1.
A rack server is a server that is placed inside a rack. Rack servers are general-purpose servers that handle a wide range of applications and computer architecture. To minimize floor space in data centers, the racks stack servers vertically. The more the hardware administrators can store upwards, the more hardware they can store horizontally.

Standardized racks are measured in 1.75-inch-tall, 19-inch-wide units (Us). Vertical multipliers allow rack servers to fit within these dimensions, therefore rack server heights can be 1U, 4U, 10U, or greater, such as the 10-foot tall 70U rack that was released in 2016. Additional devices are also made to meet the rack unit standard, allowing businesses to employ empty units in their racks.

A blade server is a container that includes several modular circuit boards known as server blades. Most majority of blade servers are reduced to CPUs, network controllers, and memory. Some models include internal storage disks. Additional components, like switches, ports, and power connections, are shared via the chassis.

Containers often meet rack unit dimensions, allowing IT to save space. Operators can cluster blades or manage and run each as a single server, such as allocating programs and end-users to specific blades. Their modular construction allows for hot exchanges. Blades include little exterior grips that make it easy to pull out or replace them.

The chassis provides electricity to many blade servers rather than powering and cooling multiple servers in separate racks. This conserves energy. Processing Power: Blade servers offer great processing power while taking up less space.

Heavy blade servers require up-to-date climate regulator technology. Administrators have to spend their expenses on heating, cooling, and ventilation such that the blade performance does not deteriorate.

The cost of initial capital, deployment, and configuration of the blade servers is more as compared to rack-mounted servers.

References: https://www.serverwatch.com/hardware/blade-servers-vs-rack-servers/

2.
The potential of lower capital and operating expenditures is a crucial motivator.
The servers present in the data centers are connected. Also, the servers are connected to the outside world. As the quantity of services grows, they must fit into the available space. The two techniques for connecting, top-of-row and end-of-row, result in distinct cabling possibilities.

Ethernet delivers a secure, dependable, high-speed backbone that allows you to manage data growth and application performance while also improving the security of every connected site.

Ethernet also provides other facilities such as:
i. Greater Productivity

ii. Ease of Adoption

iii Increased Efficiency

iv. Security and Control

References:
https://assets.lumen.com/is/content/Lumen/how-to-guide-choosing-the-right-ethernet-provider?Creativeid=7a1b9b60-f6a4-4d6b-a014-626504832d01#:~:text=Ethernet%20provides%20a%20secure%2C%20reliable,Ethernet%20is%20a%20solid%20choice.

3.
Direct-attached storage (DAS) is a form of storage that is connected to a computer without the need for a network. The storage might be linked both inside and outside. Only the host computer has immediate access to the data. To operate with the data, other devices must travel via the host computer.

A storage device that is directly coupled to a computer is not networked. There are no connections via Ethernet or Fibre Channel (FC) switches, as with network-attached storage (NAS) or a storage area network (SAN) (SAN).

DAS is better ideal for smaller firms that share data locally rather than over a large network since it does not link to the network. On individual PCs, DAS is simple to set up, requiring simply the storage device and any optional drive enclosures.

DAS has limited scalability and lacks the centralized administration and backup features that other storage solutions providers have. Furthermore, it is difficult to share and does not provide for failover if the server fails. Because of these difficulties, traditional versions of DAS may not be suitable for certain corporate applications.

When a virtual machine is relocated to a different host machine, the related storage must be moved as well, which is likely to eat a significant amount of bandwidth and time.

4.
Line coding, out-of-band signals, and other serial transmission preparations are handled by the Phy layer. The layer's name is based on the logical construct PHY, which symbolizes a device's transceiver, which consists of a transmitter and a receiver.

Cables, connections, and transceivers have physical and electrical characteristics, which are dealt with in the physical layer.

Resources:
http://www.csit-sun.pub.ro/~cpop/Documentatie_SMP/Standarde_magistrale/SCSI/SCSITApdfs/SAS_Phy_layer.pdf

5.
The generic file-related system calls are created, read, delete, write or close.

There are two reasons for which there is no RPC invocation for the close <file> system call in the NFS system

i. Because of the initial stateless architecture of servers (which do not retain account of prior requests) to aid crash detection, the NFS protocol does not feature a close procedure.

ii. There is no file modification

Even though a remote file operation has an RPC counterpart, it does not always result in an RPC invocation. When the information is saved in the client cache, no such invocation is required, which minimizes the number of remote procedure calls and increases speed.

6.
Arbitrated loop, fabric, and point-to-point are the three topologies that are supported in FC - 2M.

1)The simplest topology is a point-to-point link between two ports that are comparable to the SAS ports explained before. It has the same effect as DAS, except it can travel larger distances and work faster.

2)The topology of the fabric is the most adaptable. As demonstrated in, it consists of a set of ports connected to a network of interconnected FC switches through distinct physical lines. A 24-bit address space is organized hierarchically in the switching network or fabric, according to domains and regions.

During the fabric login procedure, which we'll go over later, each associated port is given a unique address. To be accurate, the actual port of attachment on the fabric or switch determines the exact address. The fabric is used to route frames. Based on the target port address in each frame header, the fabric routes each frame separately.

3) The arbitrated loop topology enables the interconnection of three or more ports without the use of fabric. Only two ports can interact with each other on the loop at any given moment due to arbitration.

Resources: https://www.mycloudwiki.com/san/fc-san-topologies/

7.
Based on the advertisement, an ENode chooses a suitable FCF and sends a discovery solicitation, at which point the capability negotiation begins. When the FCF receives the solicitation, it responds to the ENode with a requested discovery advertising that confirms the agreed capabilities. When the ENode receives the requested discovery advertising, it may proceed with establishing a virtual connection to the FCF. The technique is comparable to the FC fabric login procedure. When the login operation is completed successfully, a virtual port on the ENode, a virtual port on the FCF, and a virtual connection between them are created.

8.

a.
The node is recognized with a globally unique iSCSI name that is independent of the node's location or IP address. Many iSCSI nodes may be accessible at the same address, and the same iSCSI node may be accessible at multiple addresses. As a consequence, several TCP connections can be used during a communication session between two iSCSI nodes to obtain better performance.

b.
Because of dependable in-order delivery, atomic retransmission of unacknowledged packets, and congestion control, these properties are critical to SCSI operations.

c.
In terms of supporting the functionality required for SCSI operations, the Stream Control Transmission Protocol is identical to TCP. However, at the time of iSCSI standardization, the SCTP was seen to be too new to be trusted.

d.
Iscsi does not have a way of securing a connection or session. All native iSCSI communication is clear, making it vulnerable to eavesdropping and active assaults. In an untrustworthy environment, iSCSI should be used in conjunction with IPsec.

9.
Connection loyalty is a technique for supporting coordination across many connections. In this scheme, the initiator can give a command over any connection, but all subsequent messages must be sent over the same connection.
It's necessary to keep track of the iSCSI sessions. The iSCSI login mechanism handles a significant portion of session management. The login method results in the creation of a new session or the addition of a connection to an existing session.
The initiator must know the name and address of the storage device, or target, to carry out the process. One way is to pre-configure such information in the initiator. Any subsequent modification will need reconfiguration. A different strategy is based on the location of the service.

10.
The ANSI INCITS 458-201140 access control method is based on the concepts of capability and credential. A client's access privileges to an object, such as read, write, create, or delete, are described by a capability. A credential is simply a cryptographically protected tamper-proof capability comprising a shared key and a keyed-Hash Message Authentication Code (HMAC) 41.

Based on the capability key, the standardized method generates proof. According to the negotiated security approach, the proof is a number computed with the capability key over chosen request components.

11.
The three approaches to block-level virtualization is:

1. The host
2. The network
3. The Storage

Virtualization is handled by a volume manager in the host-based method, which could be part of the operating system. The volume manager is in charge of mapping native blocks into logical volumes and monitoring overall storage consumption.

Virtualization is managed by a particular function in a storage network, which might be part of a switch, in the network-based method. As long as the necessary storage network protocols, such as fc, fcoe, or iscsi, are supported by hosts and storage systems, the technique is transparent. It can be classed as either in-band symmetric or out-of-band asymmetric, depending on how control and application traffic is handled.

Virtualization is managed by the storage system's controller in the storage device-based method. This technique usually yields high performance due to the controller's near proximity to physical storage. Nonetheless, it has the disadvantage of being vendor-specific and difficult (if not impossible) to integrate with heterogeneous storage systems.

Because of its relative openness and flexibility in storage pooling, the network-based technique is best suited for Cloud Computing. Storage can be assigned to VM hosts, who can then allocate the assigned virtual storage to VMs using their own virtualization infrastructure.

Inband Solution: The virtualization function for mapping and I/O redirection is always in the path of both control and application traffic in an in-band method. The virtualization function, however, might become a bottleneck and a single point of failure. Caching and clustering are two typical methods for resolving these issues.

Advantages:
The in-band approach's central point of control makes administration and support for sophisticated storage capabilities like snapshots, replication, and migration much easier.
In Cloud Computing, the snapshot feature is quite useful. It can be used to capture the state of a virtual machine at a certain point in time, as well as the components' run-time circumstances.

Disadvantages: There is a trade-off since when a virtual machine is snapshotted, the performance of other virtual machines on the same host may suffer.

Out of band solution: The virtualization function is in the path of control traffic but not of application traffic, so it's an out-of-band solution. The application traffic is directed by the virtualization function.

Advantages: When compared to the in-band technique, the solution provides superior performance because application traffic may be routed directly to the destination without experiencing any virtualization processing delays.

Disadvantages: This method is not well suited to complex storage features. More importantly, it adds to the host's workload by requiring it to discern between control and application traffic and route it accordingly.

12.
NOR flash is quicker than a hard drive and can address a particular byte at random. It has a low storage density.

Random access is only possible in NAND in units bigger than a byte. NAND flash has made a big impression in consumer electronics, and it's utilized in a lot more digital cameras, portable music players, and smartphones than NOR memory.

13.
The three constraints that prevent NAND flash solid-state devices from being deployed in the cloud

i. A write operation over existing content necessitates that this content is wiped first. As a result, write operations are significantly slower than reading operations.

ii. Erase operations are performed on a block-by-block basis, whereas write operations are performed on a page-by-page basis.

iii. After a certain number of write-erase cycles, memory cells wear out.

14.

Consistent Hashing is a distributed hashing system that assigns each server or item in a distributed hash table a place on an abstract circle, or hash ring, regardless of the number of servers or objects in the table. This permits servers and objects to grow without harming the system's overall performance.

Memcached provides a basic key-value store for storing arbitrary data over a pool of commodity PCs' memory units. On commodity PCs, Memcached provides basic key-value storage for short bits of arbitrary data in DRAM. It's specific to caching, and it's used to allow apps to skip over intensive processes like database queries. Data durability is never considered; each cached item is only valid for a limited time.

Memcached servers are not aware of one another and are not coordinated centrally by design. A client's responsibility is to choose which server to utilize, and the client does so based on the key of the data item to be cached (armed with the information about the servers in use).

s = H(k) mod n, where H(k) is a hashing function, k is the key, n is the number of servers, and s is the server label, to which the remainder of H(k) over n is assigned. The approach

works as long as n is constant, but when the number of servers grows or shrinks dynamically, as it often does in Cloud Computing, it will most likely give a different server. Cache misses abound, as a result, application performance suffers, and all servers in the most recent cluster must be upgraded. The basic algorithm for consistent hashing is shown below.

Map a hash function's range to a circle, with the highest value circling to the lowest value clockwise. Assign each server in the pool a value (i.e., a point on the circle) as its identifier49. Select the server whose identifier is equal to or greater than H to cache a data item of key k. (k). Consistent hashing has an immediate effect on a server's exit or arrival only affecting its close neighbors.

Reference:
https://www.mikeperham.com/2009/01/14/consistent-hashing-in-memcache-client/