What is a Virtual Machine?

A **virtual machine**, known as a guest, is created within a computing environment, called a host. Multiple virtual machines can exist in one host at one time. Key files that make up a virtual machine include a log file, NVRAM setting file, virtual disk file, and configuration file.

Virtual Machine Definition

Virtual machines are software computers that provide the same functionality as physical computers. Like physical computers, they run applications and an operating system. However, virtual machines are computer files that run on a physical computer and behave like a physical computer. In other words, virtual machines behave as separate computer systems.

Why Virtual Machines?

Virtual machines are created to perform specific tasks that are risky to perform in a host environment, such as accessing virus-infected data and testing operating systems. Since the virtual machine is sandboxed from the rest of the system, the software inside the virtual machine cannot tamper with the host computer. Virtual machines can also be used for other purposes such as server virtualization.

Advantages of Virtual Machines:

- Provides disaster recovery and application provisioning options
- Virtual machines are simply managed, maintained, and are widely available
- Multiple operating system environments can be run on a single physical computer

Disadvantages of Virtual Machines:

- Running multiple virtual machines on one physical machine can cause unstable performance
- Virtual machines are less efficient and run slower than a physical computer

The Four Types of Virtual Machines:

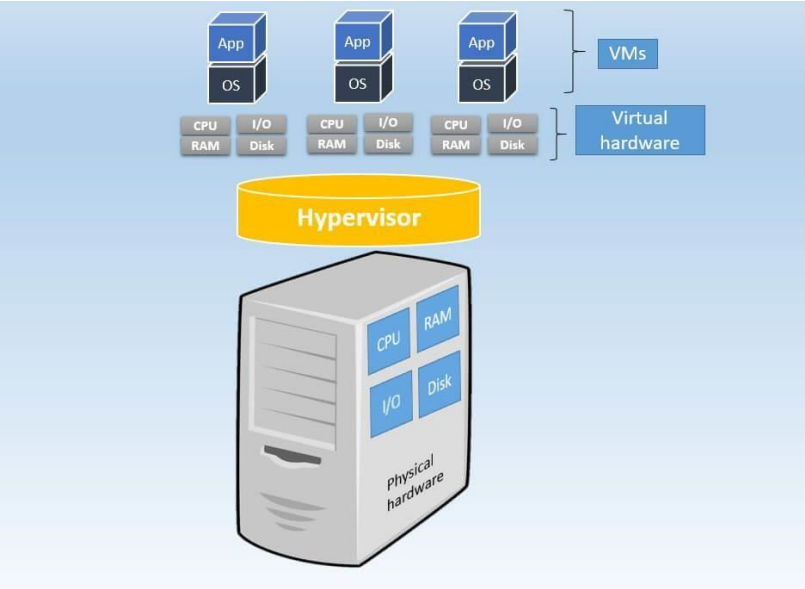
1. **Process virtual machines**: Execute computer programs in a platform-independent environment. It masks the information of the underlying hardware or operating system. This allows the program to be executed in the same fashion on any platform.

2. **System virtual machines**: Support the sharing of a host computer's physical resources between multiple virtual machines.

3. **Hosted virtual machines:** Hosted Virtual Machines are built on top of an existing operating system called the host.
   The virtualization layer sits above the regular operating system and makes the virtual machine look like an application process.

We then install complete operating systems called guest operating systems within the host virtual machines.
The VM can provide the same instruction set architecture as the host platform or it may also support a completely different Instruction Set Architecture (ISA).
VMware GSX Server is an example where the host ISA and guest ISA are same.
Isolation in hosted virtual machines is as good as the isolation provided by the hypervisor approach except that the virtual machine monitor in the case of the hosted VM does not run at the highest privilege.
The processes running inside the virtual machine cannot affect the operation of processes outside the virtual machine.

4. **Hardware Virtual Machine:** Hardware virtual machines are virtual machines built using virtualization primitives provided by the hardware like processor or I/O.
The advantage of hardware level virtualization is tremendous performance improvements over the software based approaches and guarantees better isolation between machines.
The isolation provided by the hardware assisted virtualization is more secure than that provided by its software counterpart for obvious reasons.



What does *Virtual Machine Monitor (VMM)* mean?

A Virtual Machine Monitor (VMM) is a software program that enables the creation, management and governance of virtual machines (VM) and manages the operation of a virtualized environment on top of a physical host machine.

VMM is also known as Virtual Machine Manager and Hypervisor. However, the provided architectural implementation and services differ by vendor product.

VMM is the primary software behind virtualization environments and implementations. When installed over a host machine, VMM facilitates the creation of VMs, each with separate operating systems (OS) and applications. VMM manages the backend operation of these VMs by allocating the necessary computing, memory, storage and other input/output (I/O) resources.

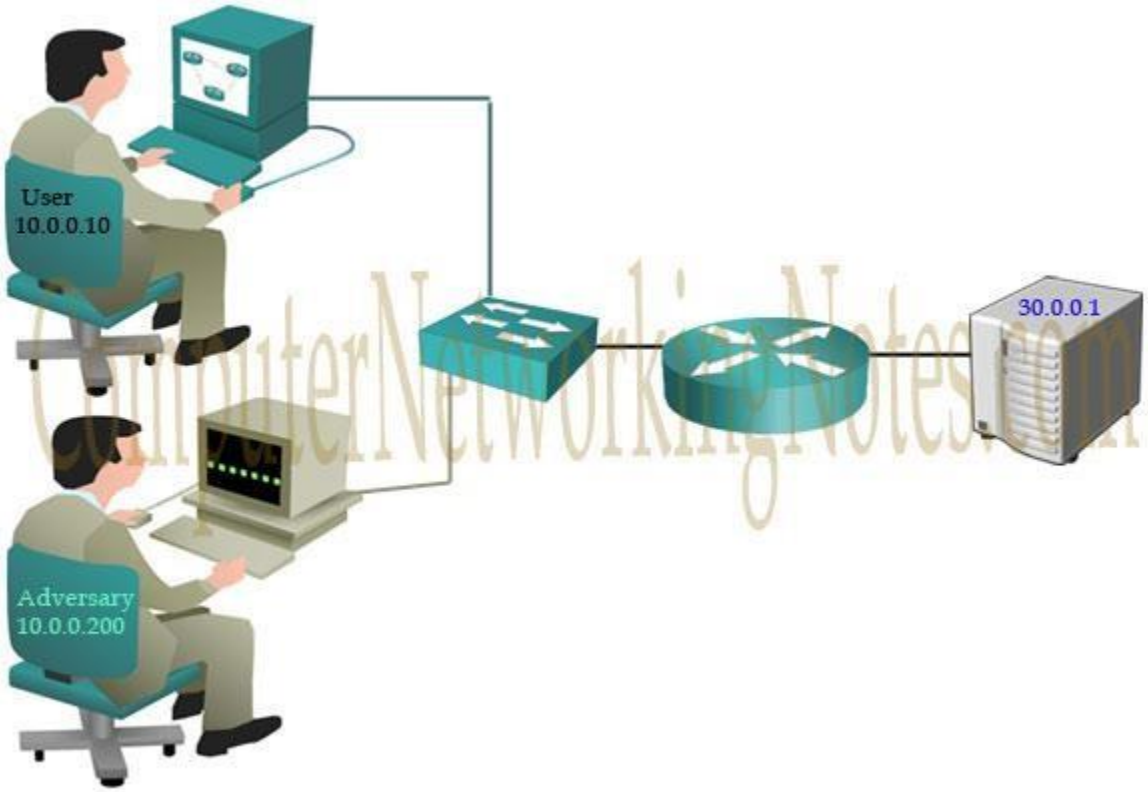
VMM also provides a centralized interface for managing the entire operation, status and availability of VMs that are installed over a single host or spread across different and interconnected hosts.

What is Access Control List (ACL)?

Basically ACL is the integrated feature of IOS software that is used to filter the network traffic passing through the IOS devices. Network traffic flows in the form of packets. A packet contains small piece of data and all necessary information which are required to deliver it. By default when a router receives a packet in interface, it takes following actions:-

- Grab destination address from the packet
- Find an entry for destination address in routing table
- If match found, forwards the packet from associate interface
- If no match found, discard the packet immediately.

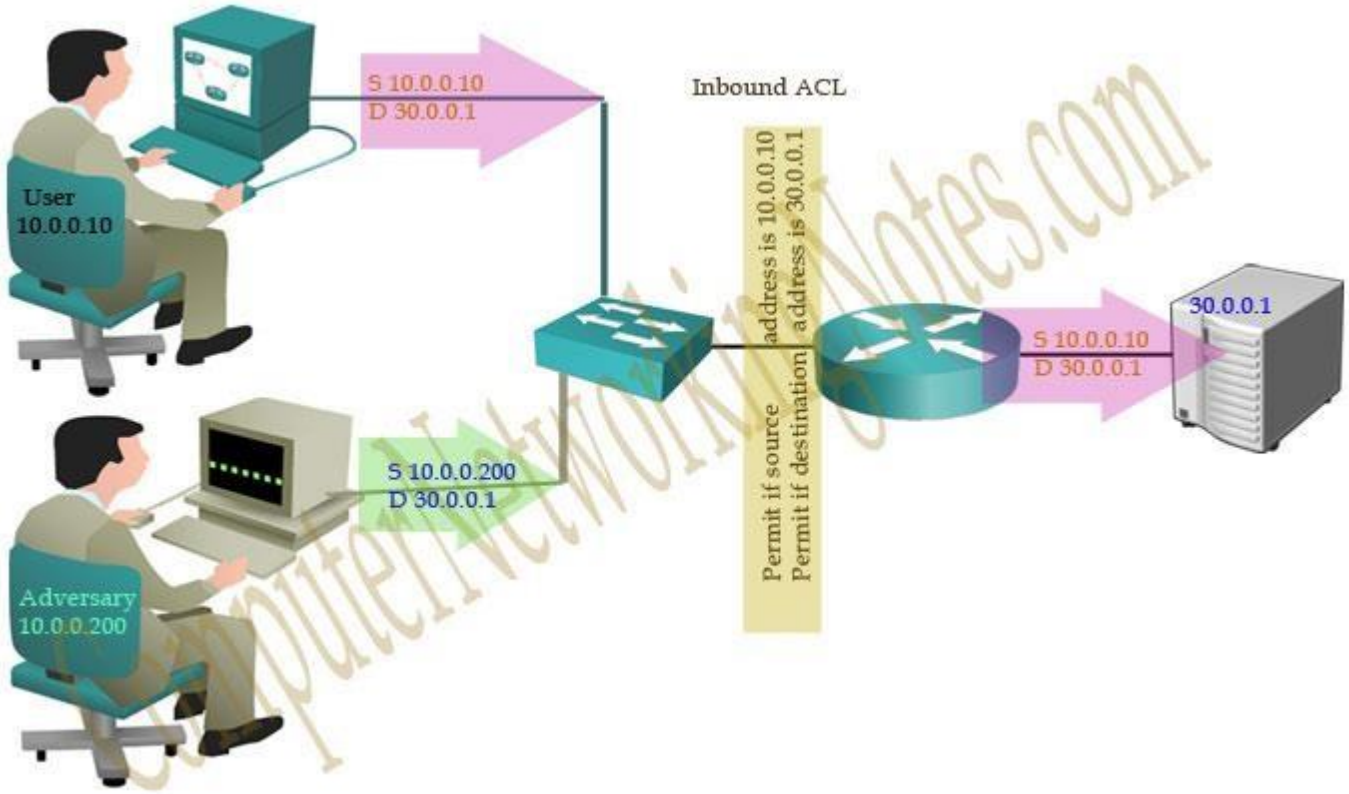
This default behavior does not provide any security. Anyone who know the correct destination address can send his packet through the router. For example following figure illustrates a simple network.



In this network, no security policy is applied on router. So router will not be able to distinguish between user's packet and adversary's packet. From router's point of view, both packets have correct destination address so they should be forwarded from exit interface.

Suppose we tell the router that only 10.0.0.10 has the right to access the 30.0.0.1. To match with this condition router will take following actions:-

- Grab source and destination address from the packet
- Match both addresses with given condition
- If packet is not arrived from 10.0.0.10, drop the packet immediately.
- If packet is not intended from 30.0.0.1, drop the packet immediately.
- If both condition match find an entry for destination address in routing table
- If match found, forwards the packet from associate interface
- If no match found, discard the packet immediately.



Now only the packets from 10.0.0.10 are allowed to pass from router. With this condition adversary will not be able to access the server. We can create as much conditions as we want. Technically these conditions are known as ACLs. Besides filtering unwanted traffic, ACLs are used for several other purposes such as prioritizing traffic for QoS (Quality of Services), triggering alert, restricting remote access, debugging, VPN and much more. Due to complexity, these uses of ACLs are not tested in CCNA level exams. CCNA level exams test only basic uses of ACLs such as filtering the traffic and blocking specific hosts.

Access Control Technology Overviews

The list of best access control technologies contains the technologies that are mostly used for communication between different components

of the access control system (ACS). So, let's have short access control technology overviews:

- **Near Field Communication (NFC):** Two NFC enabled devices establish a communication medium through an air interface by developing electromagnetic induction field between the two when they are brought near to each other. These access control devices work at 13.56 MHz frequency within the range of 1.6 inches.
- **Internet of Things (IoT):** This is IP based communication between all components of access control technologies, which are IP enabled intelligent devices. They use the internet to establish communication between them.
- **Radio Frequency Identification (RFID):** In this technology credential information is stored on a tag that is attached to a carrier. When come in proximity to the reader device, electromagnetic waves are generated and captured to read the information and allow/deny access.
- **Physical Access Control System (PACS):** This is based on personal information card verification (PIV) card and card reader. This technology is used for government and security related areas. It involves two step authentication process.
- **Power over Ethernet (PoE):** This technology uses cables that carry both data signals and power to supply the access control components like IP cameras, telephones, access controller, routers, access points and other elements. This is very cost effective access control technology.
- **Mobile Access Control:** The mobile devices are converted into electronic key fobs by installing application on it, which uses wireless technology for communication. The mobile device can also be used to manage and control the entire access control system of a particular area or building.
- **Bluetooth Access control:** This uses the power of Bluetooth enabled devices. The data transferred between two devices through frequency hopping spectrum spread radio interface, which operates in ISM band of frequency. It is effective up to 800 feet distance and 50Mbit/sec data rate.
- **Wired Access Control Technologies:** These include CAT6 cable communication, PoE access and traditional wiring solutions. The communication between different components may take place through different communication protocols.

- **Wireless Access Control Technologies:** This is a generalized category of wireless technologies used in the access control system. Bluetooth, NFC, RFID, mobile and others fall in this category of access control technologies.

The access control technology overview of individual categories can be further expanded in terms of features and capabilities to integrate different backend technologies and software applications.

Important Access Control Technology Terms

Access control technology has evolved from a very basic technique to the latest software controlled intelligent access control technology, as shown above in the access control technology overview section. There are many terms that are very necessary to know about for better understanding of the concepts of modern access control technologies. A few very important terms are explained below.

- **Access Credentials:** This is the valid password, biometric pattern or PIN code or other data used to access the system provided by the access control system administrator to the users.
- **Authentication:** Authentication is a process to verify the access credential provided by users. In this process the input credentials are compared with the original data created on the system and verified or rejected.
- **Authorization:** Authorization is the authority to a user provided by the administrator to access any particular area or assets.
- **Access Control List (ACL):** It is a list of IPs or any other intelligent device addresses in the access control systems that the users are allowed to access in a particular condition specified in the authority.
- **Access Control Topologies:** Access control topologies are the schemes or designs to connect and configure a particular access control system. There are different types of access control topologies that are used in the modern ACS systems. For example, Standalone, integrated, serial controllers, serial controllers & intelligent readers, serially connected main & sub-controllers, network enabled controllers, IoT based controllers and others.

- **Access Control Models:** The access control models are the software level management schemes to assign the access authority for a particular user. For example, the organization based control model allows the third party organization team members for a certain time, area and assets to access for contract work. Similarly, in authority level model, a CEO is assigned to access any part of the office building. There are many access control models commonly used in ACS system, such as Identity based access control, role based access control, mandatory access control, attribute based access control and many others.
- **Access Control Technology Components:** All devices and products used in an access control system are referred as access control components.

Access Control Technology Parts & Their Roles

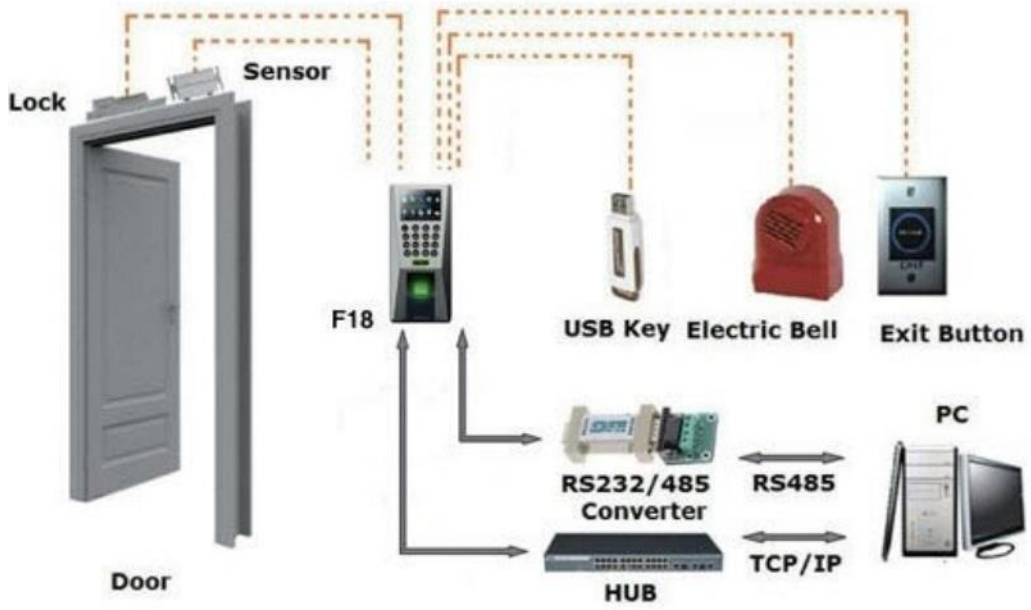


Figure: Parts of access control system

- **Electric Locks:** The most fundamental item in the access control technology components is electric lock. The lock is the device that physically prohibits the intruders from entering into the area or accessing the assets. Numerous types of locks are used in access control systems for example, mechanical locks, electromechanical locks, electric locks and digital locks.
- **Card Readers:** Card reader is another basic component of ACS system. It is used to read HID cards, key fobs, mobile apps, magnetic information and others. There are many types of card readers based on the modern technologies such as wireless, magnetic, Bluetooth and NFC card readers.

- **Access Control Keypads:** It is similar to card reader, but uses a keypad to input the password, PIN or access number. Access keypads are available in both the hard keys and digital key formats.
- **Access Controllers/Field panels:** These components are the core of the entire system. Access controllers can integrate multiple readers on the downstream side and connect to the main software platform. This is the brain of the entire access control system.
- **Access Cards/Key Fobs:** Access cards are available in different formats that carry information in the form of magnetic or digital data. Many companies offer dedicated key fobs to access the control system. The most common example is the HID card.
- **Communication Media:** This is one of the most important access control technology components. What type of technology is used in the ACS system is commonly known due to the communication media implemented in the system. Wireless, Bluetooth, NFC, RFID, IoT, Cat6, serial R-232/485 and other are the examples of communication media of access control technology; and they are referred as access control technologies too.
- **Access Control Server:** It is a computer that runs the access control management software to configure and modify the data in all access control components.