating System.
The hypervisor is small as its main task is sharing and managing hardware resources between different operating systems.A major advantage is that any problems in one virtual machine or guest operating system do not affect the other guest operating systems running on the hypervisor.

Type 2 Hypervisor: This is also known as Hosted Hypervisor.

In this case, the hypervisor is installed on an operating system and then supports other operating systems above it. It is completely dependent on host Operating System for its operations
While having a base operating system allows better specification of policies, any problems in the base operating system a ffects the entire system as well even if the hypervisor running above the base OS is secure.

1.2 Virtual machine

A virtual machine, commonly shortened to just VM, is no different than any other physical computer like a laptop, smart phone or server. It has a CPU, memory, disks to store your files and can connect to the internet if needed. While the parts that make up your computer (called hardware) are physical and tangible, VMs are often thought of as virtual computers or software-defined computers within physical servers, existing only as code.

Virtualisation is the process of creating a software-based or "virtual" version of a computer, with dedicated amounts of CPU, memory and storage that are "borrowed" from a physical host computer - such as your personal computer and/or a remote server such as a server in a cloud provider's datacentre. A virtual machine is a computer file, typically called an image, which behaves like an actual computer. It can run in a window as a separate computing environment, often to run a different operating system or even to function as the user's entire computer

experience - as is common on many people's work computers. The virtual machine is partitioned from the rest of the system, meaning that the software inside a VM cannot interfere with the host computer's primary operating system.

Here are a few ways virtual machines are used:

- Building and deploying apps to the cloud.
- Trying out a new operating system (OS), including beta releases.
- Spinning up a new environment to make it simpler and quicker for developers to run dev-test scenarios.
- Backing up your existing OS.
- Accessing virus-infected data or running an old application by installing an older OS.
- Running software or apps on operating systems that they were not originally intended for.

Back

1.3. Virtual switching

vSwitches are created under a virtualized server and enable VMs to communicate with each other and with external networks. Distributed virtual switching reduces administrative overhead by providing configuration consistency across all the hosts that are part of the distributed switch.

Virtual switching is a technology that enables the creation of virtual switches that can be used to connect virtual machines and other network resources within a virtualized environment. Virtual switches are software-based and provide the same functionality as physical switches, such as VLANs, QoS, and security policies. Virtual switches are commonly used in data center environments to simplify network management and improve resource utilization. Examples of virtual switches include Cisco Nexus 1000V, VMware vSphere Distributed Switch, and Microsoft Hyper-V Virtual Switch.
Examples of virtual machines:

1. Virtual servers: These are commonly used in enterprise environments to consolidate server resources and enable multiple operating systems to run on a single physical server.

2. Virtual desktops: These provide users with a virtualized desktop environment that can be accessed from any device, providing greater flexibility and mobility.

3. Virtual appliances: These are pre-configured virtual machines that provide specific

functionality, such as firewalls, load balancers, or web servers.

4. Virtual development environments: These are commonly used by software developers to create and test applications in a virtualized environment before deploying them to production.

5. Cloud-based virtual machines: These are virtual machines that are hosted in a cloud environment and can be accessed and managed remotely over the internet. Examples of cloud-based virtual machines include Amazon EC2, Microsoft Azure VMs, and Google Cloud VMs.

6. Virtual routers and switches: These are virtualized versions of network devices that can be used to provide routing and switching functionality in a virtualized environment.

Virtual Network Function (VNF): VNF focus primarily on optimization of the network services, contrary to software-defined networking (SDN), which separates the control and forwarding plane for a centralized view of the network. VNF basically provides a virtual networking device that a customer can access and configure according to his security/access requirements. It is also possible that a group of virtual devices form a virtual network function, and is offered to the customer. Network Functions Virtualization (NFV) is different from VNF in the sense that the former is used by the service providers for virtualizing the SPs' networking functions.

Note: In Cisco's official version VNF represents a single virtual device. Some others use VNF and NFV interchangeably

2. Configure and verify data path virtualization technologies

2.1. VRF

Virtual routing and forwarding (VRF): VRF is an IP-based computer network technology that enables the simultaneous co-existence of multiple virtual routers (VRs) as instances or virtual router instances (VRIs) within the same router. One or multiple physical or logical interfaces may have a VRF but none of the VRFs share routes. Packets are forwarded only between interfaces on the same VRF.

VRFs work on Layer 3 of the OSI model. The independent routing instances allow users to deploy IP internet protocol addresses that overlap or are the same without conflict. Because users may segment network paths without multiple routers, network functionality improves one of the key benefits of virtual routing and forwarding.

Virtual Routing and Forwarding (VRF) is a technology used to create multiple routing tables within a single router or switch. Each VRF instance provides a separate virtual network with its own unique routing table, allowing multiple logical networks to coexist on a single physical infrastructure. VRFs are commonly used in service provider and enterprise environments to separate different customers or departments, ensuring that each group's traffic is kept separate and secure.

Advantages of Virtual Routing and Forwarding

1. Enables the virtual creation of multiple routes instate on one physical device
2. Allows users to simultaneously manage multiple routing tables
3. Can be used for MP BGP and MPLS deployments
4. Multiple VPNs for customers can use overlapping IP addresses without conflict
5. Users may segment network paths without multiple routers, improving network functionality

To configure and verify VRF, you can use the following commands:

To create a new VRF instance:

ip vrf <vrf-name>

To assign an interface to a specific VRF:

interface <interface-name> ip vrf forwarding <vrf-name>

To verify VRF configuration:

show ip vrf