1. What kinds of issues does system administration cover?

System administration is not just an administrative job, it's about hardware, software, user support, diagnosis, repair and prevention. System administrator needs technical, administrative and socio-psychological skills. He works for users, so that they can use the system to produce work. He works for the benefit of whole community.

2. Is system administration management or engineering?

3. Why does the physical environment play a role in system administration?

Software requires hardware to run on and hardware requires power, a temperate climate and a conformance to basic standarts in order to wor systematically. Modern software needs to inter-operate and survive the possible hostilities of incompatible or inhospitable competitors. Part of the challenge is to knit apparently disparate pieces of this community into a harmonious whole. We apply technology in such an enviroment for a purpose, and purpose guides our actions and decisions. Administrators are forced to thing globall. Inter-networked systems are exposed to attack.

4. Describe why ethics and human values are important.

Computer systems are human-computer communities. Some decisions have to be made to protect the rights of individual. A system administrator has many responsibilities and constraints to consider. An administrator's job is to make users' lives bearable and to
empower them in the production of real work. It requires
patience, understanding, knowledge and experience.

5. Is system administration a science? Why/why not?

Unlike pshysics, chemistry or biology, SA is lacking in a systematic body of experimental data which would give its rules and principles an empirical rigor. However

6. State the top-most principles that guide network and system administrators.

- Policy is the foundation. SA begins with a policy.

- Predictability which is the basis of reliability, hence trust and therefore security.

- Scalability; growing in accordance with policy

2 System Components

1. Describe the main hardware components in a human–computer system.
- Host computers: computer devices that run software
- Network hardware:
    1) dedicated computing devices that direct traffic around Internet. Routers talk at the IP address level (layer 3)
    2) Switches: fixed hardware devices that direct traffic around local area networks. Switches talk at the level of Ethernet (layer 2)
    3) Cables that interconnect devices

2**. What rules of thumb would you use for handling the different hardware components.**
Before touching any computer components, earth yourself by touching the metal casing of the computer. If you are installing equipment inside a computer, wear a conductive wrist strap. Avoid wearing rubber sandals or shoes. Wear rubber soles when working around high voltage or current sources.

3. What effect does temperature have on computer systems?
Heat can cause systems to overheat and suddenly black out. Incrised temperature also increases noise levels that can reduce network capacities. Heat can cause RAM to operate unpredictably and disks to misread/miswrite. Suden changes from hot to cold can cause changes in electrical properties of chips and cause systems to crash.

4. What is the function of an operating system? (Hint: how do you define an operating system?)
Allocating and sharing the resources od the system between several running programs or processes. The operating system runs interactive programs for humans**, *services*** for local and distributed users and support programs which work together to provide the infrastructure which enables machine resources to be shared between many processes. Some operating systems also provide text editors, compilers, debuggers and a variety of other tools. Since the operating system (OS) is in charge of a computer, all requests to use its resources and devices need to go through the OS kernel. An OS therefore provides *legal entry points* into its code for performing basic operations like writing to devices.

5. Why is it important to distinguish between single and multiuser operating systems?
Multi-user operating system allows multiple users to share the resource of a single host. It is necessary to protect users from one another by giving them a unique identity or user name and a private login area, i.e. by restricting their privilege.

6. What is meant by a securable operating system?
Securable operating systems have the mechanisms which make a basic level of preventative security possible. They have ability to restrict access to certain system resources. Ordinary users do not have the privileges required to change system files.

7. What is meant by a shell?
It's command line user interface allowing users to express what they want with more freedom and precision. Shells can be used to write simple programs called *scripts* or *batch files* which often simplify repetitive administrative tasks.

8. What is the role of a privileged account? Do non-securable operating systems have such accounts?
System administrators need access to the whole system in order to watch over it, make backups and keep it running. Secure operating systems thus need a privileged account which can be used by the system administrator when he/she is required to make changes to the system. Operating systems that restrict user privileges need an account which can be used to configure and maintain the system. Such an account must have access to the whole system, without regard for restrictions. It is therefore called a privileged account.

9. Summarize the similarities between Unix and Windows.
Many basix commands are similar, the structure of directories and files...

10. What do the DOS/Windows drive letters A:, B:, etc. correspond to in Unix-like operating systems?
/dev and /devices

11. What is an Access Control List?
ACLs, or access control lists are a modern replacement for file modes and permissions. With access control lists we can specify precisely the access rights to files for each user individually. ACLs are literally lists of access rights.

12. How are files shared between users in Unix/Windows?

13. How are files shared between computers in Unix/Windows?

14. What is meant by a process or task?
On a multitasking computer, all work on a running program is performed by an abstraction called a *process*. This is a collection of resources such as file handles, allocated memory, program code and CPU registers that is associated with a specific running program.

15. How are processes started and stopped?
Unix starts new processes by copying old ones. Users start processes from a *shell* command line interface program or by clicking on icons in a window manager. Processes can be stopped and started, or killed once and for all. The kill command does this and more.

16. Name and describe the layers of the OSI model.

Open System Interconnect mode is a generalized abstraction of how network communication can be and is implemented. The OSI model describes seven layers of abstraction:

7 Application layer	Program protocol commands
6 Presentation layer	XDR or user routines
5 Session layer	RPC / sockets
4 Transport layer	TCP or UDP
3 Network layer	IP Internet protocol
2 Data link layer	Ethernet protocol
1 Physical layer	Cables, interfaces

1. **Physical layer**. This is the sending a signal along a wire, amplifying it if it gets weak, removing noise etc. If the type of cable changes (we might want to reflect signals off a satellite or use fiber optics) we need to convert one kind of signal into another. Each type of transmission might have its own accepted ways of sending data (i.e. protocols).
2. **Data link layer**. This is a layer of checking which makes sure that what was sent from one end of a cable to the other actually arrived. This is sometimes called handshaking. The Ethernet protocol is layer 2, as is Token Ring. This level is labelled by Media Access Control (MAC) addresses.
3. **Network layer**. This is the layer of software which recognizes structure in the network. It establishes global identity and handles the delivery of data by manipulating the physical layer. The network layer needs to know something about addresses – i.e. where the data are going, since data might flow along many cables and connections to arrive where they are going. Layer 3 is the layer at which IP addresses enter.
4. **Transport layer.** We shall concentrate on this layer for much of what follows. The transport layer builds 'packets' or 'datagrams' so that the network layer knows what is data and how to get the data to their destination. Because many machines could be talking on the same network all at the same time, data are broken up into short 'bursts'. Only one machine can talk over a cable at a time so we must have sharing. It is easy to share if the signals are sent in short bursts. This is analogous to the sharing of CPU time by use of time-slices. TCP and UDP protocols are encoded at this layer.
5. **Session layer.** This is the part of a host's operating system which helps a user program to set up a connection. This is typically done with sockets or the RPC.
6. **Presentation layer**. How are the data to be sent by the sender and interpreted by the receiver, so that there is no doubt about their contents? This is the role played by the external data representation (XDR) in the RPC system.
7. **Application layer**. The program which wants to send data has its own protocol layer, typically a command language encoding (e.g. GET, PUT in FTP or HTTP).

17. Describe the main local area networking technologies and how they differ.

• **Bus/Ethernet approach**: Ethernet technology was developed by Xerox, Intel and DEC in 1976, at the Palo Alto Research Center (PARC) [103]. In the Ethernet bus approach, every host is connected to a common cable or bus. Only one host can be using a given network cable at a given instant. It is like a conference telephone call: what goes out onto a network reaches all hosts on that network (more or less) simultaneously, so everyone has to share the line by waiting for a suitable moment to say something. Ethernet is defined in the IEEE 802.3 standard documents. An Ethernet network is available to any host at any time, provided the line isn't busy. This is called CSMA/CD, or Carrier Sense Multiple Access/Collision Detect. A collision occurs when two hosts attempt to send signals simultaneously. CSMA/CD means that if a card has something to send, it will listen until no other card is transmitting, then start transmitting and listen if no other card starts transmitting at the same time. If another card began transmitting it will stop, wait for a random interval and try again. Today, Ethernet is progressing in leaps and bounds. Switched Ethernet running on twisted pair cables can deliver up to 100 megabits per second (100BaseT, fast Ethernet). Gigabit Ethernets are already common. The main limitation of Ethernet networks is the presence of collisions. When many hosts are talking, performance degrades quickly due to time wasted by hosts waiting to get a word in. In order to avoid collisions, packet sizes are limited. With a large number of small packets, it is easier to share the time between more hosts. Ethernet interfaces are assigned a unique MAC address when they are built. The initial numbers of the address identify each manufacturer uniquely. Full-duplex connections at 100MB are possible with fast Ethernets on dedicated cables where collisions cannot occur.
• **Token Ring/FDDI approach:** In the token ring approach [253], hosts are coupled to hubs or nodes each of which has two network interfaces and the hosts are connected in a uni-directional ring. The token ring is described in IEEE 802.5. The token ring is a deterministic protocol; if Ethernet embraces chaos, then the token ring demands order. No matter when a host wishes to transmit, it must wait for a passing token, in a specified time-slot. If a signal (token) arrives, a host can append something to the signal. If nothing is

appended, the token is passed on to the next host which has the opportunity to do the same. Similarly, if the signal arriving at one of the interfaces is for the host itself then it is read. If it is not intended for the host itself, the signal is forwarded to the next host where the same applies. A common token ring based interface in use today is the optical FDDI (Fiber distributed data interface). Token rings can pass 16 megabits per second, with packet sizes of 18 kilobytes. The larger packet sizes are possible since there is no risk of collisions. Like Ethernet interfaces, token ring interfaces are manufactured with a uniquely assigned MAC address.

• **Frame Relay** is an alternative layer 2 packet-switching protocol for connecting devices on a Wide Area Network (WAN) or backbone. It is used for point-topoint connections, but is capable of basic switching, like ATM, so it can create virtual point-to-point circuits, where several switches might be involved (see chapter 10). Frame relay is popular because it is relatively inexpensive. However, it is also being replaced in some areas by faster technologies, such as ATM. Frame relay has the advantage of being widely supported, and is better suited than ATM for data-only, medium-speed (56/64 Kbps, T1): the ratio of header size to frame size is typically much smaller than the overhead ratio for ATM.

• **ATM, Asynchronous Transfer Mode technology** [23], is a high capacity, deterministic, transmission technology developed by telephone companies in order to exploit existing copper telephone networks. ATM is a layer 2–3 hybrid technology. ATM is believed to be able to reach much higher transfer rates than Ethernet, since it disallows collisions and is optimized for switching. Its expense, combined with the increasing performance of fast Ethernet, has made ATM most attractive for high speed Internet backbones and Wide Area Networks, though some local area networks have been implemented as proof of principle.

18. What are the following?: i) repeater, ii) hub, iii) switch, iv) bridge, v) router.

A **bridge** is a hardware device which acts like a filter on busy networks. A bridge works like a 'mini-router' and separates two segments of the same cable. A bridge knows which incoming cables do not offer a destination address and prevents traffic from spreading to this part of a cable. A bridge is used to isolate traffic on busy sections of a network or conversely to splice networks together. It is a primitive kind of switch.

A **repeater** is an amplifier that strengthens the network signal over long stretches of cable. A multi-port repeater also called a hub does the same thing and also splits one cable into N sub-cables for convenience. Hubs are common in twisted pair networks where it is necessary to fan a cable out into a star pattern from the hub to send one cable to each host.

A **switch** is a hub which can direct a message from one host cable directly to the intended host by routing the signal directly. The advantage with this is that other machines do not have to see the traffic between two hosts. Each pair of hosts has a virtual private cable. Switched networks are not immune to spies, net-sniffing or network listening devices, but they make it more difficult for the casual browser to see traffic that does not concern them. A switch performs many of the tasks of a router and vice versa. The difference is that a switch works at layer 2 of the OSI model (i.e. with MAC addresses), whereas a router works at layer 3 (IP addresses). A switch cannot route data on a world-wide basis.

A host which is coupled to several network segments and which forwards data from one network to another is called a **router**. Routers not only forward data but they prevent the spread of network messages which other network segments do not need to know about. This limits the number of hosts which are sharing any given cable segment, and thus limits the traffic which any given host sees. Routers can also filter unwanted traffic for security purposes [77]. A router knows which destination addresses lie on which of the networks it is connected to and it does not let message traffic spread onto irrelevant cables.

19. How is a network packet from a single host computer prevented from spreading randomly all over the planet? How is such a packet still able to reach a specified location on the other side of the planet?

A router isolates one part of a network from another, both logically and physically. It will only forward the signal if the signal needs to travel along another segment to reach its destination address.

Switches and routers prevent traffic from leaking along cables that it does not need to traverse.

Encapsulation. Protocols

20. What does it mean to say that a computer is big-endian?

It refers to byte-order of numerical representation. Big-endian systems store the most significant byte first.

21. What is an IP address and what does it look like?

Unique number of every network interface on the Internet.In version 4 IP address consists of 32 bits.

22. Do class A,B,C IP addresses have any meaning today?

The difference between class A, B and C networks lies in which bits of the IP addresses refer to the network itself and which bits refer to actual hosts within a network. With this scheme only about two percent of the actual number of IP addresses can be actually used. Classed addressing will survive in books.

23. What IPv4 addresses are reserved and why?

Some IP addresses are reserved for a special purpose.

- 0.0.0.0 Default route
- 0.*.*.* Not used
- 127.0.0.1 Loopback address
- 127.*.*.* Loopback network
- *.*.*.0 Network addresses (or old broadcast)
- *.*.*.255 Broadcast addresses
- *.*.*.1 Router or gateway (conventionally)
- 224.*.*.* Multicast addresses
- 192.0.2.0 - 192.0.2.255 example.org

The zeroth address of any network is reserved to mean the network itself, and the 255th (or on older networks sometimes the zeroth) is used for the broadcast address. Some Internet addresses are reserved for a special purpose. These include network addresses (usually xxx.yyy.zzz.0), broadcast addresses (usually xxx.yyy.zzz.255, but in older networks it was xxx.yyy.zzz.0) and multicast addresses (usually 224.xxx.yyy.zzz).

24. What is a loopback address?
The loopback address is an address which every host uses to refer to itself internally. It points straight back to the host. It is a kind of internal pseudoaddress which allows programs to use network protocols to address local services without anything being transmitted on an actual network.

25. What is meant by a broadcast address?
Završna ili broadcast adresa (Broadcast ID) je adresa na kojoj mrežni promet primaju sva računala unutar podmreže. Kad želimo poslati podatke svim uređajima u podmreži koristimo broadcast adresu.

26. Describe the purpose of a subnet and its netmask.
The purpose of subnets is to devide up networks into regions which naturally belong together and to isolate regions which are independent. This reduces the propagation of useless traffic, and it allows us to delegate and distribute responsibility for local concerns.

27. What is a default route?
Default route is a destination to which outgoing packets will be sent for processing when they do not belong to the subnet. This is address of the router or gateway on the same network segment.
If this default route is not set, a host will not know where to send packets and will therefore attempt to build a table of routes, using a different entry for every outgoing address. This consumes memory rapidly and leads to great inefficiency. In the worst case the host might not have contact with anywhere outside its subnet at all.

28. What are ARP and RARP? Are they needed in IPv6? Why/why not?
TheAddress Resolution Protocol is a name service directory for translating from IP address to hardware, Media Access Control (MAC) address. The ARP service is mirrored by a revers lookup ARP service (RARP). RARP takes a hardware address and turns it into an IP address.

29. Explain the concept of an Autonomous System.
An Autonomous System is a set of routers under a single administrative umbrella, that is responsible for its own internal routing, but which needs to exchange data along exterior or border routes between itself and othes autonomous systems.

30. What is meant by Network Address Translation, and what is its main purpose?
In a NAT, a network is represented to the outside world by a single official IP address. When one host in a private network attempts to contact an address on the Internet, the NAT creates the illusion that the requwst comes from the single representative address. The return data are routed back to the particular host.Outside world is not able to see private addresses behind a NAT. There are many problems. The most serious, perhaps, is that it breaks certain IP security mechanisms that rely on IP addresses, because IP addresses are essentially spoofed.

31. Describe how IPv6 addresses differ from IPv4 addresses.
128bits; hexadecimal notation; autoconfiguration and neighbor discovery; mobile computing

32. Can IPv6 completely replace IPv4?