B.E.

Seventh Semester Examination, May-2009

System & Network Administration (IT-403-E)

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

Q. 1. (a) What do you understand by system and network administration? Write the various goals that need to be taken care of for system and network administration.

Ans. Networks can be interconnected by different devices. In the physical layer, networks can be connected by repeaters or hubs, which just move the bits from one network to an identical network. These are mostly analog devices and do not understand anything about digital protocols.

One layer up, there are bridges and switches which operate at the datalink layer. They can accept frames, examine the MAC address and forward the frames to a different network while doing minor protocol translation in the process.

In the network layer, we have routers that can connect 2 networks. If 2 networks have dissimilar network layers, the router may be able to translate between the packet formats, although packet translation is now increasingly rare. A router that can handle multiple protocols is called multiprotocol router.

In the concatenated virtual circuit model, a connection to a host in a distant network is set up in a way similar to the way connections are normally established. The subnet sees that the destination is remote and builds a virtual circuit to the router nearest the destination network.

Q. 1. (b) What are the advantages and disadvantages of running a process in the background? Having run a process in the background, if you log out what would happen to a process?

Ans. While stable TSAP addresses work for a small number of key services that never change, user processes, in general, often want to talk to other user processes that only exist for a short time and do not have a TSAP address that is known in advance.

Furthermore, if there are potentially many server processes, most of which are rarely used, it is wasteful to have each of them active and listening to a stable TSAP address all day long. In short, a better scheme is needed. One such scheme is initial connection protocol. Instead of every conceivable server listening at a well known TSAP, each machine that wishes to offer services to remote users has a special process server that acts as a proxy for less heavily used servers. It listens to a set of a ports at the same time, waiting for a connection request. While the initial connection protocol works fine for those servers that can be created as they are needed. There are many situations in which services do exist independently of the process server.

Q. 2. (a) What is VLAN? What does trunking and frame tagging provide in establishing a VLAN?

Ans. In the early days of local area networking, thick yellow cables shaked through the cable ducts of many office buildings. Every computer they passed was plug go in. Often there were many cables, which were connected to a central back bone or to a central hub.

No thought was given to which computer belonged on which LAN. All the people in adjacent offices were put on the same LAN whether they belonged together or not geography trumped logic.

In response to user requests for more flexibility, network vendors began working on a way to rewill buildings entirely in software. The resulting concept is called a VLAN (virtual LAN) and has been standarized by the 802 committee.

It is now being deployed in many organisations. VLANs are based on specially designed VLAN aware switches, although they many also have some hubs on the periphery. To set up VLAN based network, the network administration decides how many VLANs there will be.

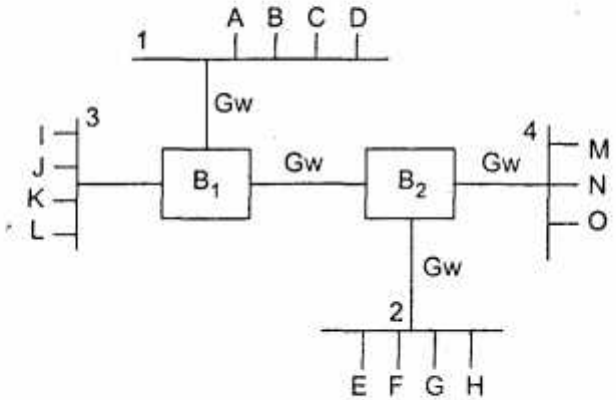

Fig. 4 physical LANs into 2 VLANs

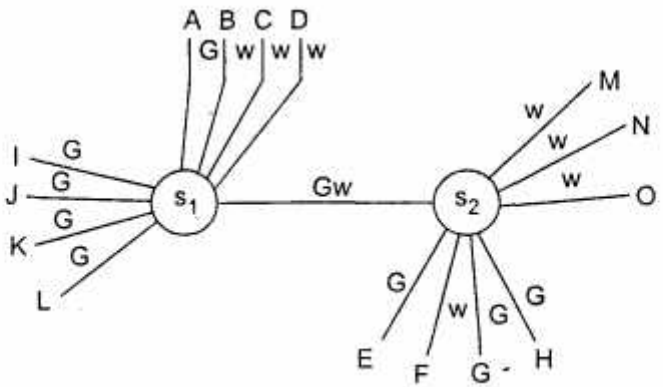

Fig. Same 15 machines organised into 2 VLANs by 2 switches

Q. 2. (b) What do you understand by open source software?

Ans. The internet is made up of a large number of autonomous systems. Each AS is operated by a different organization and can use its own routing algorithm inside.

For example, the internet networks of companies X, Y, and Z are usually seen as three A sees if three are on the internet.

All three may use different seen as AS three may use—different routing algorithms internally. Nevertheless, having standards, even for internal routing, simplifies the implementation at the boundaries between A sees and allows reuse of code. It routing algorithm witin an AS is called an interior gateway protocol.

Q. 2. (c) What is the role of swap space in installing UNIX operating system?

Ans. The role of swap space in installing UNIX operating system is same as ATM connection between 2 end points is accomplished through transmission paths, virtual paths and virtual circuits cell networks are based on virtual circuits. All cells belonging to a single message follow the same virtual circuit and remain in their original order until they reach their destination.

Q. 3. (a) Write the steps followed in configuring a Dial up connection. Explain any one protocol used in dial up network.

Ans. A dial up line has a maximum dat. rate of 50 Kbps, a difference factor of almost 20,000. That is the difference between a duck wadding leisurely through the grass and a rocket to the moon. If the dial up link is replaced by an ADSL connection, there is still a factor of 1000-2000 difference.

Each telephone has 2 copper w.res coming out of it that go directly to the telephone company's nearest end office also called local central office.

If a subscriber attached to a given end office calls another subscriber attached to the same end office, the switching mechanism within the office sets up a direct electrical connection between the 2 local loops. This connections remains intact for the duration of the call. If the called telephone is attached to another end office, a different procedure has to be used.

Each end office has a number of outgoing lines to one or more nearby switching contres called toll offices. These lines are called toll connecting trunks. If both the caller and caller's end offices happen to have a toll connecting trunk to the same toll office, the connection may be established within the toll office.

Q. 3. (b) SNMP protocol performs the function of which network layer. What are the functions of SNMP? Justify the statement 'SNMP work as a watchdog'?

Ans. The simple network management protocol is a framework for managing devices in an internet using the TCP/IP protocol suite or provides a set of fundamental operations for monitoring and maintaining an internet.

SNMP uses the Concept of Manager and Agent : SNMP has some very specific roles in network management. It defines the format of the packet to be sent from a manager to an agent and vice-versa. It also interprets the result and creates statistics. The packets exchanged contain the object names and their states. SNMP is responsible for reading and changing these values.

SNMP is called a watchdog because it continuously watches the function of manager and agent. That is a manager, usually a host, controls and monitors a set of agent and usually routers. It is an application level protocol in which a few managers stations control a set of agents. The protocol is designed at the application level so that it can monitor devices made by different manufactures like a watchdog does.

Q. 4. (a) What are Denial of Service attacks? How such attacks are detected? What measures are followed in preventing such attacks?

Ans. Attacks in which the intruder's goal is to shut down the target rather than steal data are called DOS attacks. Usually the request packets have false source addresses so the intruder cannot be traced easily.

As even worse variant is one in which the intruder has already broken into hundreds of computers elsewhere in the world, and then commands all of them to attack the same target at the same time. Not only does the approach increase the intruder's firepower, it also reduces his chance of detection, since the packets are coming from a large number of machines belonging to unsuspecting users. Such an attack is called a DDOS attack (Distributed Denial of Service). This attack is difficult to defined against.

Even if the attacked machine can quickly recognize a bogus request, it does take some time to process and discard the request, and if enough requests per second arrive, the CPU will speed all time dealing with them.

Q. 4. (b) What are Firewalls? What filtering rules do they follow? Write what firewalls can and cannot block.

Ans. Firewalls are just a modern adaptation of that old medieval security standby : digging a deep moat around your castle. This design forced everywhere entering or leaving the castle to pass over a single drawbridge, where they could be inspected by the I/O police. With networks, the same trick is possible; a company can have many LANs connected in arbitrary ways, but all traffic to a from the company is forced although an electronic drawbridge. A common firewall has packet filtering and an application gateway. Simpler configurations also exist, but the advantage of this design is that every packet must transit 2 filters and an appliction gateway to go in or out. No other route exists readers who think that one security checkpoint is enough have not made an international flight on a scheduled airline security.

Each packet filter is a standard router equipped with some extra functionality. The extra functionality allows every incoming or outgoing packet to be inspected packets meeting some criterion are forwarded normally. Those that fail the test are dropped.

Q. 5. (a) Explain the directory structure of UNIX operating system in detail.

Ans. While the initial connection protocol works fine for the servers that can be created as they are needed, there are many situations in which services do exist independently of the process server. A file server, for example, needs to run on special hardware and cannot just be created on the fly when someone wants to talk to it.

To handle this situation, an alternative scheme is often used. In this model, there exists a special process called a name server or sometimes a directory server. To find the TSAP address corresponding to a given service name, such as "time of day" a user sets up a connection to the name server. The user then sends a message specifying the service name, and the name server sends backs the TSAP address.

Then the user releases the connection with the name server and establishes a new one with the desired service.

In this model, when a new service is created, it must register itself with the name server, giving both its service name and its TSAP. The name server records this information in its internal database so that when queries come in later, it will know the answers.

Q. 5. (b) Explain the use of any five administrative commands along with their syntax.

Ans. Admission control refers to the mechanism used by a router or a switch, to accept or reject a flow based on predefined parameters called flow specifications. Before a router accepts a flow for processing, it checks the flow specifications to see if its capacity and its previous commitments to other flows can handle the new flow.

Path : Recall that the receivers in a flow make the reservation in RSVP. However the receivers do not know the path travelled by packets before they reservation is made.

ResV : After receiver has received a path message, it sends a ResV message. The ResV message travels towards the sender and makes a resource reservation on the routers that support RSVP. If a router do not support RSVP on the path, it routes the packet based on the best effort delivery methods.

Q. 6. (a) Write a shell program to find the greatest among the three numbers entered thro' the keyboard.

Ans.
```
void protocol 6(void)
{
        seq_nr ack_expected
        seq_nr next_frame_to_send;
        int i;
        frame r;
        pa              [NR_BUFs];
          ...           R_BUFs];
          ...an arriv...  NR_BUFs];
                ...ffered;
        even...  ...pe event;
        enable_network_layer( );
        ack_expected = 0;
        next frame_to_send = 0;
        nbuffered = 0;
        for (i = 0, i < NR_BUFs; i++) arrived [i] = false;
        while (true){
        wait_for_event (&event);
        start_ack_timer( );
    }
  }
}
```

Q. 6. (b) Write the use and syntax of the following TCP/IP trouble shooting commands : ping, ipconfig, tracert, ifconfig and netstat.

Ans. Basically all of these commands are TCP/IP trouble shooting commands, whose main task is to find out the IP address.

ping is used to ping; to initiate the IP address, when we have just started internet.

ipconfig is used to configure the IP address.

tracert is used to trace the IP address.

netstat gives us the network status whether the network connection is enabled or disabled.

IPv4 is the delivery mechanism used by TCP/IP protocols. IPv4 is an unreliable and connectionless datagram protocol—a best effort delivery service. If reliability is important it must be paired with reliable protocol such as TCP.

Q. 7. (a) Differentiate between static a..d dynamic routing. What is the need of routing protocols? Explain any one protocol in detail.

Ans. The routing algorithm is that part of the network layer software responsible for deciding which output line an incoming packet should be transmitted on. If the subset uses datagrams internally, this decision must be made a new for every arriving data packet since the best route may have changed since last time. If the subnet uses virtual circuits internally, routing decisions are made only when a new virtual circuit is being set

up. Therefore, data packets just follow, the previously established route. The later case is sometimes called session routing because a route terminal in force for an entire user session.

Routing algorithms can be grouped into 2 major classes : non-adaptive and adaptive. Non-adaptive algorithms donot base their routing decisions on measurements or estimates of the current traffic and topology. Instead, the choice of the route to use to get from I to J is computed in advance, off line, and downloaded to the routers when the network is booted. This procedure is called static routing.

Adaptive algorithms, in contrast, change their routing decisions to reflect changes in the topology and usually the traffic as well. Adaptive algorithms differ in where they get their information (from all routers) when they change the routers, when the load changes or when the topology changes and what metric is used for optimization. i.e., distance, number of hops or estimated transit time.

Q. 7. (b) Write the various steps followed in configuring a web server.

Ans. When the user types in a URL or clicks on a line of the hypertext, the browser passes the URL and interprets the part between http:// and the next slash as a DNS name to look up. Arrived with the IP address of the server, the browser establishes a TCP connection to port so on that server. Then it sends over a command containing the rest of the URL, which is the name of a file on that server. The server then returns the file for the browser to display. The steps that server performs in its main loop are :

(i) Accepts the TCP connection from a client i.e., browser.

(ii) Get the name of file requested.

(iii) Get the file i.e., from disk.

(iv) Return the file to the client.

(v) Release the TCP connection.

Modern web servers have more features, but in essence, this is what a web server does.

A problem with this design is that every request requires making a disk access to get the file. The result is that the web server cannot serve more requests per second that it can make disk accesses.

A high end SCSI disk has an average access time of around 5m sec., which limits the server to at most 200 requests/sec.

Q. 8. Write short notes on :

(a) NAT

(b) CERT

(c) Wrappers

(d) Categories of security

Ans. (a) NAT (Network Address Translation) : The problem of running out of IP addresses is not a theoretical problem that might occur at same point in the distant future. It is happening right here and right now. The long term selection is for the whole internet to migrate to IPv6, which has 128 bits addresses. This transition is slowly occurring, but it will be years before the process is complete.

As a consequence, some people felt that a quick fix was needed for the short term. This quick fix came in the form of NAT, which is described in RFC 3022. The basic idea behind NAT is to assign each company a single IP address, at most, for internet traffic.

Within the company, every computer gets a unique IP address. Which is used for routing intramural traffic. However, when a packet exists the company and goes to the ISP, an address transaction takes place.

(b) CERT : By the early 1970s, a number of countries were defining national standards for telecommunication, but there was still little international compatibility. The united nations responsed by forming, as a part of its International Telecommunication Union (ITU), a committee, the consultive committee for international telegraphy and telephony. this committee was general and for phone and data systems in particular on March 1, 1993, the name of this committee was changed to the International Telecommunication Union Telecommunication Standards Sector (ITU-T). All communication technology is subject to regulation by government agencies such as federal communication.

(c) Wrappers : Each voice channel is digitized using wrappers. It is a very complex PCM and compression technique. A voice channel is digitized to 7.95 Kbps. Three 9.75 Kbps digital voice channels are combined using TDMA. The result is 48.9Kbps of digital datas much of this is overhead. Each slot holds 324 bits. However, only 159 bits comes from the digitized voice; 64 bits are for control and 101 bits are for error correction. In other words, each channel drops 159 bits of data into each of 2 channels assigned to it. The system adds 64 control bits and 101 error correcting bits.

(d) Categories of Security : Security is a broad topic and covers a multitude of sins. In its simplest form, it is concerned with making sure that nosy people cannot read, or worse yet, secretely modify messages intended for other recipients. It is concerned with people trying to access remote services that they are not authorized to use. It also deals with ways to tell whether that message purportedly from the IRS saying : Pay by Friday or else is really from the IRS and not from the Mafia security also deals with ways to tell whether that message purportedly from the IRS saying being captured and replayed and with people trying to deny that they sent certain messages. Most security problems are intentionally caused by malicious people trying to gain some benefit, get attention or to train someone.