

## ISM

### Securing the Storage Infrastructure

Topic I.

#### Storage Security Framework :-

- ① Accountability Service
- ② Confidentiality Service
- ③ Integrity Service
- ④ Availability Service

① Accountability → Refers to accounting for all the events and operations that take place in the data center infrastructure. The accountability service maintains a log of events that can be audited or traced later for purpose of security.

② Confidentiality :- Provides required security secrecy of information and ensures that only authorized user have access to data. It covers both data in transit and data at rest.  
↓  
(data transmitted over cable)  
(stored in storage device)

③ Integrity :- Ensures that information is unaltered. The objective of the service is to detect and protect against unauthorized update and deletion of data. It typically covers both data in transit and data at rest.

④ Availability :- Ensure that authorised user has reliable and timely access to data. These services enable users to access the required computer system, data and applications residing on these systems.

Availability services are also implemented on the common system used to transmit information among computers that may reside at different locations. This ensures availability of information if a failure in one particular location occurs. This service must be implemented for both electrical data & physical data.

~~Topic~~  
II:

Risk Triad :-

→ Threats  
→ Assets  
→ Vulnerability.

Risk Triad defines the risk in terms of threat, assets and vulnerabilities.

\* Risk → Risk arises when an attack seeks to access assets by exploiting an existing vulnerability.

To manage risk, organisation primarily focus on vulnerability because they cannot eliminate threats that appear in various forms and sources to its assets.

Risk Assessment is the first step in determining the extent of potential threats and risks in an IT infrastructure. The process assess risk and helps to identify appropriate control to mitigate or eliminate risks.

## ① Assets :-

Information is one of the most important assets for any organisation. Other assets include hardware, software and other infrastructure components required to access the information. To protect these assets, organisation must develop a set of parameters to ensure the availability of the resources to authorized users and trusted network.

Security method has 2 objective. First objective is to ensure that network is easily accessible to authorized user. Second objective is to make it difficult for potential attackers to access and compromise the system.

The effectiveness of a storage security methodology can be measured by two key criteria :-

- (i) The cost of implementing the system should be fraction of value of protected data.
- (ii) It should cost heavily to a potential attacker in terms of money, effort & time.

## ② Threats :-

Threats are potential attack that can be carried out on a IT infrastructure. Attack is classified as :-

a) Active attack :- Active attack includes data modification, denial of service (DoS), and repudiation attack. They pose threat to data integrity, availability and accountability.

b) Passive attack :- Passive attack are attempt to gain unauthorized access into the system. They pose threat to confidentiality of information.

→ In data modification attack, the unauthorized user attempt to modify information for malicious purposes. A modification attack can target the data at rest or data at transit. These attack pose threat to data integrity.

→ Denial of Service (DoS) attack prevent legitimate user from accessing resources and services. These attack generally do not involve access to or modification of information. They pose threat to data availability.

→ Repudiation is an attack against the accountability of information. It attempt to provide false information by either impersonating someone or denying that an event or a transaction has taken place.

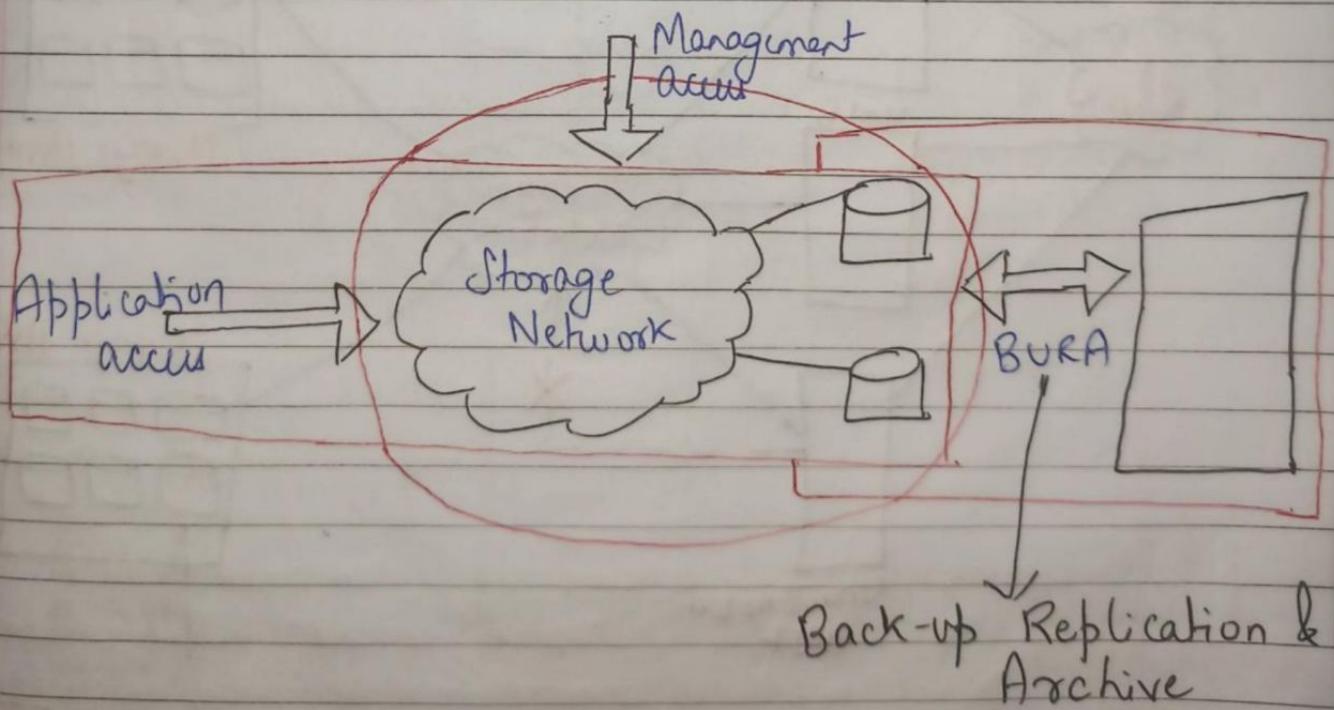
### ③ Vulnerability :-

The paths that provide access to information are often vulnerable to potential attack. Each of the path may contain various access points which provide different level of access to storage resource.

It is important to implement adequate security controls at all the access points on an access path. Implementing security controls at each <sup>access</sup> point of ~~an~~ every access path is known as defense in depth.

Topic  
III:

## Storage Security Domain :-

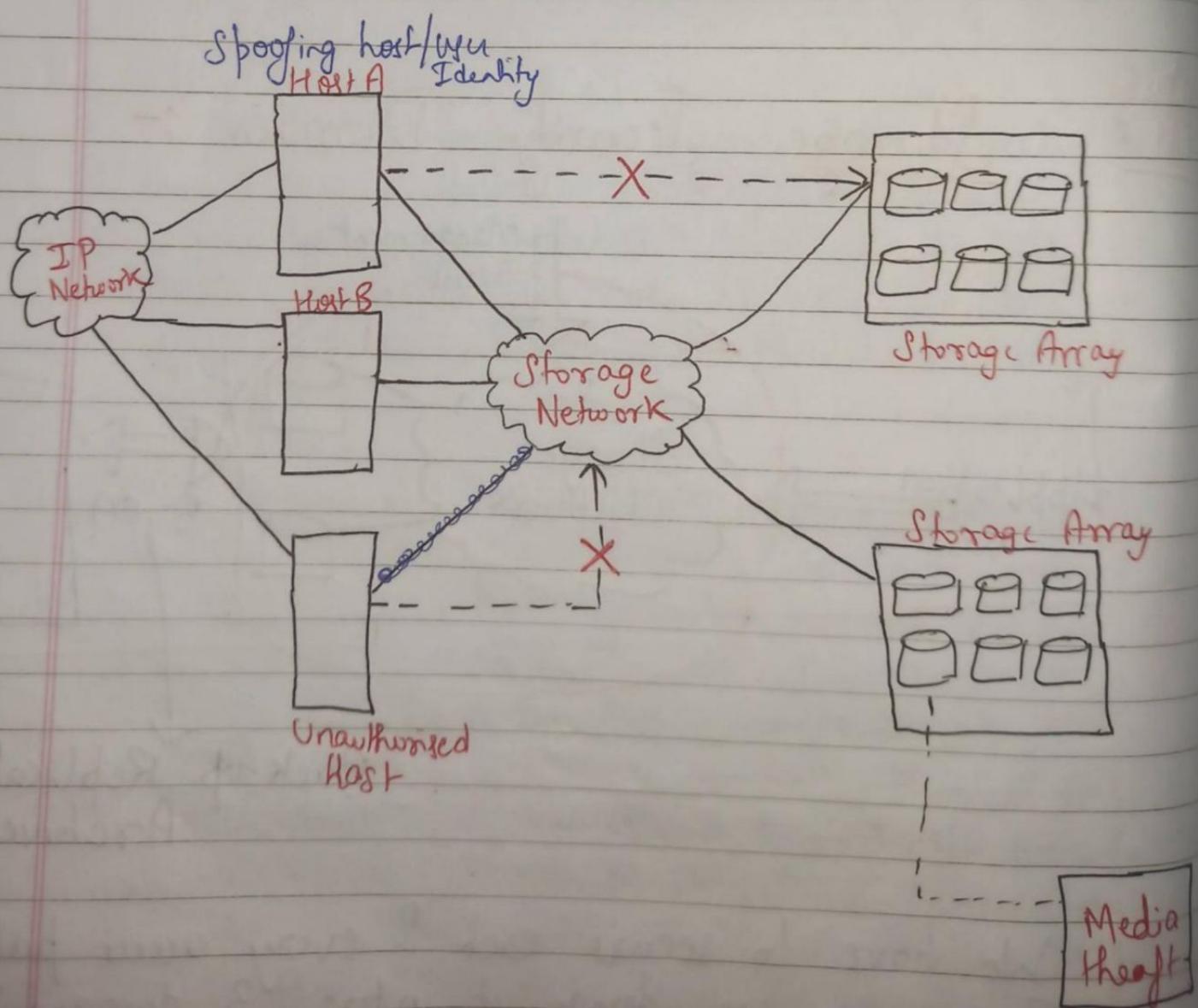


We have to secure each & every access path. To secure we divide it into 3 domains :-

- (i) Application Domains
- (ii) Management Domains
- (iii) BURA

## (i) Securing the Application Access Domain :-

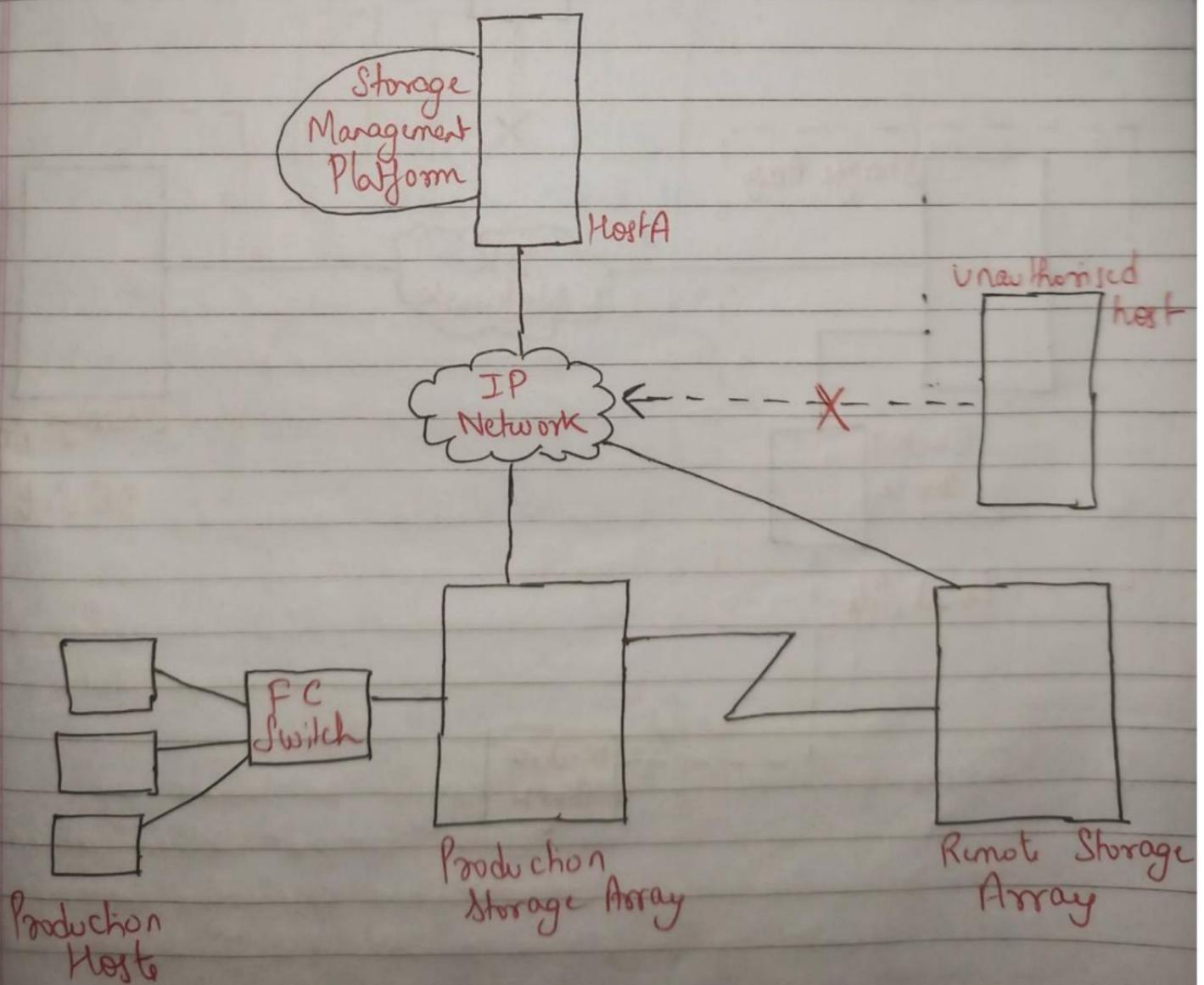
The application access domain may include only those application that access the data through the file system or a database interface.



## (ii) Securing the Management Access Data :-

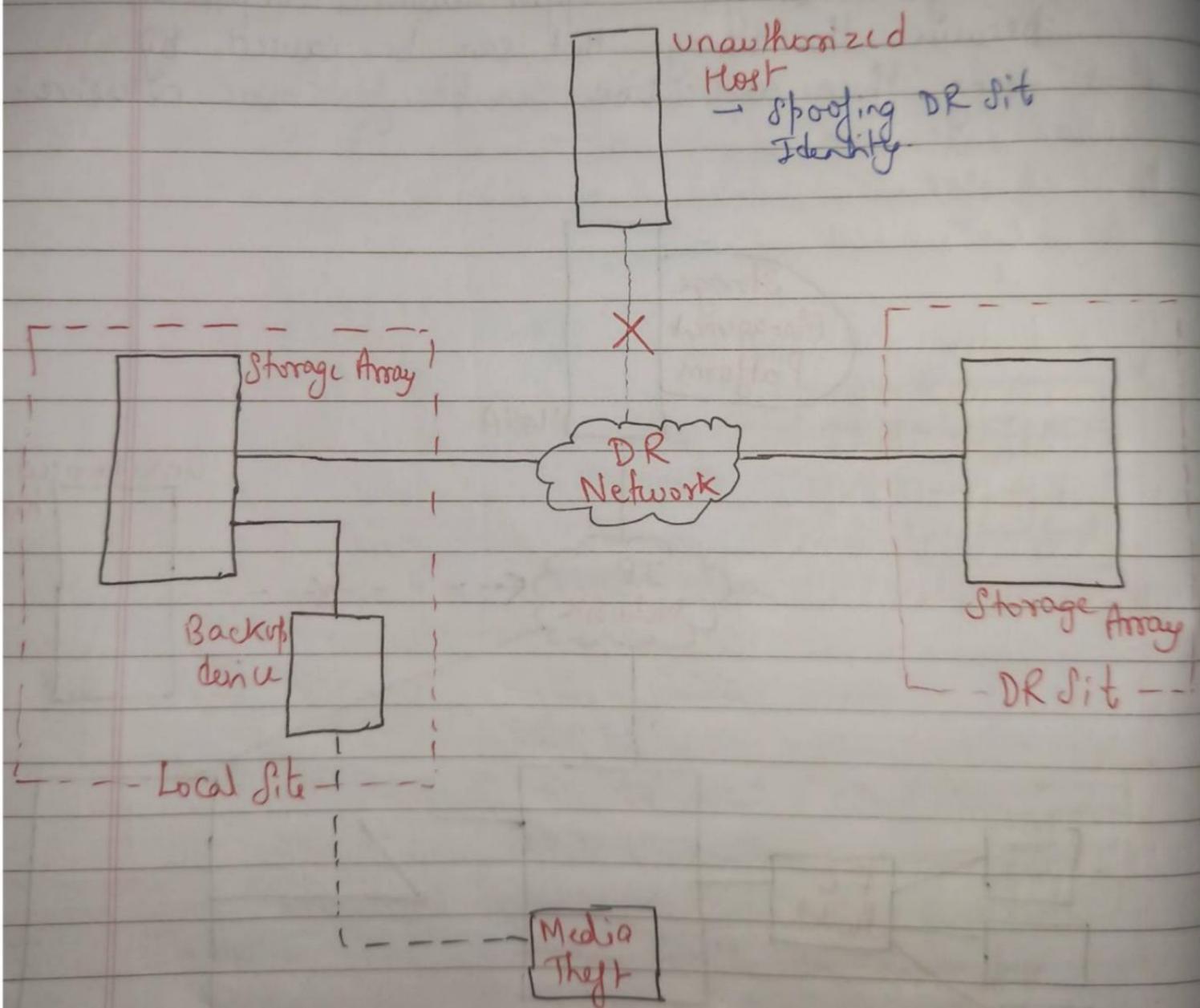
Management access whether monitoring, provisioning, or managing storage resource, is associated with every device within the storage network.

Implementing appropriate controls for securing storage management application is important because the damage that can be caused by using these application can be far more extensive.



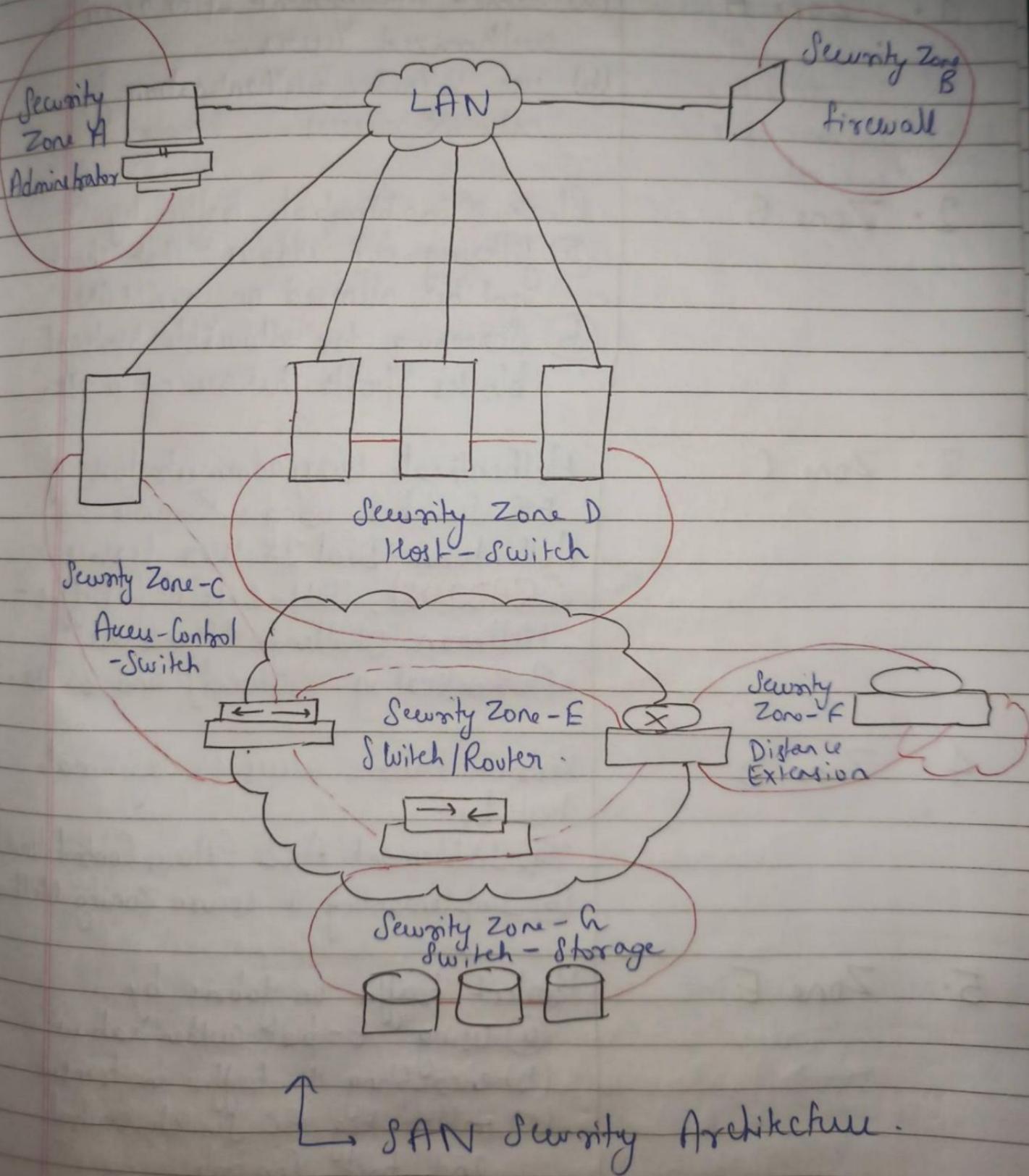
### (iii) Securing Backup, Replication & Archive (BURA) :-

Backup, Replication and Archive is the third domain that needs to be secured against an attack.



Topic  
IV.

## Security Implementations in Storage Network :-



## S.No. Security Zones      Protection Strategies

|           |   |
|-----------|---|
| 1. Zone A | (a) Restrict management LAN access to authorized users.<br>(b) use - 2-factor authentication for network access.  |
| 2. Zone B | Block @ inappropriate traffic by<br>① filtering out address that should not be allowed on your LAN.<br>② Screening for allowable protocol blocks ports that are not in use.                 |
| 3. Zone C | Authenticate users/administrators of FC Switches using Remote Authentication Dial In User Service (RADIUS), DH-CHAP (Diffie-Hellman Challenge Handshake Authentication Protocol) and so on. |
| 4. Zone D | Restrict Fabric access to legitimate host by<br>① Implement ACL (Access Control List)<br>② Implementing a secure Zoning Method  |
| 5. Zone E | Protect traffic on fabric by<br>① Using E-port authentication<br>② encrypting the traffic in transit<br>③ implementing FC Switch control and port control                                   |

6. Zone F

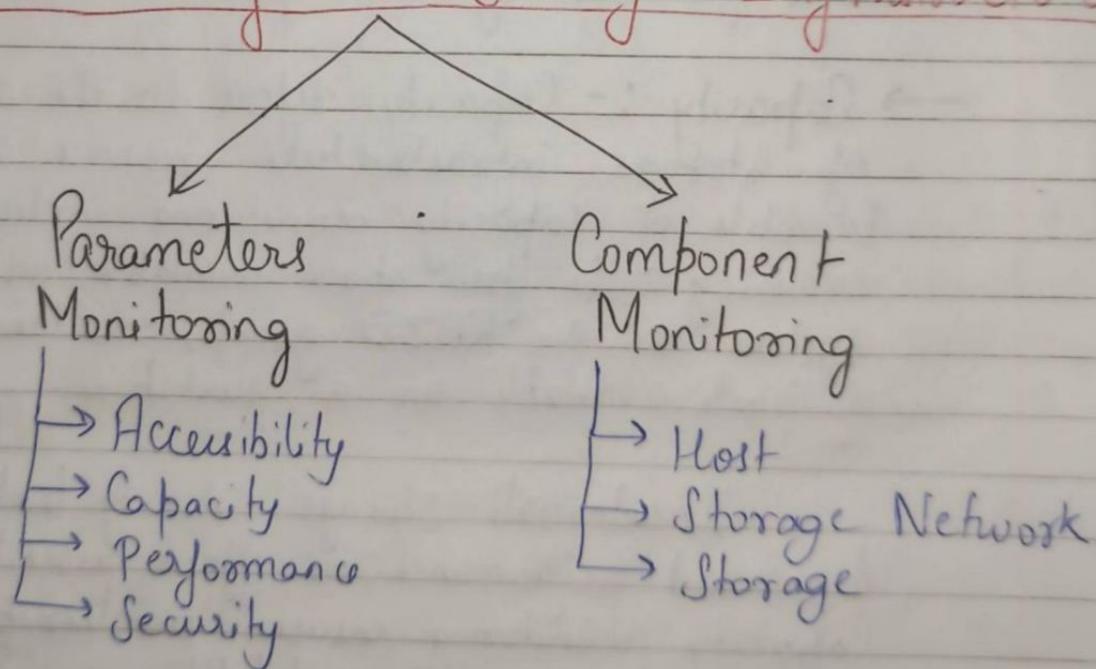
Implementing encryption for in-flight data  
① FC-SP for long distance FC extension  
② IPsec for SAN extension via FCIP.

7. Zone G

Protect the Storage Array on your SAN  
① WWPN-based LUN masking  
② SPI locking

Topic  
①

## Monitoring the Storage Infrastructure :-



\* Monitoring helps to analyze the utilization and consumption of various storage infrastructure resources. This analysis facilitates capacity planning, forecasting, and optimal use of these resources.

\* Monitoring Parameters :- Storage infrastructure components should be monitored for accessibility, capacity, performance and security.

→ Accessibility refers to availability of a component to perform its desired operation during a specified time period. A component is said to be accessible when it is functioning without any fault at any given point in time.

Monitoring hardware and software component for accessibility involves checking their availability status by reviewing the alerts generated by the system.

→ Capacity :- Capacity refers to the amount of storage infrastructure resource available. Example of capacity monitoring includes examining the free space available on a file system or a RAID group, or the number of ports available on a switch.

Inadequate storage capacity leads to degraded performance or effect accessibility. Capacity monitoring ensures uninterrupted data availability and scalability.

→ Performance :- Performance monitoring evaluates how efficiently different storage infrastructure components are performing and helps to identify bottlenecks.

Performance monitoring usually measures and analyzes behaviour in terms of response time or ability to perform at certain predefined levels.

→ Security :- Monitoring a storage infrastructure for security helps to track and prevent unauthorized access and login failures, whether accidental or malicious.

Security monitoring helps to track unauthorized configuration changes to storage infrastructure resources.

### \* Components Monitored :-

Host, network, and storage are components within the storage environment that should be monitored for accessibility, capacity, performance and security.

#### Host :-

The accessibility of a host depends on the availability status of hardware components and software processes running on it. For example, a host's NIC failure might cause inaccessibility of host to its user.

File system utilization of host also needs to be monitored. Monitoring helps estimate the file system's growth rate and predict when it will reach 100%.

Accordingly, the administrator can extend the file system space proactively to prevent application outage.

Server performance mainly depend on Input/Output profile, utilization of CPU and memory. For example, if a server running an application is experiencing 80% of CPU utilization continuously, it indicates that server may be running out of processing power which can lead to degraded performance and slower response time.

Administrator can take several action to correct the problem such as upgrading or adding more processor and shifting the workload to different servers.

Security monitoring on server involves tracking of login failures and execution of unauthorized application or software process.

## Storage Network :-

Storage Network need to be monitored to ensure uninterrupted communication between the server and the storage array. Uninterrupted access to data over the storage network depends on the accessibility of the physical and logical component of the storage network.

The physical component of storage network includes switches, ports and cables. Logical component includes constructs such as zones. Any failure in physical & logical component may cause data unavailability.

Capacity monitoring in storage network involves monitoring the availability of port in the switch, the no. of available port in entire fabric, individual port and each interconnect device in fabric.

Monitoring the performance of storage network enables assessing individual component performance and helps to identify network bottleneck. For example, heavily used ports can cause queuing delays on the server.

Security in Storage Network provides information for any unauthorized change to the configuration of a fabric. Login failures, and unauthorized access to switches for performing administrative changes should be logged and monitored continuously.

### Storage :-

The availability of the storage array should be monitored for its hardware components and its various processes. For example, failure of a replication task affect disaster recovery capability.

Capacity monitoring of a storage array enables the administrator to respond to storage needs as they occur.

A storage array can be monitored by using a number of performance metrics such as utilization rate of various storage array components, I/O response time, and cache utilization.

Monitoring security helps to track unauthorized configuration of the storage array and ensures that only authorized users are allowed to access it.

## Topic VI

## Storage Infrastructure Management Activities

The key storage infrastructure management activities performed in a data center can be broadly classified as :-

- (i) Availability Management
- (ii) Capacity Management
- (iii) Performance Management
- (iv) Security Management
- (v) Reporting.

(i) Availability Management :- A critical task in availability management is establishing a proper guidelines based on defined service levels to ensure availability.

Availability management involves all availability related issue for component or service to ensure that service levels are met.

A key activity in activity management is to provision redundancy at all levels, including component, data, or user sites.

### (ii) Capacity Management :-

- Goal :- ensure adequate availability of resources based on their service level requirements.
- involves optimization of capacity based on cost & future needs.
- provide capacity analysis that compare allocated space to forecast space.
- provide trend analysis based on rate of consumption.

### (iii) Performance Management :- Ensures the optimal operational efficiency of all components. Performance analysis is an important activity that helps to identify the performance of storage infrastructure components.

### (iv) Security Management :- Key objective is to ensure confidentiality, integrity and availability of information in both virtualized and non-virtualized environments. Prevent unauthorized access.

(v) Reporting :- involves keeping track and gathering information from various component and process.

This information is compiled to form a reports for trend analysis, capacity planning, chargeback, and performance.

Capacity planning reports contain current & historic information about utilization of storage, file system, database tablespace, port, etc.

Chargeback reports contain information about allocation or utilization of storage infrastructure components.

Performance reports provide details about the performance of various storage infrastructure components.

## 6 Storage Management Activities

### 7 Authentication, Authorization & Kerberos in NAS environment:

- NAS is open to multiple exploits, including viruses, unauthorized access & data tampering.
- Permissions and ACLs (access control lists) are deployed over form the 1<sup>st</sup> level of protection to NAS resources by restricting accessibility and sharing.

### \* NAS File sharing : Authentication and Authorization

- In a file sharing environment, NAS devices use standard file-sharing protocols - NFS & CIFS.
- Therefore, authentication & authorization are implemented & supported on NAS devices same as in a unix or windows file sharing environment.

#### → Authentication :

- Authentication requires verifying the identity of a network user and therefore involves a login credential lookup on a network information system (NIS) server in a unix environment.

- Similarly, a windows client is authenticated by a windows domain controller that houses the Active Directory.

- NAS devices uses same authentication technique to validate network user credentials.

## → Authorization :-

- defines user privileges in a network
- UNIX uses mode bits to define access rights granted to owners, groups & other users
- Windows uses an ACL (Access Control List) to allow or deny specific rights to a particular user for a particular file.

## \* KERBEROS :-

- Kerberos is a network authentication protocol, which is designed to provide strong authentication for client / server applications by using secret-key cryptography.
- It uses cryptography so that a client and server can perceive their identity to each other across an insecure network connection.
- In Kerberos, authentication occurs b/w clients & servers.
- The client gets a ticket for a service and the server decrypts this ticket by using its secret key.
- An user, or host that gets a service ticket for a Kerberos service is called a Kerberos client.
- The term Kerberos generally refers to the Key Distribution Center (KDC).
- The KDC implements the authentication service (AS) and the Ticket Granting Service (TGS).
- KDC has a copy of every password associated with every principal, so it is absolutely vital that KDC remains secure.