Nitesh Tuladhar
CSIT 4124

Question no. 1 (a)

ans:- In computer networks, reference models give a conceptual framework that standardizes communication between the heterogeneous networks.

The two popular reference models are
- OSI Model
- TCP/IP Model

OSI Reference Model

The Open Systems Interconnection (OSI) is a standard reference model for communication between two end users in a network. The model is used in developing products and understanding networks.

OSI model are divided into seven layer. Where the upper four layers are used whenever a message passes from or to a user, and the lower three layers are used when any message passes through the host computer.

Application	→ (SMTP, FTP, Telnet)
Presentation	→ (Format Data, Encryption)
Session	→ (Start & stop sessions)
Transport	→ (TCP, UDP, Port Numbers)
Network	→ (IP Address, Switches)
Data link	→ (MAC Address, Switches)
Physical	→ (Cable, Hubs, NIC.)

Fig: OSI Reference Model.

The application Layer :

This is the layer where communication partners are identified, quality of service is identified user authentication and privacy is concideved, and any constraints on data syntax are identified.

The presentation Layer :

This is the layer which is the part of the operating system, that converts incoming and outgoing data from one presentation format to another

The session Layer :

This layer sets up, coordinates, and teminates conversations, exchanges dialogs between applications at each end.

The Transport layer :

This layer manages end-to-end control and error checking. It also ensures complete data transfer

The network Layer

The network layer handles the routing of data i.e. sending it in the ~~write direction right direction~~ right destination.

The data-link layer :

This layer provides synchronization for the physical level and does bit-stuffing.

The physical Layer.

This layer conveys the bit stream through the network at electrical and mechanical level.

TCP/IP Reference Model

Application Layer
Transport Layer
Network Layer
Network interface Layer.

TCP/IP reference model is based on suite of protocols in which each protocol solves a particular network communication problem. There are four layers on the TCP/IP model

The Network Layer

The Network Layer is responsible for exchanging data between a host and the network. IP datagrams are encapsulated to frames and mapping of IP addresses into physical address is done.

Internet Layer

The Internet layer is responsible for sending source packets from any network on the internetwork.

Transport Layer.

This layer is responsible for reliability, flow control and error correction of the data being transmitted

Application Layer

This layer is responsible for handling high-level protocols, encoding and dialog control.

Question no. 1(b)

Ans: Network Routing is a ~~proto~~ process of selecting a path across one or more network. The principles of routing can apply to any type of network, from telephone network to public transportation.

In packet-switching network, such as the internet, routing selects the path for Internet Protocol (IP) packets to travel from their origin to the destination. These internet routing decision are made by specialized pieces of ~~net~~ network hardwares called routers.

When a packet is introduced in the network and received by one of the routers, it

reads the header of the packet to understand the destination and checks its routing table marked with its metrics to see what would be the next best nopes for the packet to optimally reach the destination. Then it pushes the packet to the next node and the above process repeats at the new node too until the packets reaches the destination.

There some of the applications of routing are:

Unicast:

Unicast messaging is used for all network processes in which a private or unique resource is requested.

This method is used mostly on the Internet and restricts an IP address to be associated to only one particular node in a network which is known as one-to-one association

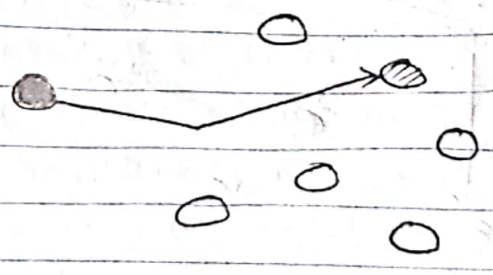
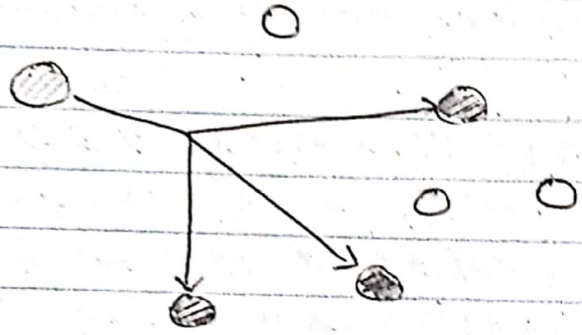


Fig: Unicast

2. Multicast :

Multicast allows for request from a sender to be routed to various selected end points simultaneously, and uses one-to many-of-many or many-to-many-of many association.



Multicast.

3. Broadcast :

Broadcasting can be performed as a high level operation in a program and refers to transmitting a packet that will be received by every device on the network

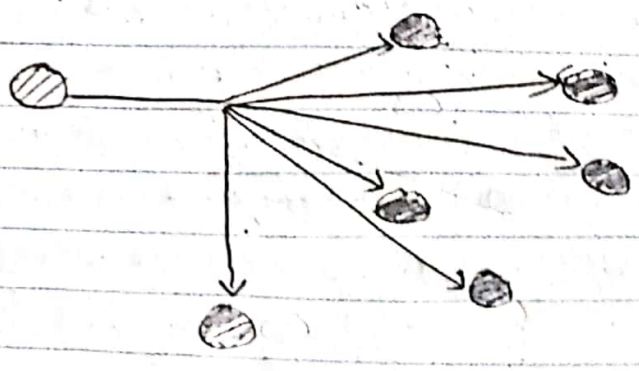


Fig: Broadcast.

4. Anycast :

Anycast, also known as IP Anycast is a networking technique that allows for multiple machines to share the same IP address. Based on the location of the user request, the router sends it to the machine in the network that is near.

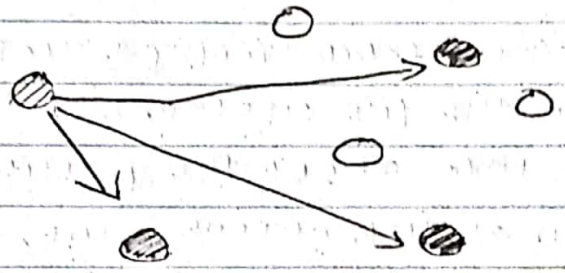


Fig : Anycast

Question no. 2(a) .

Ans:- A disk quota is a limit set by a system administrator that restricts certain aspects of the file system usage on modern operating systems. The function of using disk quotas is to allocate limited disk space in a resonable way. Disk quotas are typically implemented on a per-user or per-group basic. That is, a system administrator defines a usage or file quota specific to a certain user or group.

There are basically two types of disk quotas

The first known as a usage quota or block quota, limits the amount of disk space that can be used. The second known as a file quota or inode quota limits the number of files and directories that can be created.

Disk quota can be configured in four steps:

a) Enable quota:

Linux uses /etc/fstab configuration file to mount all partitions in the file system at boot time. The file contains ~~all~~ info about the partition such as partition location at disk, mount point, attributes and other control options. Each entry in this file has six-fields x what to mount, where to mount, file system, options dump support, automatic check.

In order to enable user quota, we have to add usrquota option in fourth field. To enable group quota add grpquota option to the forth field.

b) Remounting file system:

If partition is not used by any process, we can remount it with following command.

mount -o remount [partition]

If patition is remounted without any error use mount/grep [partition] command.

c) Creating quota files:

Run the following command on third step

quotacheck -cug [partition where quota is enabled]

This command will create necessary files for quota.

d) Configuring quota policies:

To configure quota policies, we have to define three values soft limit, hard limit & grace period.

Soft limit: flexible limits where user or group is allowed to cross the limit temporarily.

Hard limit: Fixed limit where user or group is not allowed to cross the limit

Grace period: It is a time period while user or group is allowed to use additional space.

Question no. 2(b)

Ans: The following are the 6-high level stages of a typical Linux boot process

BIOS — Basic Input/output system executes MBR.

MBR — Master Boot Record executes GRUB

GRUB — Grand Unified Bootloader executes kernel.

Kernel	kernel executes /sbin/init
Init	Init executes runlevel programs
Runlevel	Runlevel programs are executed from /etc/rc.d/rc*.d/.

a) BIOS:
- Stands for Basic Input/output system.
- Performs some integrity checks
- loads and executes the MBR boot loader

b) MBR
- Stands for Master Boot Record.
- located at /dev/hda or /dev/sda.
- Size is less than 512 bytes and contains information about GRUB.
- It loads and executes the GRUB boot loader.

c) GRUB:
- Stands for Grand Unified Bootloader.
- configuration file of GRUB is /boot/grub/grub.conf
- It has knowledge of the file system and loads and executes kernel and initrd images.

d) Kernel.
- Mounts the root file system as specified in the "root=" in grub.conf.

- Executes the /sbin/init program

Init
- Looks at /etc/initlab file to decide the Linux run level.
- Identifies the default initlevel and uses that to load all appropriate programs.

Runlevel program.
- Runlevel Program are executed from the run level directory

Question no. 3(a)

Ans:- DHCP (Dynamic Host Configuration Protocol) is a network protocol used to assign various network parameters to a device.

Linux can be used as both DHCP client & server. The dhcp package contains an ISC DHCP server. First, install the package as the superuser.

```
# yum install dhcp
($ sudo apt-get update)
($ sudo apt-get install isc-dhcp-server)
```

Installing the dhcp packages creates a file /etc/dhcp/dhcpd.conf, which is merely an empty

configuration file :

$cat /etc/dhcp/dhcpd.conf

Configuring DHCP server

DHCP configuration file is located at /etc/dhcp/dhcpd.conf. We can open this file by running the following command in terminal.

$sudo nano /etc/dhcp/dhcpd.conf.

Defining the subnet :

To define subnet add following lines to configuration file.

subnet 192.168.110.0 netmask 255.255.255.0{

}

To specify the range of leased address add.

range 192.168.110.5 192.168.110.10;

To specify default gateway, add.

option routers 192.168.110.1;

To specify the domain name servers

option domain-name-servers 8.8.8.8, 8.8.4.4;

To make DHCP server the official DHCP server for clients.

$ authoritative.

Manage DHCP services

To verify if DHCP service is running,

$sudo systemctl status isc-dhcp-server.service

To start DHCP service,

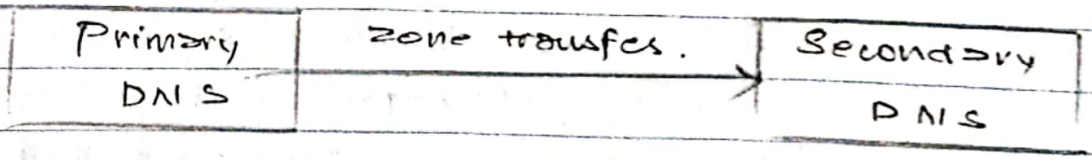
$sudo systemctl start isc-dhcp-server.service

To stop DHCP service

$sudo systemctl stop isc-dhcp-server.service

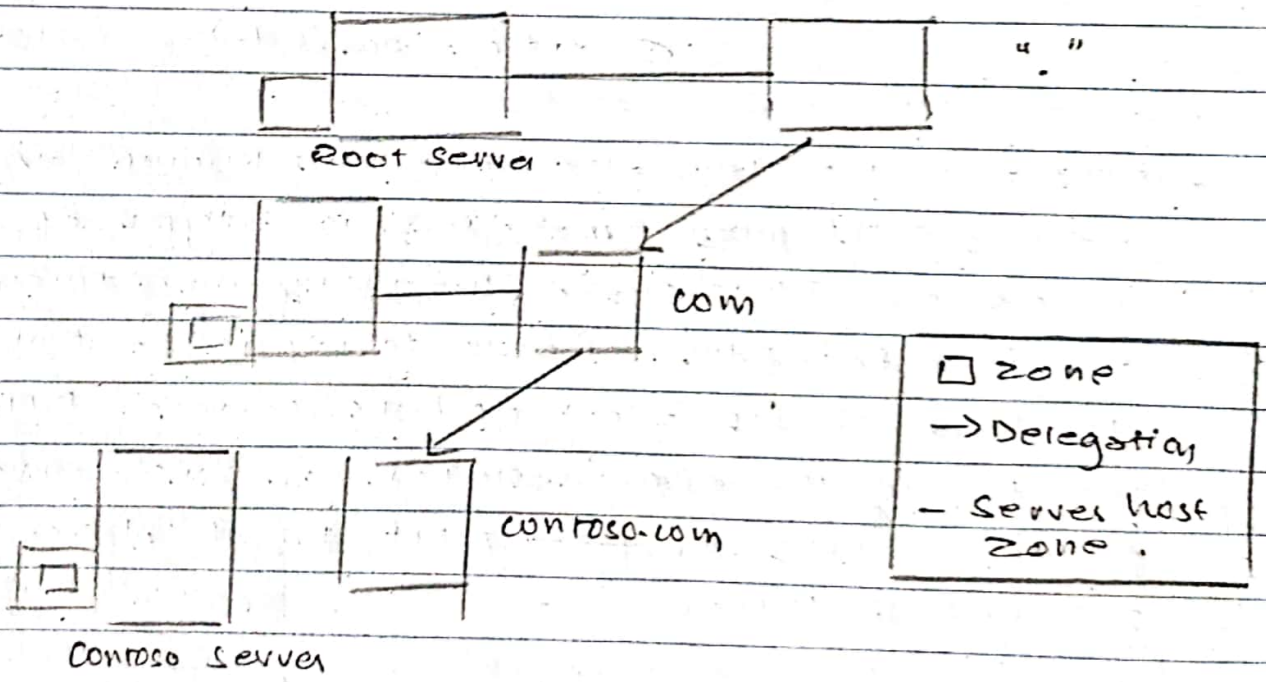
Question no. 3(b)

Ans:- DNS zone transfer, also sometimes known by the inducing DNS query type AXFR, is a type of DNS transaction. It is one of the many mechanism available for administrator to replicate DNS database across a set of DNS servers. DNS zone transfer is the process where a DNS server passes a copy of ~~part~~ part it's database to another DNS server.



DNS delegation:

For a DNS server to answer queries about any name, it must have a direct or indirect path to every zone in the namespace. These paths are created by means of delegation. A delegation is a record in a parent zone that lists a name server that is ~~authoritative~~ authoritative for the zone in the next level of hierarchy. Delegation makes it possible for servers in one zone to refer clients to servers in other zone.



Question no. 4(a).

Ans:-

Virtual hosting is a method for hosting multiple domains name on a single server. This allows one server to share its recources such as memory and processor cycles, without requiring all services provided to use the host name. The term virtual hosting is usually used in reference to web servers but the principles vary over to other internet services.

There are two main types of virtual hosting name based & IP based. Name based virtual hosting uses the host name presented by the client. IP based virtual hosting uses a separate IP addresses for each host name.

HTTP caching :-

HTTP is typically used for distributed information systems, where performance can be improved by the use of response caches. The HTTP/1.1 protocol includes a number of elements intended to make caching work.

The goal of caching in HTTP/1.1 is to eliminate the need to send requests in many cases, and to examinate the need to send full response in many other cases.

The following cache request directives can

be used by client in its HTTP request

i) no-cache ii) no-store iii) max-age = seconds
iv) max-state v) min-fresh vi) no-transform
vii) only-if-cached.

The following cache response directives can be used by the server in its HTTP response

i) public ii) private iii) no-cache
iv) no-store v) no-transform vi) must-revalidate
vii) proxy-revalidate viii) max age = seconds
ix) s-smaxage = seconds

Question no. 4(b)

ans:-

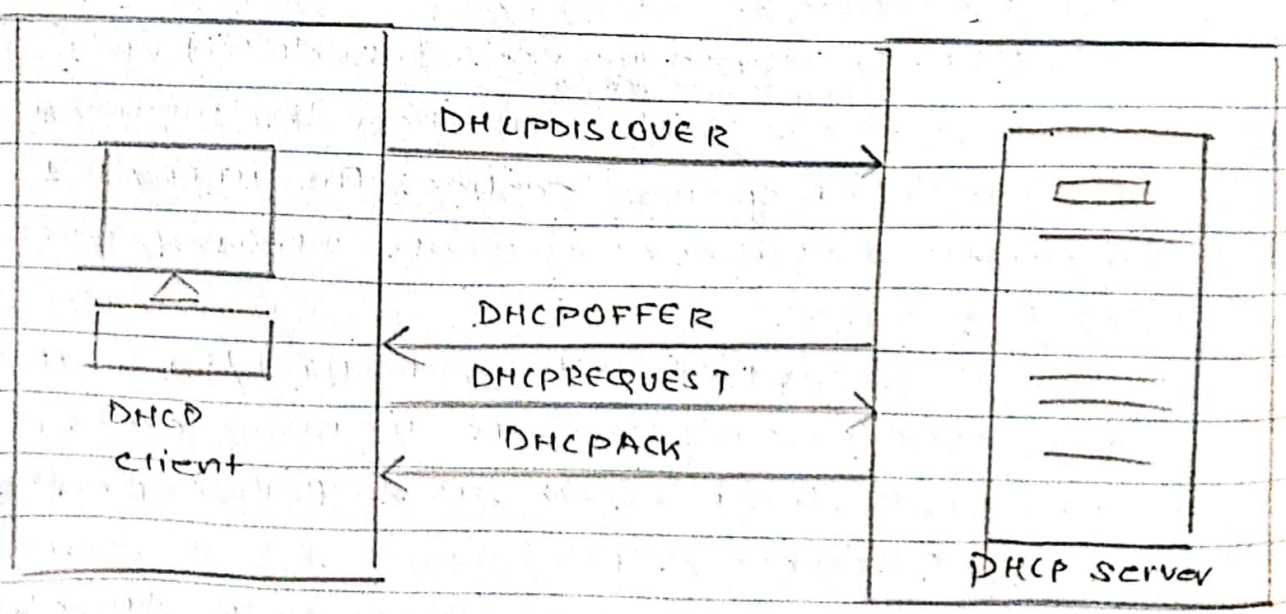
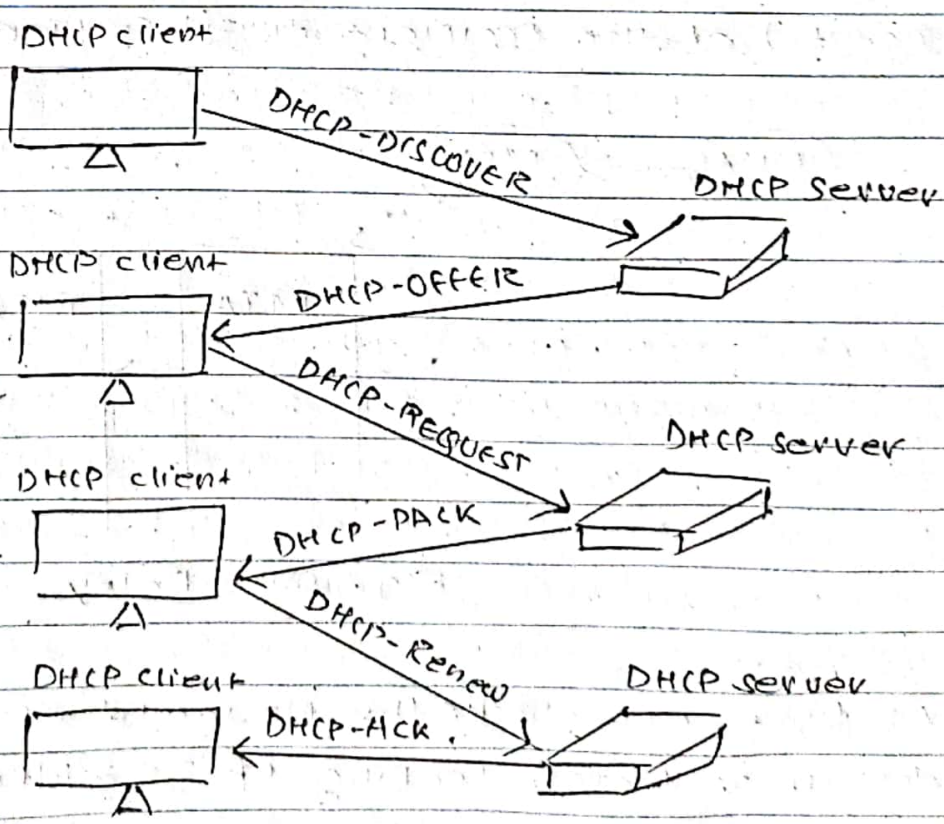


Fig DHCP principle

DHCP stands for Dynamic Host configuration Protocol. DHCP is a client-server protocol that uses DHCP servers and DHCP clients. The DHCP server typically has pool of IP addresses that is allowed to distribut to clients.

DHCP clients obtain a DHCP lease for an IP address, a subnet mask, and various DHCP options from DHCP server in a four step process.

1) DHCP DISCOVER
2) DHCP OFFER
3) DHCP REQUEST
4) DHCP ACK



Question No. 6(a)

Ans:. A simple mail transfer protocol relay is service that is used as a means to transport email messages in between different email hosting ~~de~~services or domains.

When we send an emails the email application on our computer connects to an SMTP relay and sends the message along with details the relay needs to figure out the next step. The relay uses the domain name in the email address and the DNS to figure out where the emails should be sent. The email may be sent directly to MDA (Message Delivery Agent) of the recipient email service

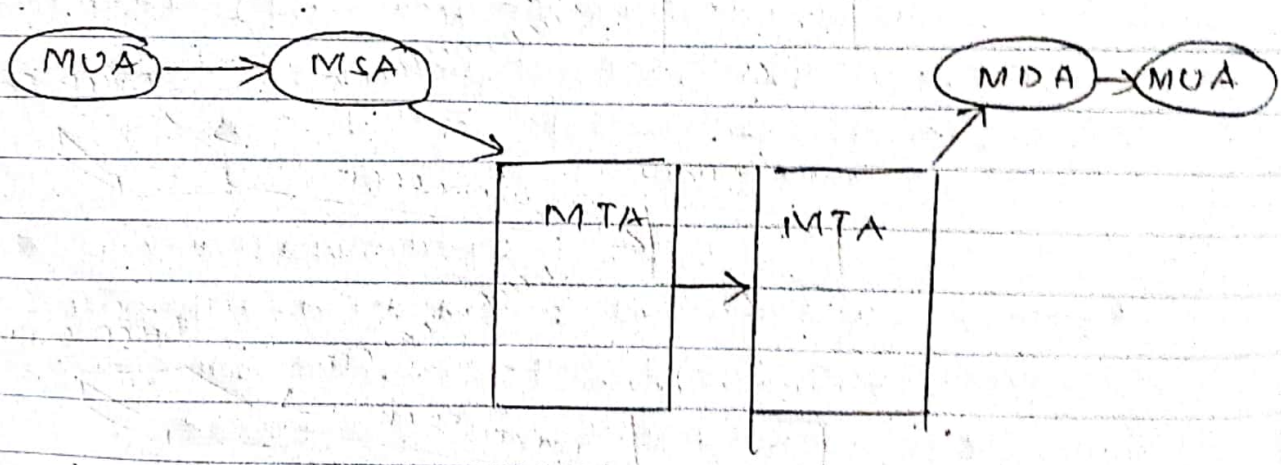


Fig: SMTP Relay

At first, MTA checks the MX record of the receipient domain as though looking up an address book where our mail should be routed. When it finds a match, it transfers the message to another MTA.

Depending on the destination and number of recipients message is moved between two or more MTAs before it finally reaches by MDA. Then the software stored in the receivers server converts them to a proper form and passes them to the recipient MUA.

Question no. 6(b)

Ans:- Email spam blocking techniques fall into one of two broad areas.

The first area, common in small to midsize sites is to add spam blocking technology to the Mail Transfer Agent (MTA)

The second technique is ~~now~~ used by larger sites with dedicated mail administrators, i.e. to put a mail blocking appliance between the MTA and the Internet.

We can control SPAM in mail server using following methods.

1) Spam blocking technologies.

Spam blocking technique can be added into the Mail Transfer Agent Exchange. Send mail postfix

and communicate are some examples of MTAs. Blocking the MTA has the advantage that no additional hardware is required

ii) Mail blocking appliance :

Mail blocking appliance can be placed between the MTA and the Internet. It is mainly used by larger sites as they can handle high volumes.

iii) Anti-spam techniques.

Both users and administrators of the email system uses anti-spam techniques. Anti-spam techniques can be broken into four broad categories : those that require action by individuals, those that can be automated by email administrators, those that can be automated by Email senders and those employed by researcher and law enforcement officials.

iv) 24/7 Server monitoring :

Hiring expert teams to monitor critical server metrics such as disk usage and server processes round the clock helps direct anomalies.