LESSON 1

System Administrator – is an IT expert who manages an organization's network.

Knowledge areas required of a Sys. Admin:

- Operating systems
- Application software
- Software troubleshooting
- Network management
- Hardware

System Admin related jobs

- Database Administrator
- Network Administrator
- Security Administrator

Training and Certification

- Microsoft Certified Professional (MCP)
- Red Hat Certification Programs (RHCP)
- Cisco Certified Network Associate (CCNA)
- Sun Certified Network Administrator (SCNA)
- A+ (CompTIA)
- N+ (CompTIA)

Windows Server – is a line of operating systems that Microsoft specifically creates for use on a server.

Servers – are extremely powerful machines that are designed to run constantly and provide resources for other computers.

Active Directory – user management service that allows a server to act as a domain controller.

Dynamic Host Configuration Protocol (DHCP) – protocol that lets a server automatically assign IP addresses to all devices on the network.

File and Storage – Having a file server for your company is another common use. This allows you to keep important data in a central location and set permissions to control who can access which files.

Print Service – Setting up a print server allows you to easily map printers to computers and reduce redundant work.

Windows Update Services – you can route all workstation updates through that server and configure specific rules for how they should work.

Linux server is a variant of the Linux operating system that is designed to handle more intense storage and operational needs of larger organizations and their software.

LESSON 2

RAID (Redundant Array of Independent Disks) - is a data storage virtualization technology that combines multiple physical disk drive components into one or more logical units for the purposes of data redundancy, performance improvement, or both.

RAID 0 – Striping system data are split up into blocks that get written across all the drives in the array.

RAID 1 – Mirroring Data are stored twice by writing them to both the data drive (or set of data drives) and a mirror drive (or set of drives).

RAID 5 – Striping with parity The most common secure RAID level. It requires at least 3 drives but can work with up to 16. Data blocks are striped across the drives and on one drive a parity checksum of all the block data is written.

RAID 6 – Stripping with double parity good all-round system that combines efficient storage with excellent security and decent performance.

RAID level 10 – combining RAID 1 & RAID 0
This is a nested or hybrid RAID configuration.

RAID levels 2, 3, 4 and 7 – These levels do exist but are not that common (RAID 4 is essentially like RAID 5 but with the parity data always written to the same drive).

Types of RAID

Hardware-based

- Hardware RAID setup, the drives connect to a special RAID controller inserted in a fast PCI-Express (PCI-e) slot in a motherboard.
- Hardware RAID controllers can be configured through card BIOS before an operating system is booted, and after the operating system is booted, proprietary configuration utilities are available from the manufacturer of each controller.

Software-based

- When storage drives are connected directly to the motherboard without a RAID controller, RAID configuration is managed by utility software in the operating system, and thus referred to as a software RAID setup.
- Software RAID implementations are provided by many modern operating systems.

LESSON 3

DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

History

- DHCP was created by the Dynamic Host Configuration Working Group of the Internet Engineering Task Force.
- October 1993: RFC 1531 initially defined DHCP as a standard-track protocol succeeding the Bootstrap Protocol (BOOTP), which is a network protocol used by a network client to obtain an IP address from a configuration server.

- October 1997: RFC 2131 released is the current DHCP definition for Internet Protocol version 4 (IPv4) networks.
- The extensions of DHCP for IPv6 (DHCPv6) were published as RFC 3315.

What is DHCP?

- Dynamic Host Configuration Protocol.
- It is a method for assigning Internet Protocol (IP) addresses permanently or to individual computers in an organization's network.
- DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

Motivation for DHCP

Configuration parameters for network hosts:

- IP address
- Router
- Subnet Mask
- Others..

Two types of IP Addresses

DHCP is used to assign IP addresses to hosts or workstations on the network.

Two types of IP addresses:

Static

- Is a number that is assigned to a computer by an Internet service provider (ISP) to be its permanent address on the Internet.

Dynamic

- The temporary IP address is called a dynamic IP address.

Why is DHCP Important?

Important when it comes to adding a machine to a network.

When a computer requests an address, the administrator would have to manually configure the machine.

- Mistakes are easily made.
- Causes difficulty for both administrator as well as neighbors on the network.

DHCP solves all the hassle of manually adding a machine to a network.

How does DHCP work?

When a client needs to start up TCP/IP operations, it broadcasts a request for address information.

The DHCP server will not reallocate the address during the lease period and will attempt to return the same address every time the client requests an address.

LESSON 4

Virtualization

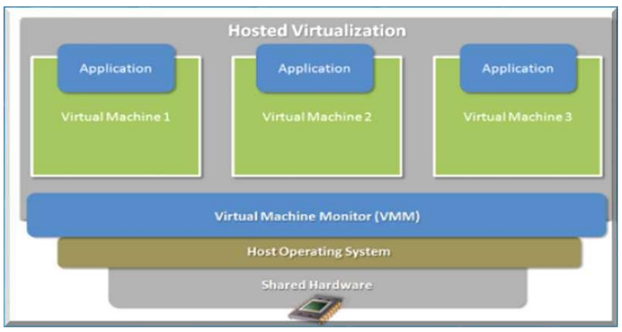
Virtualization is the simulation of the software and/or hardware upon which other software runs. This simulated environment is called virtual machine. Each VM can run its own operating systems and applications as if it were in a physical machine. So, It is a way to run multiple operating systems on the same hardware at the same time.

- For e.g., Windows and Linux both can run on the same laptop at the same time.

Virtualization Architecture

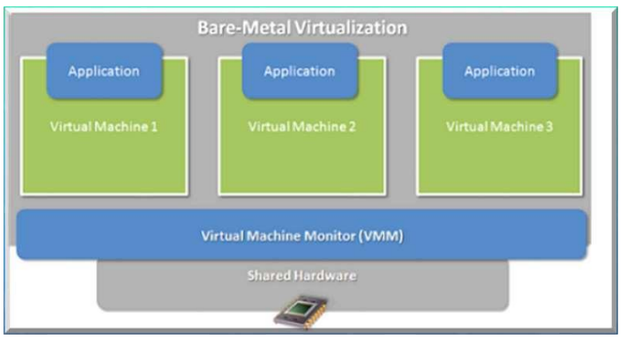
- Hosted Architecture.
- Bare-Metal Architecture.

Hosted Architecture



Hosted Virtual Machine Monitor is installed on top of host OS

Bare-Metal Architecture



Bare-metal virtual machine monitor is installed directly on system hardware

Types of Virtualization

- Desktop Virtualization
- Server Virtualization
- Network Virtualization
- Storage Virtualization
- Application Virtualization

Vendors of Virtualization

vmware

Microsoft CITRIX

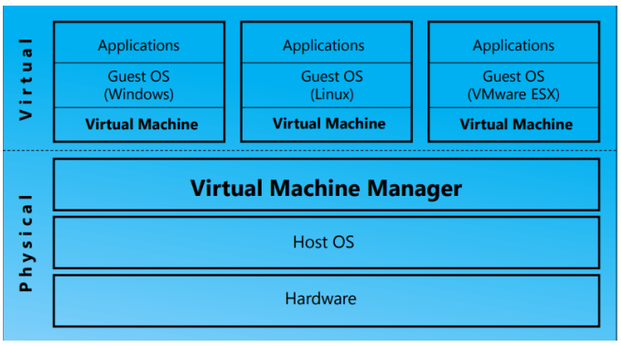
Benefits from Virtualization

- Save money and energy
- Simplify management

Desktop Virtualization

- VMware Workstation (Local)
- Microsoft Virtual PC (Local)
- Citrix XenDesktop (Centralized)

Desktop Virtualization Architecture



Components of Virtual Machines

- Configuration file
- Hard disk file(s)
- Virtual machine state file
- In-memory file

Comparison

VMware Workstation

- Costs more
- More host & guests support
- Better features (Snapshots, USB)
- 64-bit hosts and guests

Microsoft Virtual PC

- Free
- Less hosts & guests support
- Less VM features and capabilities

Uses

- Development
- Testing
- Training

Server Virtualization

- Software (SoftV)
- Hardware (HardV)

SoftV Server Virtualization

- VMware Server

HardV Server Virtualization

- Microsoft Virtual Server
- Citrix XenServer
- VMware ESX Server
- Microsoft Hyper-V Server
- VMware ESXi Server

Common Virtualization Uses Today

Reduce costs by consolidating services onto the fewest number of physical machines

Test and Development – Rapidly provision test and development servers; store libraries of pre-configured test machines.

Business Continuity – Reduce cost and complexity by encapsulating entire systems into single files that can be replicated and restored onto any target server.

Enterprise Desktop – Secure unmanaged PCs without compromising end-user autonomy by layering a security policy in software around desktop virtual machines.

LESSON 5

Basic Configuration Commands

Command	Purpose
enable	Logs you into enable mode, which is also known as user exec mode or privileged mode
configure terminal	Logs you into configuration mode
interface *fastethernet/number*	Enters interface configuration mode for the specified fast ethernet interface
reload	An exec mode command that reboots a Cisco switch or router
hostname *name*	Sets a host name to the current Cisco network device
copy *from-location to-location*	An enable mode command that copies files from one file location to another
copy running-config startup-config	An enable mode command that saves the active config, replacing the startup config when a Cisco network device initializes
copy startup-config running-config	An enable mode command that merges the startup config with the currently active config in RAM
write erase **erase startup-config**	An enable mode command that deletes the startup config
ip address *ip-address mask*	Assigns an IP address and a subnet mask
shutdown **no shutdown**	Used in interface configuration mode. "Shutdown" shuts down the interface, while "no shutdown" brings up the interface.
ip default-gateway *ip_address*	Sets the default gateway on a Cisco device
show running-config	An enable mode command that displays the current configuration
description *name-string*	A config interface command to describe or name an interface
show running-config interface *interface slot/number*	An enable mode command to display the running configuration for a specific interface
show ip interface *[type number]*	Displays the usability status of interfaces that are configured for IP
ip name-server *serverip-1 serverip-2*	A configure mode command that sets the IP addresses of DNS servers

Troubleshooting Commands

ping *{hostname | system-address} [source source-address]*	Used in enable mode to diagnose basic network connectivity
speed *{10 | 100 | 1000 | auto}*	An interface mode command that manually sets the speed to the specified value or negotiates it automatically
duplex *{auto | full | half}*	An interface mode command that manually sets duplex to half, full or auto
cdp run **no cdp run**	A configuration mode command that enables or disables Cisco Discovery Protocol (CDP) for the device
show mac address-table	Displays the MAC address table

show cdp	Shows whether CDP is enabled globally
show cdp neighbors*[detail]*	Lists summary information about each neighbor connected to this device; the "detail" option lists detailed information about each neighbor
show interfaces	Displays detailed information about interface status, settings and counters
show interface status	Displays the interface line status
show interfaces switchport	Displays a large variety of configuration settings and current operational status, including VLAN trunking details.
show interfaces trunk	Lists information about the currently operational trunks and the VLANs supported by those trunks
show vlan **show vlan brief**	Lists each VLAN and all interfaces assigned to that VLAN but does not include trunks
show vtp status	Lists the current VTP status, including the current mode

Routing and VLAN Commands

ip route*network-number network-mask {ip-address | interface}*	Sets a static route in the IP routing table
router rip	Enables a Routing Information Protocol (RIP) routing process, which places you in router configuration mode
network *ip-address*	In router configuration mode, associates a network with a RIP routing process
version 2	In router configuration mode, configures the software to receive and send only RIP version 2 packets
no auto-summary	In router configuration mode, disables automatic summarization
default-information originate	In router configuration mode, generates a default route into RIP
passive-interface *interface*	In router configuration mode, sets only that interface to passive RIP mode. In passive RIP mode, RIP routing updates are accepted by, but not sent out of, the specified interface.
show ip rip database	Displays the contents of the RIP routing database
ip nat *[inside | outside]*	An interface configuration mode command to designate that traffic originating from or destined for the interface is subject to NAT
ip nat inside source *{list{access-list-number | access-list-name}} interface type number[overload]*	A configuration mode command to establish dynamic source translation. Use of the "list" keyword enables you to use an ACL to identify the traffic that will be subject to NAT. The "overload" option enables the router to use one global address for many local addresses.
ip nat inside source static *local-ip global-ip*	A configuration mode command to establish a static translation between an inside local address and an inside global address
vlan	Creates a VLAN and enters VLAN configuration mode for further definitions
switchport access vlan	Sets the VLAN that the interface belongs to.
switchport trunk encapsulation dot1q	Specifies 802.1Q encapsulation on the trunk link.
switchport access	Assigns this port to a VLAN
vlan vlan-id *[name vlan-name]*	Configures a specific VLAN name (1 to 32 characters)
switchport mode *{ access | trunk }*	Configures the VLAN membership mode of a port. The access port is set to access unconditionally and operates as a non-trunking, single VLAN interface that sends and receives non-encapsulated (non-tagged) frames. An access port can be assigned to only one VLAN. The trunk port sends and receives encapsulated (tagged) frames that identify the VLAN of origination. A trunk is a point-to-point link between two switches or between a switch and a router.
switchport trunk *{encapsulation { dot1q }*	Sets the trunk characteristics when the interface is in trunking mode. In this mode, the switch supports simultaneous tagged and untagged traffic on a port.
encapsulation dot1q vlan-id	A configuration mode command that defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance

DHCP Commands

ip address dhcp	A configuration mode command to acquire an IP address on an interface via DHCP
ip dhcp pool name	A configuration mode command to configure a DHCP address pool on a DHCP server and enter DHCP pool configuration mode
domain-name *domain*	Used in DHCP pool configuration mode to specify the domain name for a DHCP client
network *network-number [mask]*	Used in DHCP pool configuration mode to configure the network number and mask for a DHCP address pool primary or secondary subnet on a Cisco IOS DHCP server
ip dhcp excluded-address *ip-address [last-ip-address]*	A configuration mode command to specify IP addresses that a DHCP server should not assign to DHCP clients
ip helper-address *address*	An interface configuration mode command to enable forwarding of UDP broadcasts, including BOOTP, received on an interface
default-router *address[address2 ... address8]*	Used in DHCP pool configuration mode to specify the default router list for a DHCP client

Security Commands

password*pass-value*	Lists the password that is required if the login command (with no other parameters) is configured
username *name* **password** *pass-value*	A global command that defines one of possibly multiple user names and associated passwords used for user authentication. It is used when the login local line configuration command has been used.
enable password *pass-value*	A configuration mode command that defines the password required when using the **enable** command
enable secret*pass-value*	A configuration mode command that sets this Cisco device password that is required for any user to enter enable mode
service password-encryption	A configuration mode command that directs the Cisco IOS software to encrypt the passwords, CHAP secrets, and similar data saved in its configuration file
ip domain-name *name*	Configures a DNS domain name
crypto key generate rsa	A configuration mode command that creates and stores (in a hidden location in flash memory) the keys that are required by SSH
transport input *{telnet | ssh}*	Used in vty line configuration mode, defines whether Telnet or SSH access is allowed into this switch. Both values can be specified in a single command to allow both Telnet and SSH access (default settings).
access-list *access-list-number {deny | permit} source [source-wildcard] [log]*	A configuration mode command that defines a standard IP access list
access-class	Restricts incoming and outgoing connections between a particular vty (into a basic Cisco device) and the addresses in an access list
ip access-list *{standard | extended} {access-list-name | access-list-number}*	A configuration mode command that defines an IP access list by name or number
permit source *[source-wildcard]*	Used in ACL configuration mode to set conditions to allow a packet to pass a named IP ACL. To remove a permit condition from an ACL, use the "no" form of this command.
deny source *[source-wildcard]*	Used in ACL configuration mode to set conditions in a named IP ACL that will deny packets. To remove a deny condition from an ACL, use the "no" form of this command.
ntp peer *<ip-address>*	Used in global configuration mode to configure the software clock to synchronize a peer or to be synchronized by a peer
switchport port-security	Used in interface configuration mode to enable port security on the interface
switchport port-security maximum maximum	Used in interface configuration mode to set the maximum number of secure MAC addresses on the port
switchport port-security mac-address *{mac-addr | {sticky [mac-addr]}}*	Used in interface configuration mode to add a MAC address to the list of secure MAC addresses. The "sticky" option configures the MAC addresses as sticky on the interface.
switchport port-security violation *{shutdown | restrict | protect}*	Used in interface configuration mode to set the action to be taken when a security violation is detected
show port security *[interface interface-id]*	Displays information about security options configured on the interface

Monitoring and Logging Commands

logging *ip address*	Configures the IP address of the host that will receive the system logging (syslog) messages
logging trap level	Used in configuration mode to limit messages that are logged to the syslog servers based on severity. Specify the number or name of the desired severity level at which messages should be logged.
show logging	Enable mode command that displays the state of system logging (syslog) and the contents of the standard system logging buffer.
terminal monitor	An enable mode command that tells Cisco IOS to send a copy of all syslog messages, including debug messages, to the Telnet or SSH user who issues this command