

B.E.

Seventh Semester Examination, 2010-11

System & Network Administration (IT-403-E)

Note : Attempt any *five* questions. All questions carry equal marks.

Q. 1. (a) What do you mean by system and Network administration ? Discuss the system components and their management.

Ans. System Administrator : A system administrator or sysadmin is a person employed to maintain and operate a computer system and/or Network. System administrator may be members of an IT or EC.

Sysadmins are usually charged with installing, supporting and maintaining servers or other computer systems, and planning for and responding to service outages and other problems.

Network Administrator : A network administrator is a person responsible for the maintenance of computer hardware and software that comprises a computer network. This normally includes deploying, configuring, maintaining and monitoring active network equipment.

Network administrator tasks such as network address assignment, assignment of routing protocols and routing tables configuration as well as configuration of authentication and authorization-directory service. Network administrator can do drivers and settings of personal computers as well as printers.

Q. 1. (b) What do you understand by File system ? Differentiate between UFS, NFS and NTFS. Which one is better and why ?

Ans. File System : A file system is a method of storing and organizing arbitrary collections of data in a form that is human readable. A file system organizes data into an easy to manipulate database of human readable names for the data usually with a human readable, hierarchical organization of data, for the shortage, organization manipulation and retrieval by computer's OS. Each discrete collection of data in a file system is referred to as a computer file.

NFS, UFS & NTFS :

NFS : Network File System
UFS : Unix File System
NTFS : Window NT File System

NFS are common place. They are typically integrated with the overall directory structure and interface of client system. NFS is a good example of a widely used, well implemented client-server network file system.

File system may contain information about how to boot an operating system stored there, the total number of blocks, the number and location of free blocks, directory structure, and individual files.

A boot control block (per volume) can contain information needed by the system to boot an OS from that volume. If disk does not contain OS, block is empty.

In UFS, it is called boot block (first block of a volume), NTFS it is portion boot sector.

Q. 2. (a) What are the various steps in booting the window OS ? Explain.

Ans. Booting Process : In computing, booting is a bootstrapping process that starts operating systems when the user turns on a computer system. A boot sequence is the initial set of operations that

the computer performs when it is switched on. The boot loader typically loads the main operating system for computer. Upon starting, a personal computer's X86 CPU runs the Instruction.

Basically booting process is bootstrapping process (to pull oneself up by bootstraps) that starts operating system whenever the user turns on or switch on the computer system.

Steps of the booting process in single OS :

- (i) The boot process starts by executing code in the first sector of the disk, MBR.
- (ii) The MBR looks over the partition table to find active partition.
- (iii) Control is passed to that partition's boot record (PBR) to continue booting.
- (iv) The PBR locates the system specific boot files (Win 98's io.sys or Win X P's ntoskrnl).
- (v) Then these boot files continue the process of loading and initializing the rest of OS.

Q. 2. (b) Write short note on process management and monitoring.

Ans. Process Management : Process management is an integral part of any modern day operating system. The OS must allocate resources to processes, enable processes to share and exchange information, protect the resources of each process from other processes and enable synchronization among processes. To meet these requirements, the OS must maintain a data structure for each process, which describes the state and resource ownership of that process, and which enables the OS to exert control over each process.

A program in execution, as mentioned is a process. The following duties done by OS connection with process management :

- (i) Creating and deleting both user and system processes
- (ii) Suspending and resuming processes
- (iii) Providing mechanisms for process synchronization
- (iv) Providing mechanisms for process communication
- (v) Providing mechanisms for deadlock handling.

Monitors : Semaphores provides a convenient and effective mechanism for process synchronization, using them incorrectly can result in turning errors that are difficult to detect, since these errors happens only if some particular execution sequences take place and these sequences do not always occur.

Q. 3. What are integrating Multiple operating system ? How user's ID are created in these system ? Also discuss the authentication, process in detail.

Ans. The windows preinstallation environment operating system is different from other windows systems in that it is used to help distribute workstations and servers through larger business groups. It is also considered to be an alternative to MS-DOS operating system. In fact the Win PE operating system can work to be an smaller version of more recent windows programs, including windows vista.

When Win PE operating system was created it was used to help with the deployment of another OS that is window based. Today however, the Win PE operating system is being used to help send servers around multiple computers in a larger business. This makes the Win PE operating system, ideal for a larger business that requires several similar computer working together.

The win PE operating system is used to help replace the MS-DOS prompt in terms of activating and accessing programs. This is generally used by technicians to help with repairing computers and checking on the general health of computer. It can also be used for accessing other utilities that are common on a computer with greater ease that what is normally used or MS-DOS.

One of best benefits of Win PE operating system is that it can be used as a recovery CD for an administrative system in a Network. This will help to give the user better access to the O/S in case of a major crash or damage on a computer.

On inception, `tcpd` will perform some access control checks and execute the desired service program.

tepd offers following features :

- (i) Complete Access control
- (ii) Checks against host name/address spoofing
- (iii) RFC 931 lookup for remote user who owns the connection.
- (iv) Support for services that use XT1 as well as sockets.
- (v) Setting traps
- (vi) Banner messages.

With TCP wrappers, you can :

- (i) Monitor incoming requests for Internet Services
- (ii) Control access to services spawned by inetd.
- (iii) Enforce access control in stand alone daemon programs.
- (iv) Predict how TCP wrapper would handle a specific request for a service.

Q. 4. (a) What is mean by subnetting and supernetting ? Discuss the different class of IP-address in detail.

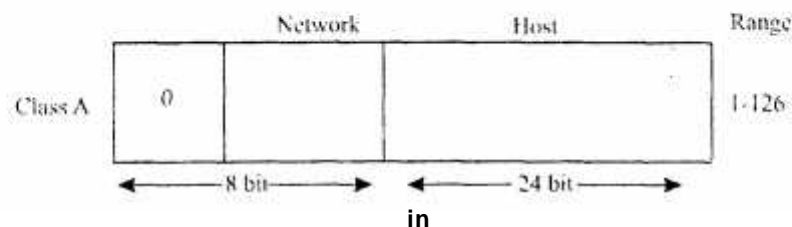
Ans. Subnetting : Subnetting allows you to create multiple logical networks that exists within a single class A, B or C. If you do not subnet, you are only able to use one network from your class A, B or C Network which is unrealistic. Each data link on a Network must have a unique.

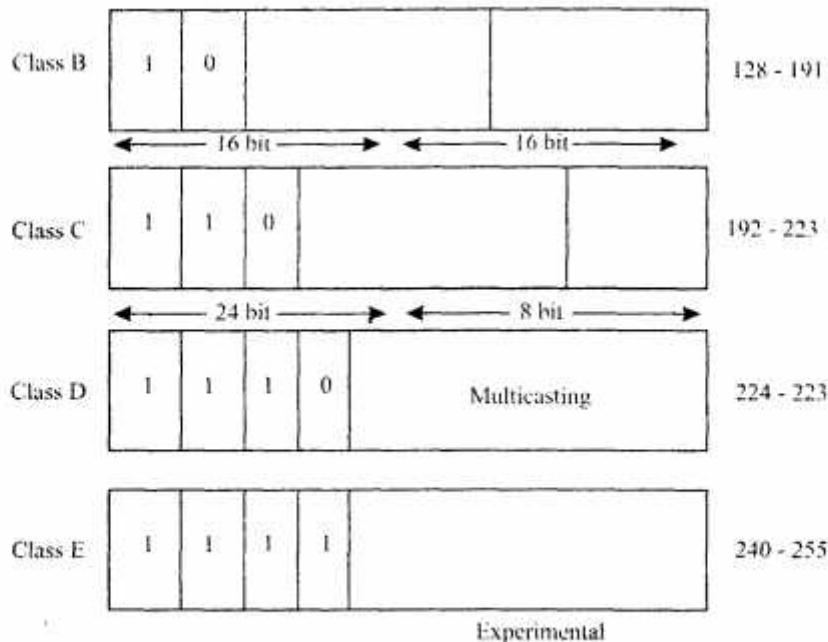
Network ID, with every node on that link being a member of same network, if you break a major network into smaller sub networks, it allows you to create a network of interconnecting subnetworks.

Example : $204.17 - 5.0 \quad \rightarrow \quad 11001100, 00010001, 00000101, 00000000$
 $255, 255, 255, 254 = \quad 11111111, 11111111, 11111111, \underbrace{111\ 000000}_{\text{sub}}$

Supernetting : A supernet is an Internet Protocol network that is formed from the combination of two or more networks (or subnets) with a common Classless Inter Domain Routing (CIDR) routing prefix. The new routing prefix for the combined network aggregates the prefixes of the Constituent Networks. The process of forming a supernet is called supernetting, route aggregation or route summarization.

ID Address Classes :





Q. 4. (b) For a given IP address 222.16, 21.10 and mask 255.255.255.240 answer the following :

- (i) What is broadcast IP address ?
- (ii) What is Subnet IP address ?
- (iii) What is valid range for host IP address ?

Ans. IP address 222.16.21.10

mask = 255.255.255.240

(i) **Broadcast IP Address :**

222.255.255.255

(ii) **Subnet IP Address : First subnet ID**

222.16.21.0001 0000

└───┘

4 bit for subnet

mask

255.255.255.240

255.255.255.1111

0000

└───┘

└───┘

N/w

Lost part

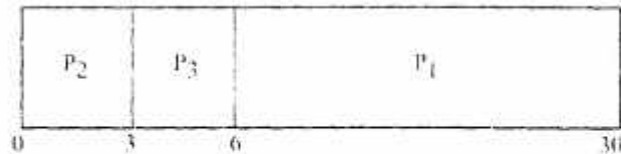
(iii) **Valid Range for Host**

Ist subnet 222.16.21.0001 0000

↓

222.16.21.0001 1111

Example : above example :



Q. 6. Discuss all the trouble shooting commands in detail with the help of examples.

Ans. Troubleshooting : Troubleshooting computer network is among the most important job descriptions of the network administrators, system administrator network technicians and IT consultants. A computer network can have different kinds of problems such as it can be infected with virus and spyware, attacked by hackers, accessed by unauthorized users and may face connectivity failure issues due to the faulty network devices or configurations. The right use of these troubleshoots commands can help a lot in diagnosing and resolving the issues with your computer network.

Ping : Ping is the most common & important troubleshooting command and it checks the connectivity with other computers.

IPCONFIG : IPCONFIG is another important command in windows. It shows the IP address of the computer and also it shows the DNS, DHCP Gateway addresses of Network and Subnet mask.

NET STAT : NETSTAT helps to troubleshoot the NETBIOS name resolutions problems.

ARP : ARP displays and modifies IP to physical address translation table that is used by ARP protocols.

Route : Route command allows you to make manual entries in routing table.

FINGER : Finger command is used to retrieve the information about a user on a network.

Q. 7. Why security is important in computers ? How does TCP wrappers provides access control ? Write the limitations of TCP wrapper.

Ans. Security is Important : Security is important in the computer. Security concern related with data communication using internet. Hackers and crackers want to Hack data and modified the information. Basic principle of Information Security is CIA.

C → Confidentiality

I → Integrity

A → Availability

TCP wrappers product suite provides an enhanced security mechanism for services spawned by the Internet Services daemon, inetd. TCP wrappers is available on HP—U X 11 i.e., platform as a web upgrade. Please visit www.docs.hp.com for related product documentation.

Whenever a connection is established with inetd for a service, inetd runs tcpd, the wrapper program instead of running the service program directly. NAT function was developed to address the limited number of IPv4 routable addresses that could be used or assigned to companies or individuals as well as reduce both amount and therefore cost of obtaining enough public addresses for every computer in an organization.

Q. 8. What is firewall ? Explain the different types of firewall in brief. What information might a stateful inspection firewall want to examine from multiple packets ?

Ans. Firewall : A Firewall is a device or set of devices designed to permit or deny network transmissions based upon a set of rules and is frequently used to protect networks from unauthorized access while permitting legitimate communications to pass.

Different Types of Firewall : There are several classifications of firewalls depending on where the communication is intercepted and state that is being traced.

(i) Network Layer & Packet Filters : Network layer firewalls; also called packet filters, operate at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set.

Network layer firewalls generally fall into two sub categories—stateful and stateless.

(ii) Application Layer Firewall : Application firewall work on the application level of the TCP/IP stack. (i.e., all browser traffic, or all telnet or ftp traffic) and may intercept all packets traveling to or from an application. Application firewalls can prevent all unwanted outside traffic from reaching protected machines.

(iii) Proxies : A Proxy device may act a firewall by responding to input packets in the manner of an application, while blocking other packets.

(iv) NAT : NAT stands for Network Address Translation. Firewalls often have NAT functionality and hosts protected behind a firewall commonly have addresses in the private address range.