Unit 3

Storage & Security Management

Dr. Dilip Kumar Kothari
dilip.kothari@ganpatuniversity.ac.in

Ganpat University
॥ विद्यया समाजोत्कर्षः ॥

What is data storage? and its need?

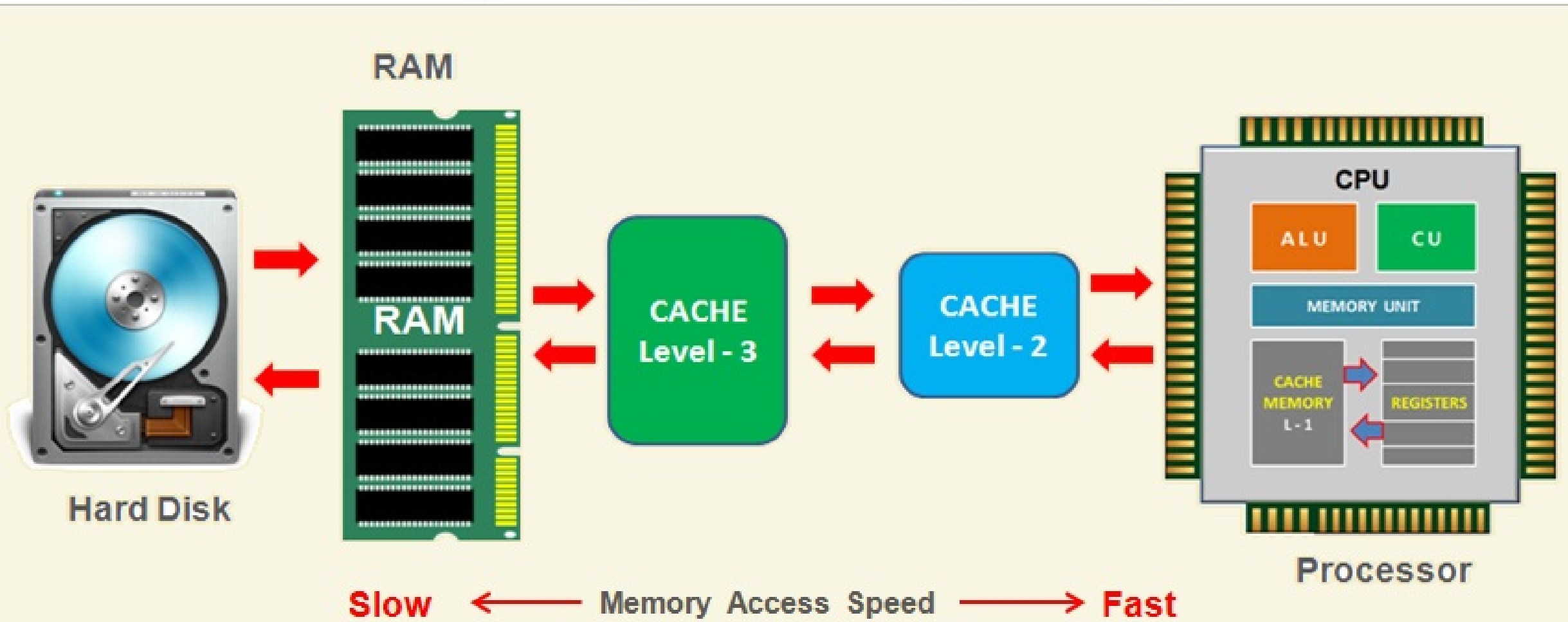
- An storage are (memory) that electronically holds program(s) and data and allow computer to access it easily
- Provides one major function of information retention in a computer system
- Types of Storage

  a) Primary : a form of semiconductor storage, known as Random Access Memory (RAM)
  - volatile
  - small capacity
  - faster access time

  b) Secondary memory: holds the information on other media like hard disk, and tapes,
  - a form of magnetic storage
  - non-volatile
  - huge capacity; mass storage
  - slower access time

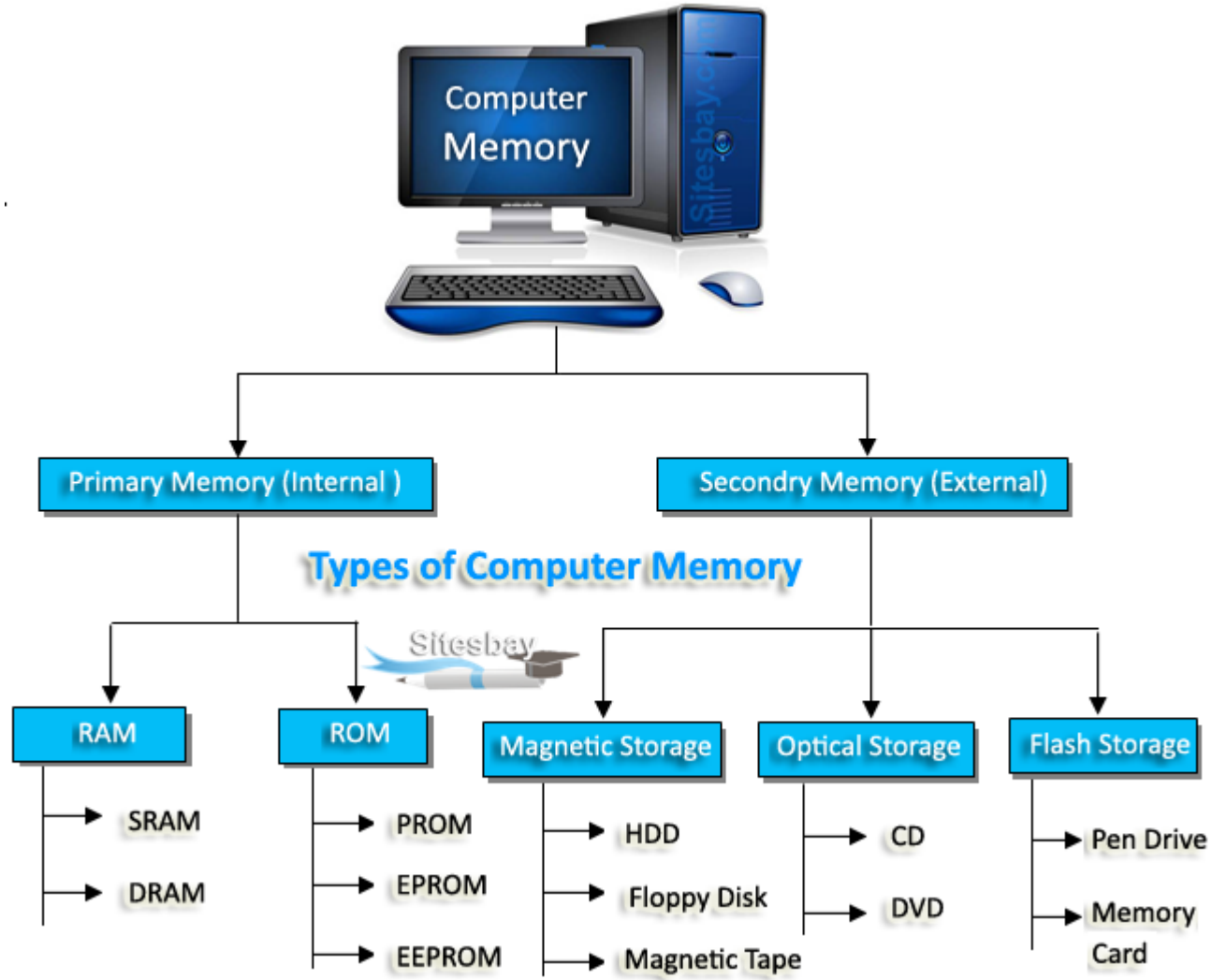
Storage units: bit/byte/Kilobyte/Megabytes/Gigabytes/Terabytes

Computer System Memory Hierarchy



www.learncomputerscienceonline.com

Primary and Secondary Memory in Computer



Removable or off-line storage

- Offline storage, also often called offline backup or removable storage,
  - a type of storage that is kept away from your network
  - a device that is not under the control of a processing unit.
  - the medium is recorded, usually in a secondary storage device, and then physically removed or disconnected

- In order to access stored data, storage devices (flash drives, hard drives, etc.) have to be manually inserted into the system.

- This way of keeping a copy of your data is a good security practice:
  - if anything happens to your data, you can use the offline copy to restore the lost files.

- Most common forms: tape media, optical media, virtual optical media

Tertiary Storage

- Widely employed for offsite storage or for the long-term retention of of data that are rarely accessed
- Often slower and less expensive than primary and secondary storage
- Frequently used for data archiving and long-term storage
- Tape libraries, optical jukeboxes, and cloud storage are a few examples of tertiary storage systems
  - Data is kept on magnetic tapes, which are affordable, and long-lasting, but slower
  - optical jukeboxes are faster than tape libraries but have a shorter lifespan CDs and DVDs
  - Data storage on remote servers that are maintained by a third party and are accessible online is referred to as “cloud storage.”

Tape Library is a example of tertiary memory which can store immense amount of data ranging from 20 terabytes to 2.1 exabytes

- ✓ It involves a robotic mechanism for mount and dismount the removable storage
- ✓ This data is copied to secondary storage before its use
- ✓ When a computer needs to fetch information from the TS, it consults a catalogue to determine which tape or disc contains that information
- ✓ Then computer issues a command for robotic arm to fetch that medium and place it in a drive
- ✓ Once the computer has finished reading the information, arm is controlled again to return the medium back to the library

Storage Management :

- The goal is to define, maintain and track data and data resources
- To take care of operation and maintenance aspects of storage media
- Includes
  - Selecting storage media
  - Maintaining storage media
  - Performing backups and restoration processes
  - Deals with storage of both on-site and off-site data storage for data restoration and historical archiving
  - Maintain physical security of archives and backups
  - Thus increasing business continuity and reducing the risk of data loss

Backup and Storage

- **Storage, backup and service recovery management covers all aspects** of information storage and data restoration
  - ✓Storage management
  - ✓Storage allocation
  - ✓System back-ups and restoration
  - ✓Information management
  - ✓Data base management and
  - ✓Administration
- **Backup**:
  - Process of periodically saving data in some device other than its own hard disk,
  - Need some planning and strategy
    - ✓ Method of backup
    - ✓ periodicity
    - ✓ Potential retrieval
    - ✓ Storage medium
    - ✓ Type of information
    - ✓ Defined policies
    - ✓ Life span of back up information

Storage management and data recovery

- **Key operations of storage management**
  - ✓Data storing
  - ✓Data Backup: proper storing of data
  - ✓Data restoration and recovery: as per business needs
  - ✓Storage resources management:
    formatting, loaded with proper file system installed, checks for removable media
- **Data recovery process: against natural and man-made disasters**
  - ✓ Restoring data to the state as it was earlier
  - ✓ Performed in case of data loss
  - ✓ Requires proper planning and execution

Backup and restore policies

- **Require prior to storage management : Define and agree various policies**
  - ✓Storage resources management:
    formatting, loaded with proper file system installed, checks for removable media
  - ✓Management issues: **Monitoring storage resources** to meet criteria's
    - Availability
    - Capacity
    - Performance requirements
    - Security

Note: To be discussed further

Archive and retrieve

- **Archive**: Maintaining all the different versions of the file in a manner that these are accessible at all times
- **Difference between backup and archive**
  - ✓ In archiving, individual file has to be selected to go into the archive which is not the case with a backup
  - ✓ Also archive suggests an inherent value in the data to be secured
- **Factors to be considered before archiving**

✓ **User Account**: The same user (account) which used to do archiving is allowed to see the file in the archive and retrieve if required

✓ **Archive file deletion**: care must be taken as once deleted, file will no more be available in the archive

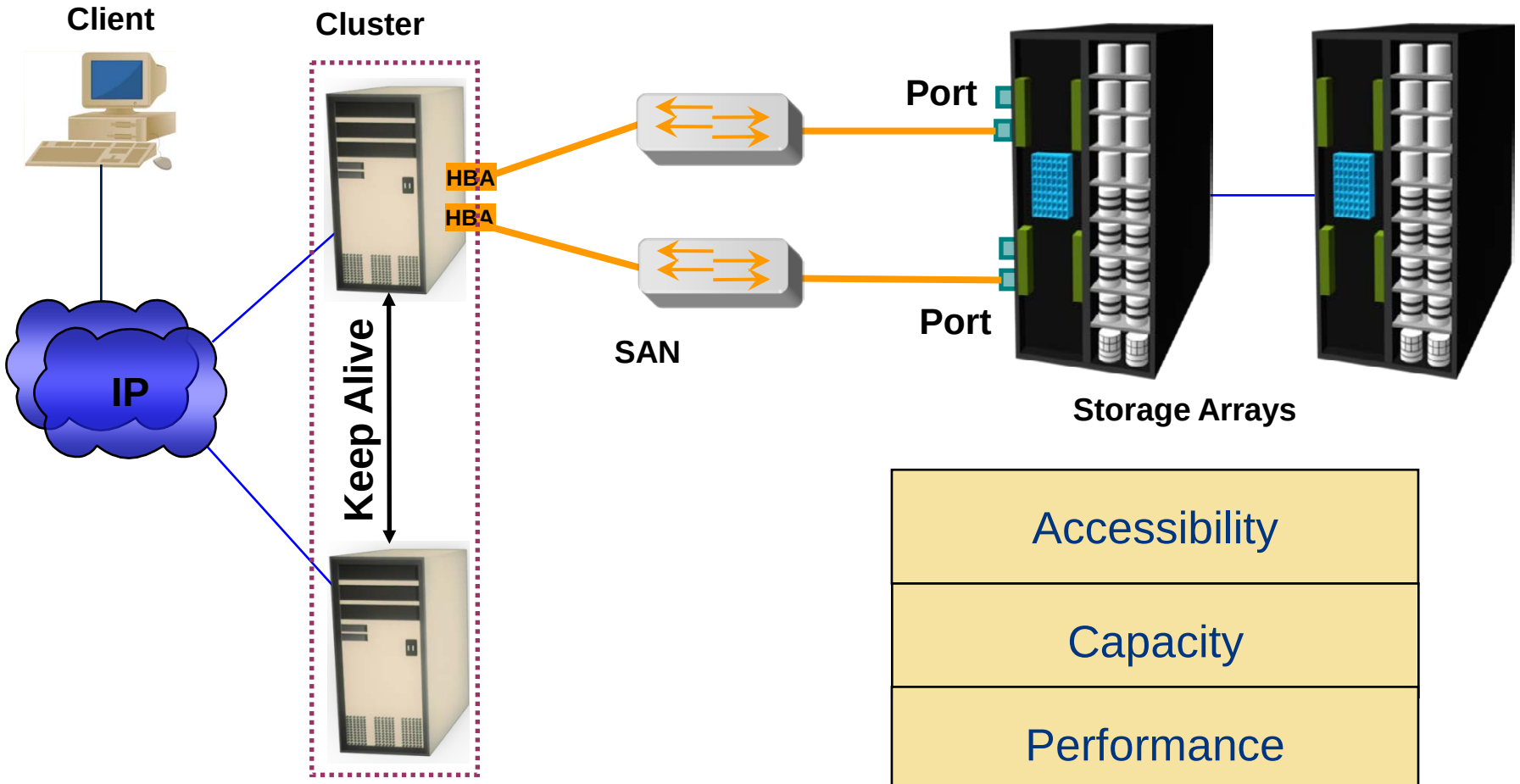
✓ **Local file deletion**: Allow deletion of all the local files immediately on successful archival to the server

✓ **Archive file identification**: if backup at the client side, location of the file has to be identifies as local directory/folder path (additionally README or INDEX file may be added to get date and time recording of the file archival

Storage Infrastructure Management :

- Managing storage infrastructure is a key to ensure continuity of business
- Establishing management processes and implementing appropriate tools is essential to meeting service levels proactively
- Management activities include availability, capacity, performance, and security management
- Monitoring is the most important aspects that forms the basis for storage management
- Continuous monitoring enables availability and scalability by taking proactive measures

Monitoring Storage Infrastructure



- Accessibility
- Capacity
- Performance
- Security

Terminologies :

- A host bus adapter (HBA): a circuit board or integrated circuit adapter that connects a host system, such as a server, to a storage or network device.
- A storage area network (SAN): a dedicated high-speed network or subnetwork that interconnects and presents shared pools of storage devices to multiple servers.
- A storage array, also called a disk array, is a data storage system for block-based storage, file-based storage, or object storage.
  - ✓ Rather than store data on a server, storage arrays use multiple drives in a collection capable of storing a huge amount of data, managed by a central management system.

Parameters Monitored – Accessibility :

- Accessibility refers to the availability of a component to perform a desired operation
- **Why monitor accessibility of different components?**
  - Failure of any hardware/software component can lead to outage of a number of different components
  - Example: HBA failure could cause degraded access to a number of devices in multi-path environment or loss of data access in single path environment
- **Monitoring accessibility involves**
  - Checking availability status of the hardware or software components through predefined alerts

Parameters Monitored – Capacity :

- Capacity refers to the amount of storage infrastructure resources available.

- **Why monitor capacity?**
  - Capacity monitoring prevents outages before they can occur
    - ✓ Inadequate capacity may lead to degraded performance or affect application/service availability
  - More preventive and predictive in nature
    - ✓ Report indicates 90% of all the ports have been utilized in SAN, a new switch must be added if more arrays/servers are to be added

Parameters Monitored – Performance :

- Performance monitoring evaluates how efficiently different components are performing
- **Why monitor Performance metrics?**
  - Want all data center components to work efficiently/optimally
  - Helps to identify performance bottlenecks
  - Measures and analyzes the ability to perform at a certain predefined level
- **Examples**
  - Number of I/Os to disks
  - Application response time
  - Network utilization
  - Server CPU utilization

Parameters Monitored – Security :

- Monitoring security helps to track and prevent unauthorized access
- **Why monitor security?**
  - Need to be protected for confidentiality, integrity and availability
  - To meet regulatory compliance
- Examples
  - Tracking and reporting changes made to zoning configurations
  - Physical security through badge readers, scanners and cameras

Monitoring Environmental parameters

–Temperature, humidity, airflow, hazards (water, smoke, etc.)

–Voltage – power supply

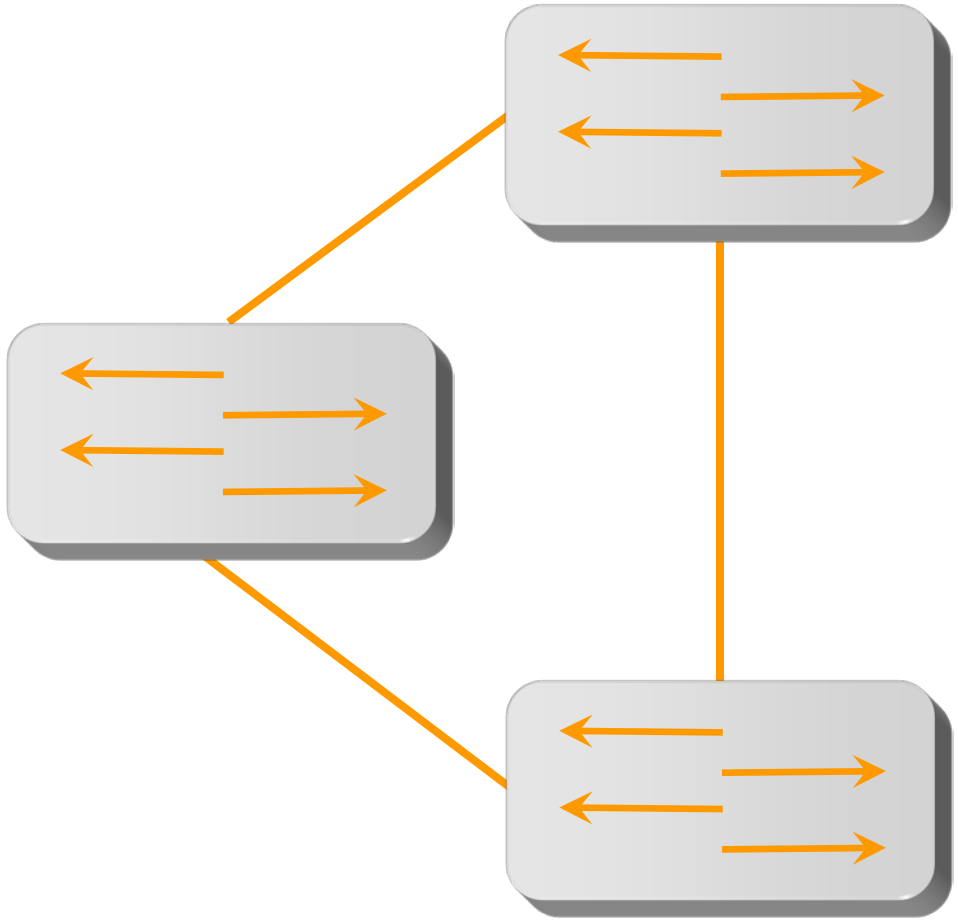
Monitoring Hosts :

- Accessibility
  - Hardware components: HBA, NIC, graphic card, internal disk
  - Status of various processes/applications
- Capacity
  - File system utilization
  - Database: Table space/log space utilization
  - User quota
- Performance
  - CPU and memory utilization
  - Transaction response times
- Security
  - Login and authorization
  - Physical security (Data center access)

Host

Monitoring SAN :

- Accessibility
  - Fabric errors, zoning errors, GBIC failure
  - Device status/attribute change
  - Processor cards, fans, power supplies
- Capacity
  - ISL (inter-switch link) and port utilization
- Performance
  - ✓ Connectivity ports
    - Link failures, loss of signal, link utilization
  - ✓ Connectivity devices
    - Port statistics
- Security
  - ✓ Zoning and LUN Masking
  - ✓ Administrative tasks and physical security
    - Authorized access, strict passwords



LUN Masking:

- A logical unit number (LUN) is a unique identifier that is used when allocating physical storage.
- A LUN can reference an entire RAID group, a single drive or partition, or multiple drives or partitions.
- A LUN is used by a transport protocol associated with an SCSI, iSCSI, Fibre Channel (FC) or similar interface.
- LUNs are central to the management of block storage arrays shared over a SAN.

LUN Masking:

- LUN masking is an authorization mechanism used in storage area networks (SANs) to make LUNs available to some hosts but unavailable to other hosts.

- LUN masking is typically implemented at the host bus adapter (HBA) level on the servers accessing the SAN's storage systems, although some storage controllers also support LUN masking.

- When LUN masking is configured, a host can see only the LUNs that have been assigned to that host and cannot see or access any other LUNs.

LUN Masking:

- Without LUN masking, a host connected to a SAN can see all available LUNs and, in some cases, take actions that might not be desired.

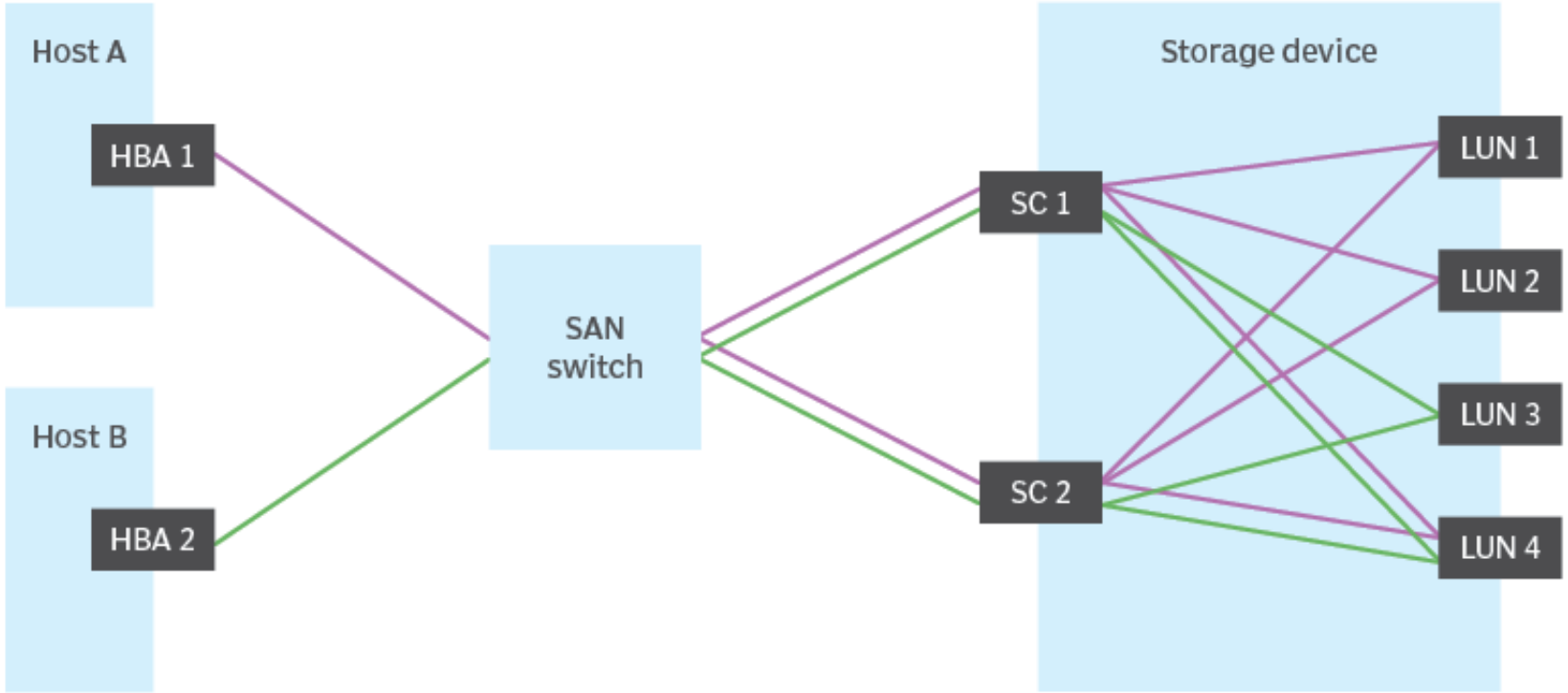
- For example, a Windows server might inadvertently corrupt non-Windows storage by trying to write volume labels to them.

- LUN masking makes it possible to prevent the server from accessing or even seeing those non-Windows LUNs.

LUN Masking:

- LUN masking subdivides access to a given port. Then, even if multiple LUNs are available through the same port, the LUN masks can be set to limit the host's access to specific LUNs.

- For example, the following illustration shows a storage device with four available LUNs and two hosts, each configured with an HBA.



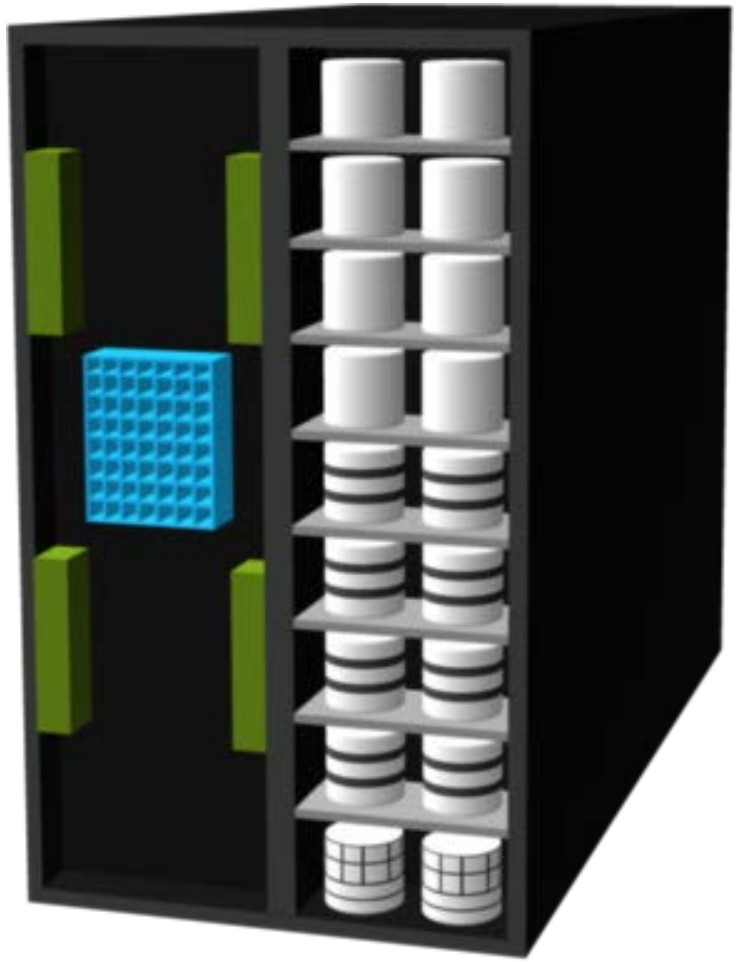
Host A contains HBA 1 and Host B contains HBA 2. Each HBA connects to the SAN switch, which in turn connects to the two storage controllers (SC 1 and SC 2). Without masking, both HBAs would have access to all four LUNs. In this case, however, LUN masking has been applied at the HBA level so that Host A can access only LUN 1, LUN 2 and LUN 4, and Host B can access only LUN 3 and LUN 4.

LUN Zoning:

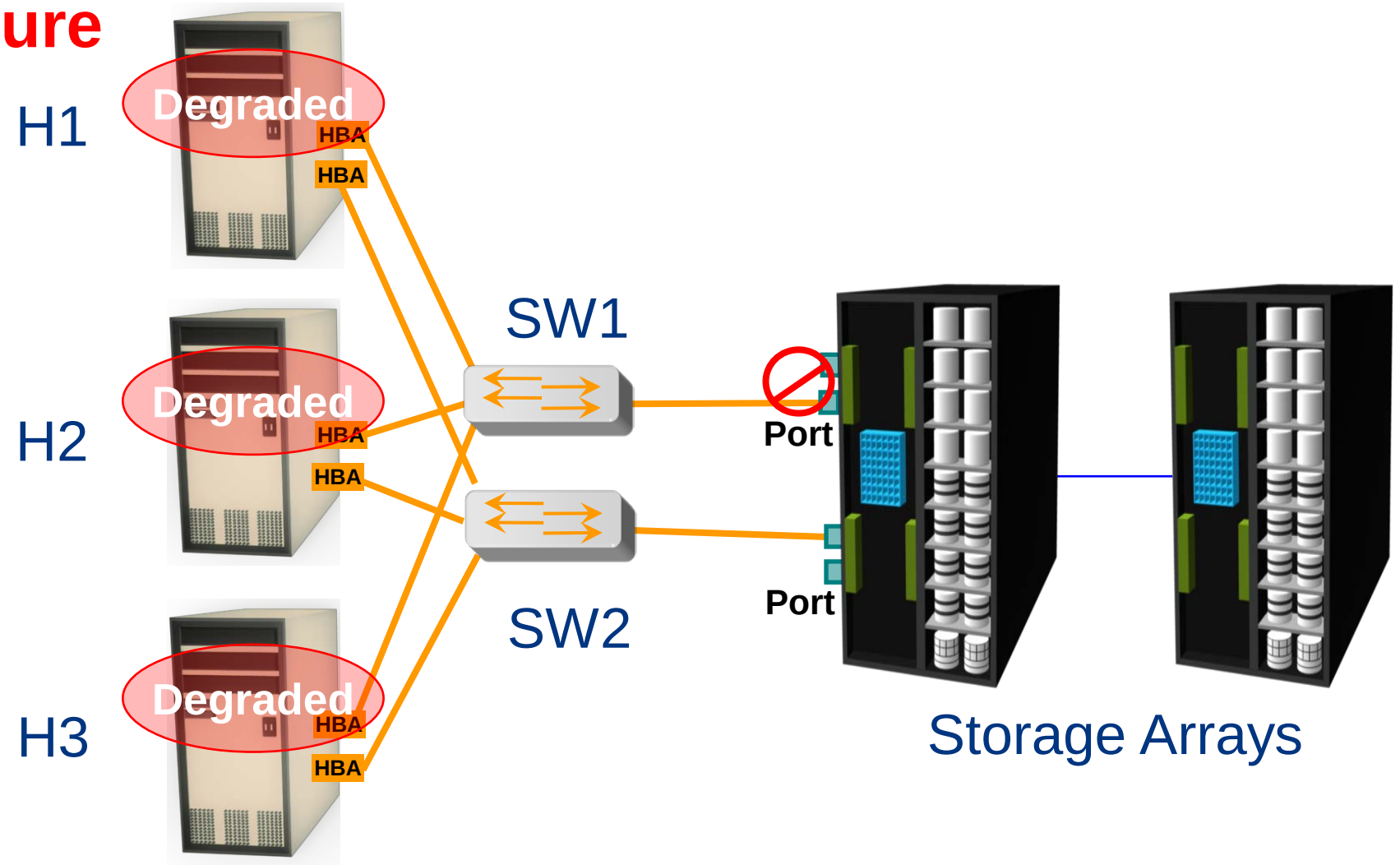
- LUN masking can be a useful tool for controlling server access to specific LUNs, but it offers only limited security protection because it is still possible for the HBAs to be compromised, leaving the SAN infrastructure vulnerable.
- For this reason, most SAN deployments also implement **zoning** and other mechanisms to provide additional levels of protection, relying on LUN masking primarily to protect against potential server issues.

Monitoring Storage Arrays :

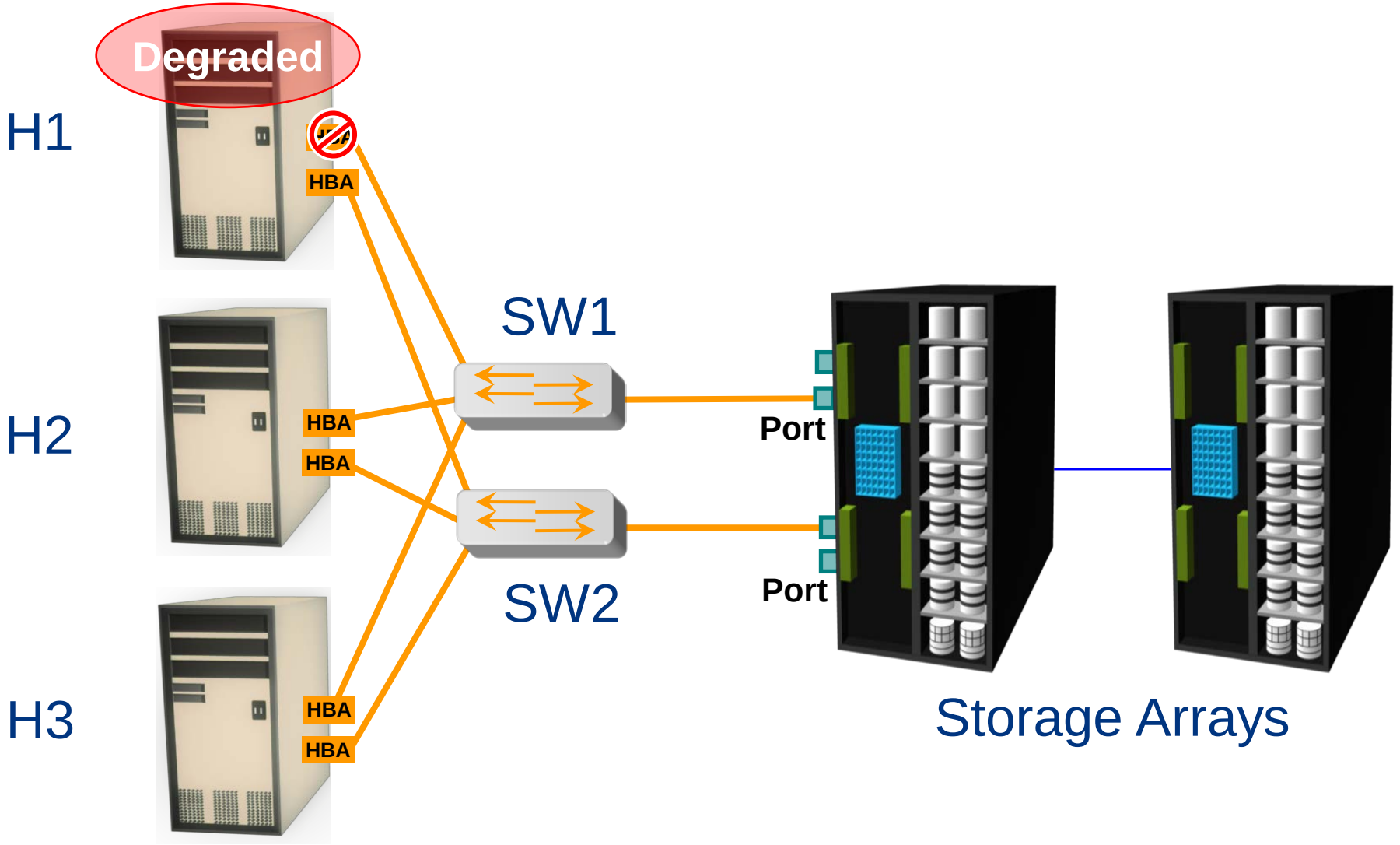
- Accessibility
  - ✓ All Hardware components
  - ✓ Array Operating Environment
    - RAID processes
    - Environmental sensors
    - Replication processes
- Capacity
  - Configured/un-configured capacity
  - Allocated/unallocated storage
  - Fan-in/fan-out ratios
- Performance
  - FE (front-end) and BE (back-end) utilization/throughput
  - I/O profile, response time, cache metrics
- Security
  - Physical and administrative security



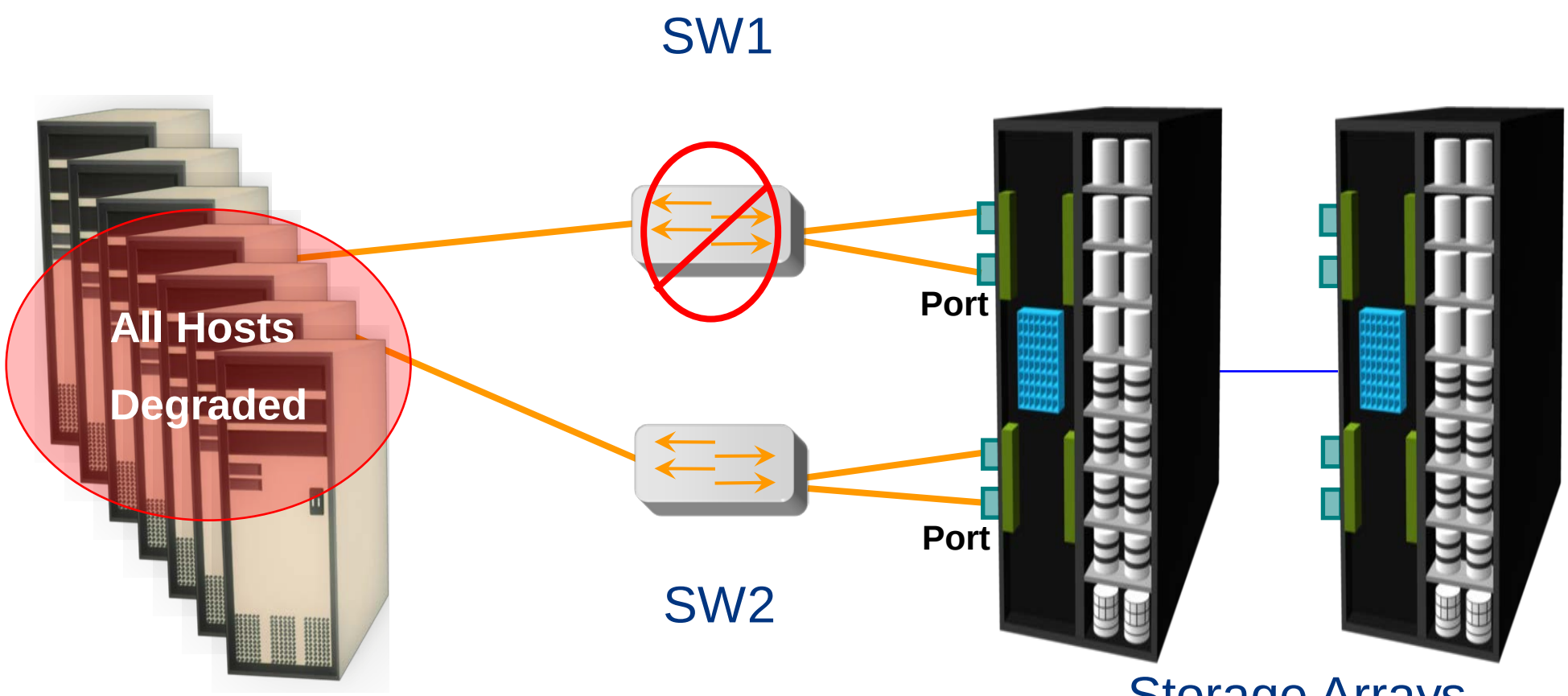
Accessibility Monitoring Example: Array Port Failure



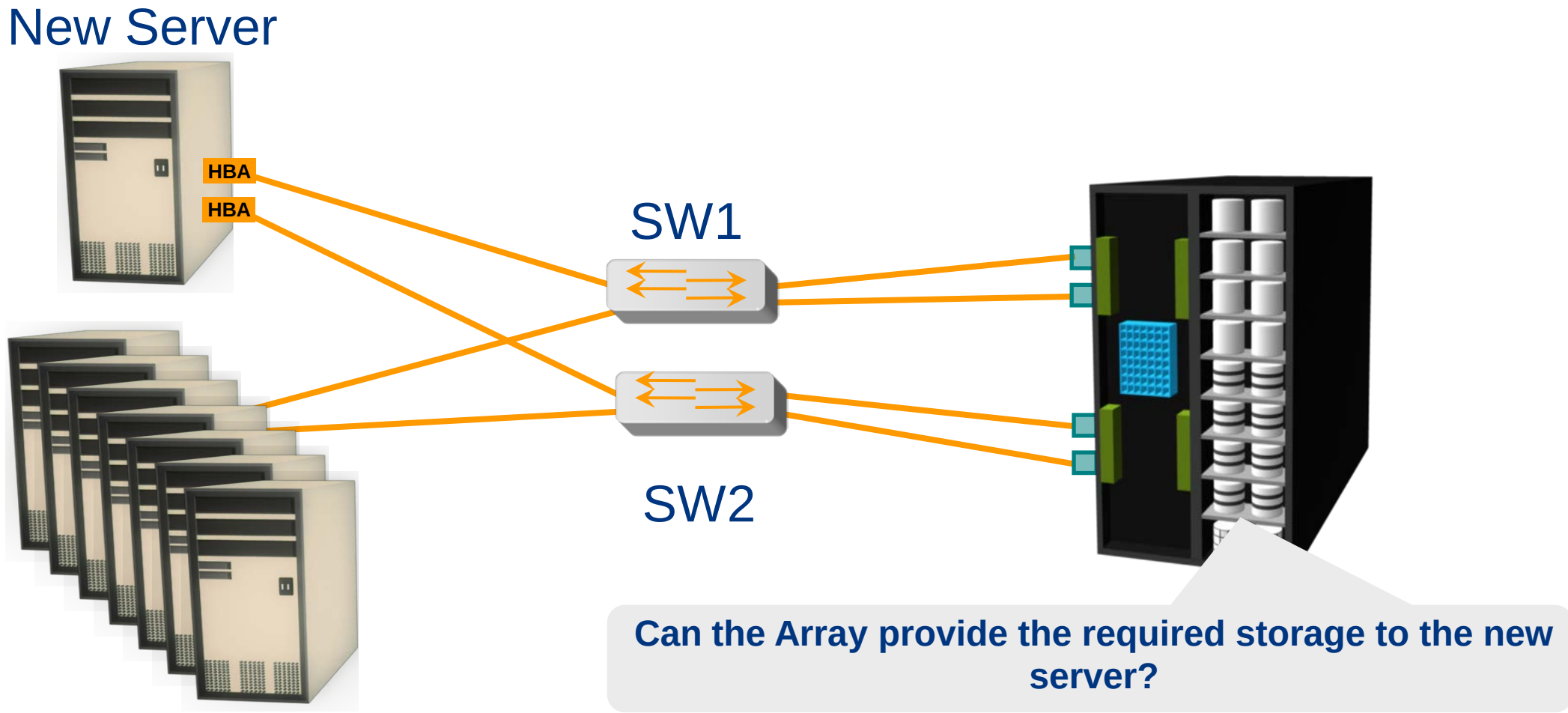
Accessibility Monitoring Example: HBA Failure



Accessibility Monitoring Example: Switch Failure

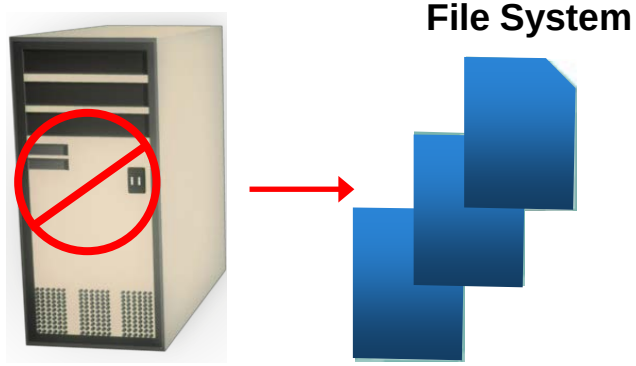


Capacity Monitoring Example: Storage Array

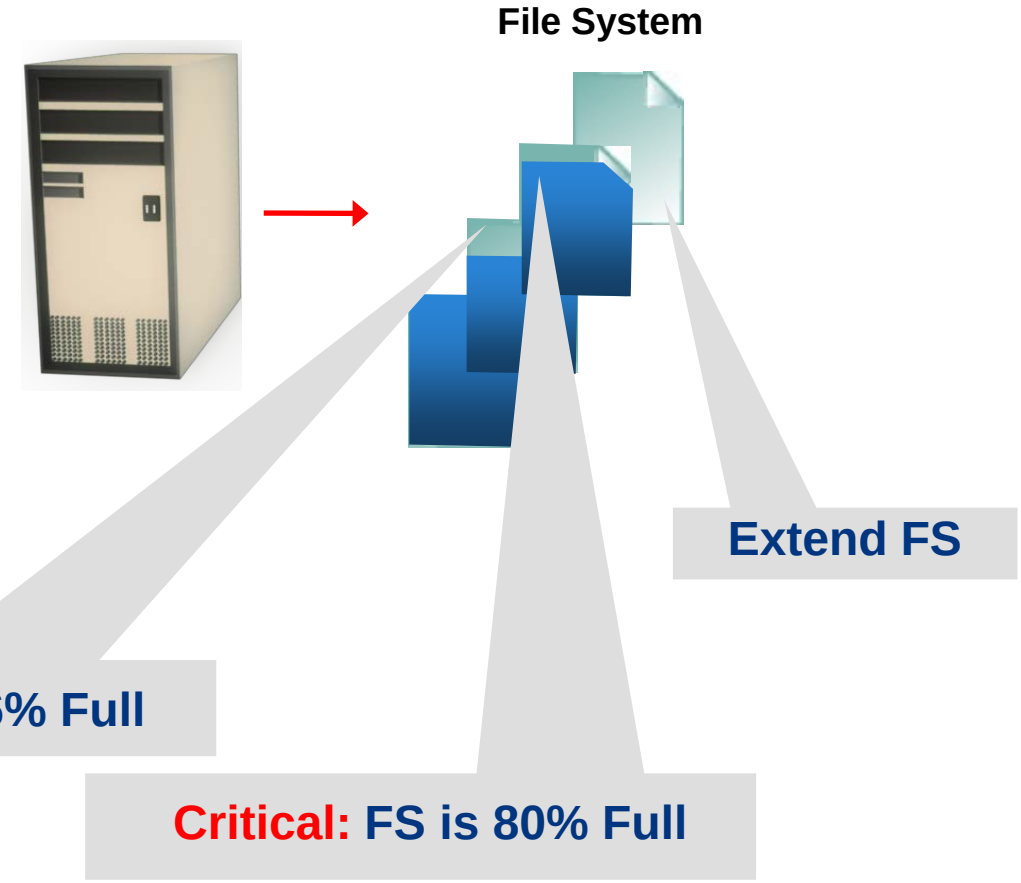


Capacity Monitoring Example: File System Space

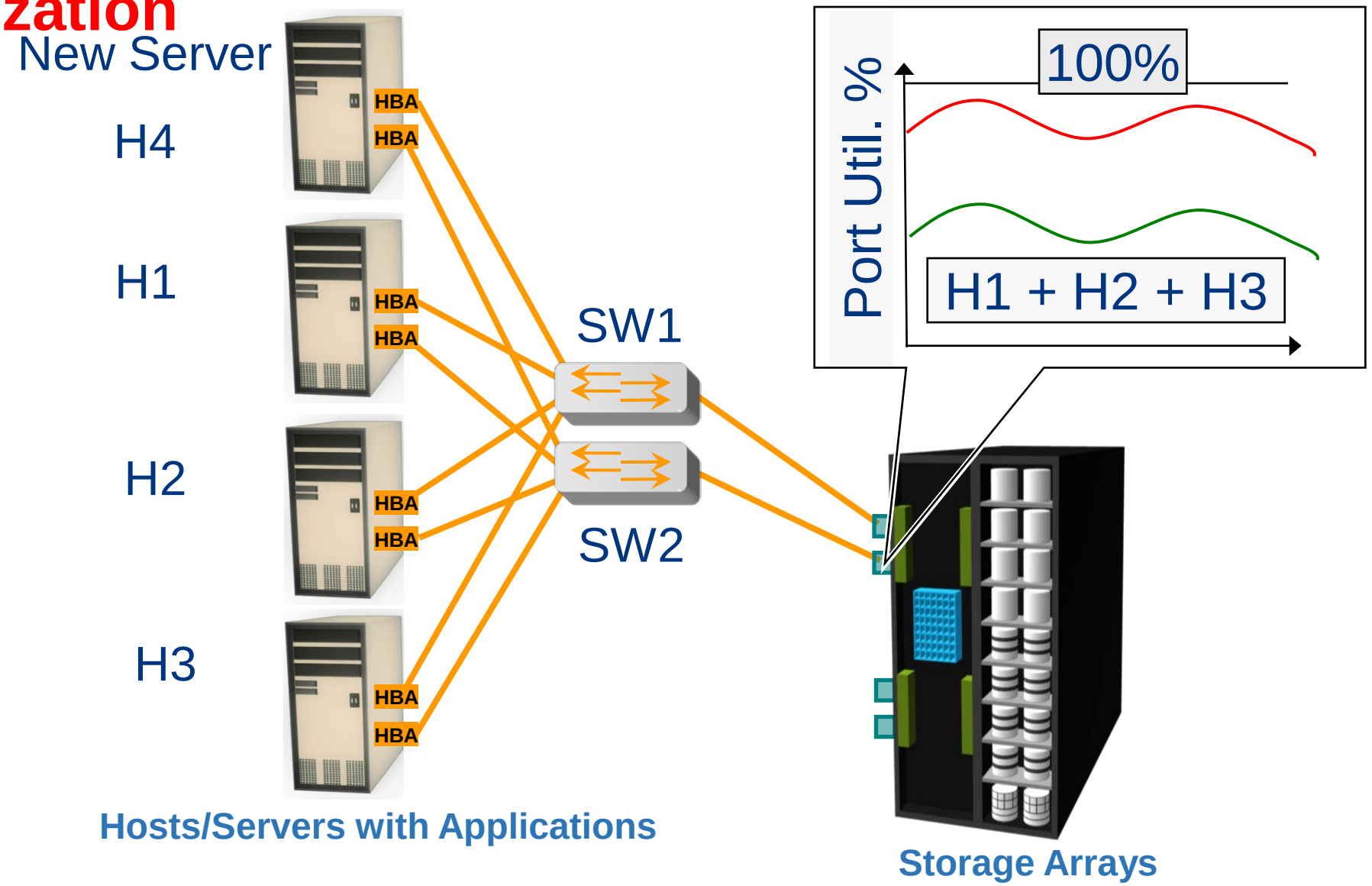
No Monitoring



FS Monitoring

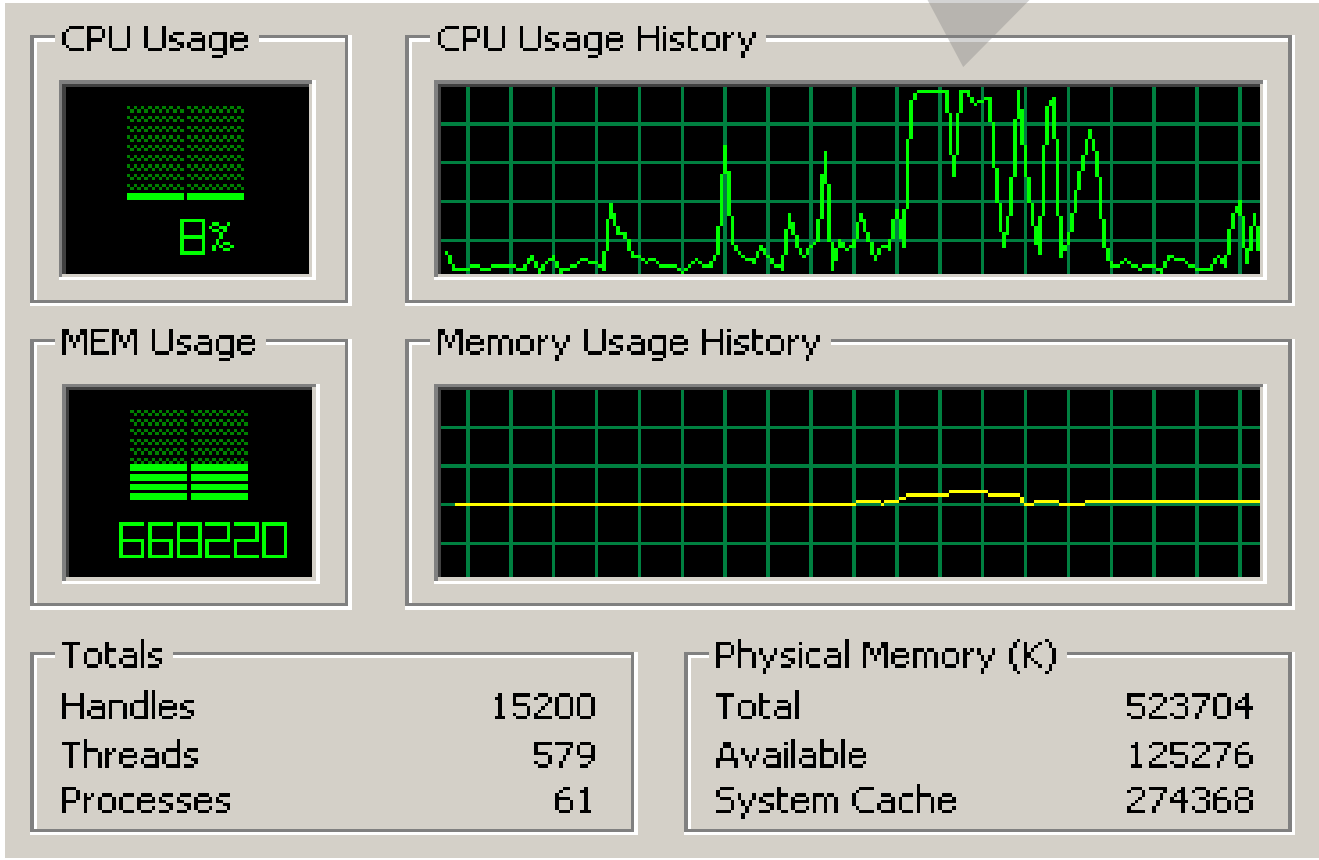


Performance Monitoring Example: Array Port Utilization

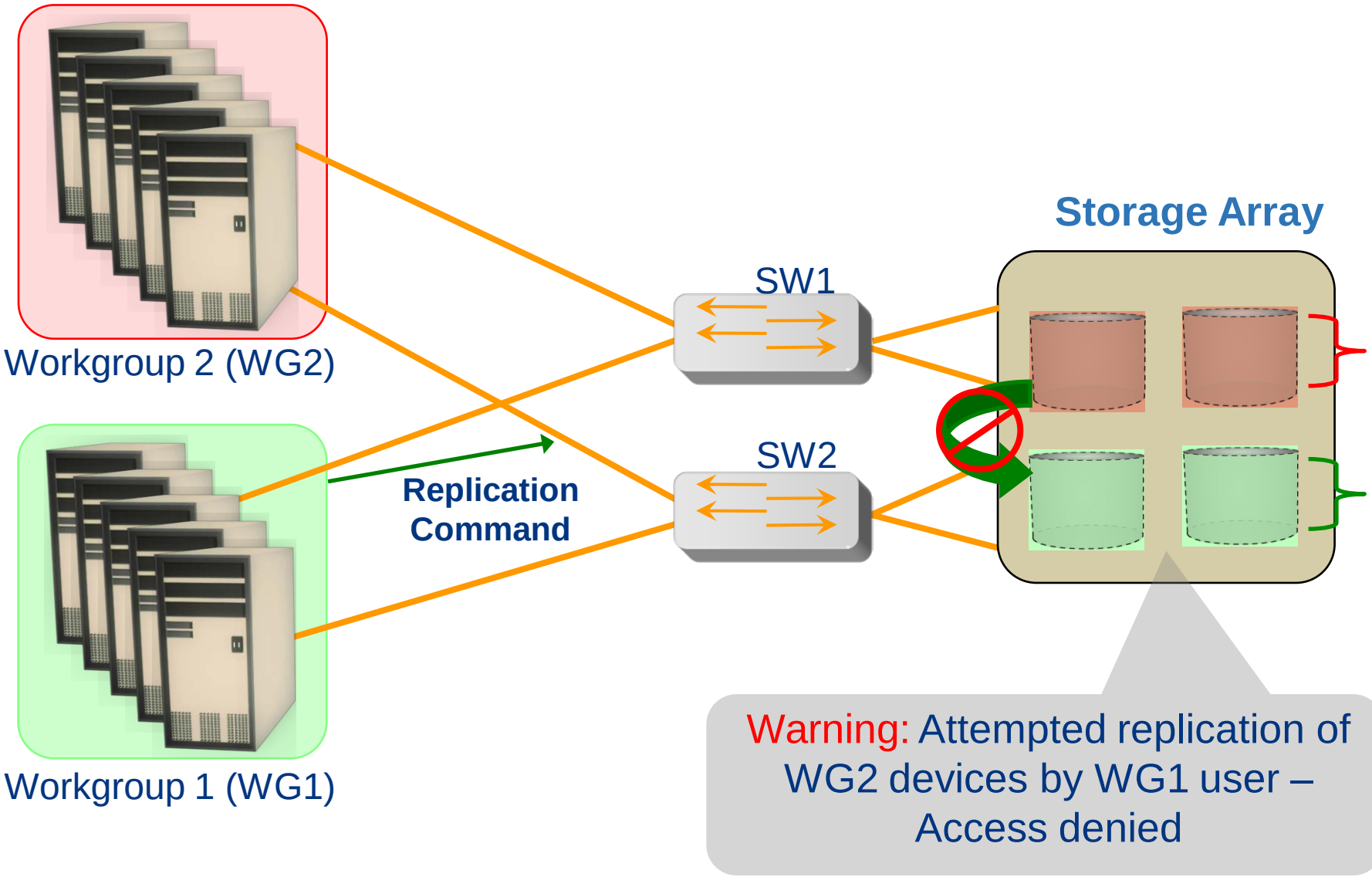


Performance Monitoring Example: Server CPU Utilization

Critical: CPU Usage above 90% for the last 90 minutes



Security Monitoring Example: Storage Array



Alerting Events

- Alerting is an integral part of monitoring
- Monitoring tools enables administrators to assign different severity levels for different events
- Level of alerts based on severity
  - ✓ Information alert: Provide useful information and may not require administrator intervention
    - Creation of zone or LUN
  - ✓ Warning alerts: Require administrative attention
    - File systems becoming full/Soft media errors
  - ✓ Fatal alert: Require immediate administrative attention
    - Power failures/Disk failures/Memory failures/Switch failures

Storage Management Activities

- **All the management tasks in a storage infrastructure can be broadly categorized into:**
  - **Availability management**
  - **Capacity management**
  - **Performance management**
  - **Security management**
  - **Reporting**

Availability Management

- Establishing a proper guideline for all configurations to ensure availability based on service levels.
- Example: When a server is deployed to support a critical business function, the highest availability standard is required. This involved deploying the following components:
  - Two or more HBAs
  - Multipathing software
  - Server clustering
  - Two independent fibre channel switches
  - RAID protection
  - Backup
  - Local and remove replication

Capacity Management

- Ensure adequate availability of resources for all services based on their service level requirements
- Capacity management provides:
  - Capacity analysis – compare allocated storage to forecasted storage on a regular basis
  - Trend analysis – actual utilization of allocated storage and rate of consumption
- Example 1: Storage provisioning
  - Device configuration and LUN masking on storage arrays
  - Zoning configuration on SAN and HBA components
- Example 2: Estimating future needs of resources
  - Gather and analyze related information to come up with estimates

Performance Management

- Ensures the optimal operational efficiencies of all components
- Performance analysis is performed on existing storage infrastructure components
  - Provides information whether a component is meeting expected performance levels
- When a new application or server is to be deployed, every components involved must be validated for adequate performance capabilities as defined by the service levels.
  - Server: volume configuration, database design, application layout on multiple HBAs, multipathing software
  - SAN: designing sufficient ISLs in a multi-switch fabric with adequate bandwidth
  - Storage arrays: selecting appropriate RAID type and LUN layout, front-end and back-end ports, LUN masking

Security Management

- **Prevents unauthorized access and configuration of storage infrastructure components**

- **Example: When deploying a new application or server**
  - **Managing user accounts and access policies**
  - **Zoning configuration in the SAN**
  - **LUN masking**

Reporting

- Keeping track and gathering information from various components / processes

- This information is compiled to generate reports for:
  - Trend analysis and capacity planning: current and historic information about utilization of storage, file system, database tablespace, ports
  - Configuration or asset management: device allocation, local and remote replicas, fabric configuration, list of equipment with details such as their value, purchase date, lease status and maintenance record
  - Chargeback: allocation and utilization of storage infrastructure components by various departments / user groups.
  - Performance : performance of various storage infrastructure components

Disaster Recovery

- Should not be equated with backups, archiving and data recovery
- It refers to Process, Policy and Procedures related to recovery of continuity of technology infrastructure critical to an organization after a natural or human-induced disaster
- A proper disaster recovery mechanism (i.e., recovering for critical data and all aspects of IT infrastructure) must be planned in advance
- Disaster Recovery Planning (DRP) or Business Process Contingency Plan (BPCP)
  - a subset of Business Continuity Plan (BCP) which includes non-IT related other factors
  - defines the strategy of organization to deal against potential disaster
  - Identify method of Testing DRP and simulate Dry run to check the effectiveness of the plan

Space Management-Hierarchical Storage Management

- **Space Management** : Identifies and moves low-activity and inactive files to the hierarchy of storage

- **Technique** that storage manger uses is called **Hierarchical storage management (HSM)**
  - automatically and transparently migrate unused or infrequently used files from a computer's online storage to the offline storage which is managed by a server
  - **Adv** – remove manual file-pruning tasks
    - ensure effective utilization of online storage space
    - reduces cost of retaining large no. of data files for a longer period

Use of HSM

In addition to automate space management to achieve lifecycle management, HSM have some other uses as well

❑ **Supports Unlimited Online Data storage:**

- automatically sends files that meet user definable, policy-based criteria to a designated offline server
- replaces original file with a STUB file that retails the original file attributes
- make feel the client computer that the original file is still there by automatic recall from the offline storage

❑ **Data Backup:** Data backup and file migration coordinate in two ways with the storage manager

I – the option setting allows a migration to occur only when the data backup of that file has already been performed

II – If a file has been previously migrated, the storage manager server can clone the migrated file and move it to the data backup storage pool as a backup copy

- This technique avoids the need to first recall and then re-send files from the client to the server

HSM...

❑ Maintain Total File System Sizes

- Administrator specifies the amount of local online storage that must be filled with data before any migration occurs
- and also the amount that should be available when the migration stops
- This triggers the max and min sizes of total file system for storage manager for space management
- Based on this max space-utilization threshold storage manager initiates file migration considering the priorities assigned to the file size and its age

❑ Maintain the Stub file sizes

- Administrator can also specify various stub file sizes
- Larger stub file sizes means the existence of more data locally on the client storage
- Generally , a portion of the complete data remains in the stub file
- So when some application wants to read the file, stub file may be adequate, thereby reducing the recall of the entire file from the offline storage

HSM...

❑ Improve Scalability

- Separate candidate search from the optimized reconciliation process that synchronizes the hierarchical storage management client and the storage management server
- i.e., candidate search can be performed continuously in the background while the synchronization process can be independently run or scheduled
- Thus provide better scalability and processing performance for large number of files in HSM

❑ Pre-migration

- It helps increasing the network efficiency by allowing the administrator to schedule pre-migration during the period when the network or the client is less active
- It moves a copy of the selected file to the offline storage of the server of the storage manager, leaving the entire original file on the client's online storage
- The client software of space manager can then quickly and easily convert client copy of the file into a stub file
- Thereby freeing clients online storage space as and when needed, with no further requirement of data transfer

Database and Application Protection

Clear goal: To ensure Simplicity and Availability

- ❑ Perform online backup of databases and applications
- ❑ While their recovery it should simplify the complexity of database backup while increasing availability and flexibility
- ❑ Allows consistent data protection policies to be established across the enterprises
- ❑ Database backup means back of table space and data files
- ❑ Backup and recovery operations can be performed either locally or remotely
- ❑ Organizations can manage all aspects of database backup and recovery centrally

Database Protection

To provide following features

- ❑ Flexible data protection: should include b/u and recovery of databases, database related files, file groups and transactions logs
- ❑ Archiving: Integrated capability enables the archiving data in XML format for long term storage
- ❑ Allows faster recovery in damaged pages
- ❑ Point-in-time recovery: Should recover databases to the exact point in time
- ❑Continuous logical Log Backup: The d/b has to configure the automated logical log b/u to prevent logical logs from filling up and locking up d/b server
- ❑

Application Protection…

- **Direct** attacks against web applications have become common place due to relative ease of manipulation
- **Rigorous security** on client site as well as an understanding of manipulation techniques are essential to identity the potential failure points
- **Other application attacks may include**

  exploitation of privileges, buffer overflow attack, client side manipulations etc
- There exists **some sub-categories of the applications** on the top of the web server's operating systems which may be subjected to vulnerabilities such as
  - ✓ Web and application server
  - ✓ Website and application
  - ✓ Flexible Restore
  - ✓ Data Base

Application Protection...

- Considering all these applications and taking vulnerabilities into account , the application management provides following facilities
  - Alternate Restoration Techniques
  - Online Backup
  - Centralized backup
  - Robust Data Integrity

Storage Infrastructure Management Challenges :

- Large number and variety of storage arrays, networks, servers, databases and applications
- Variety of storage devices varying in capacity, performance and protection methodologies
- Deployment of both SAN and IP networks for storage devices
- Servers with different operating systems: UNIX, LINUX, Windows, mainframe
- Interoperability issues between services from multiple vendors
- Multiple vendor-specific tools to monitor devices from different vendors

Computer or Network Security

Commonly used terminologies

Computer security, **Cyber security**, **Digital Security** or I**nformation Technology security** (**IT security**)

Protection of computer systems and networks
from attacks by malicious actors
that may result in
Unauthorized information disclosure, theft of, or damage
to hardware, software, or data,
as well as
from the disruption or misdirection of the services they provide

Security Management

Why it is essential to make provisions of security in any enterprise?

- Growing use of internet brought in many business opportunities (e-commerce) and new business models
- Collaborative activities has increased tremendously (sharing of information amongst partners and suppliers)
- Need for Virtual sharing of information (access to the information source from anywhere at any time), taking part of the company's information outside from its secured infrastructure

❑ At the same time the threat perception on theft, hacking, disruption of services, damage to h/w and s/w etc is increasing every other day.

➢ This necessitates

- ✓ risk identification and protection
- ✓ access control , defining users rights, safeguarding critical s/w, h/w, and information,
- ✓ preventing intrusion and
- ✓ continuous risk analysis and deploying appropriate prevention mechanism

Security Management – some terminology

Security: Preventing of unauthorized access, use or modification of information
: Also called the protection of information and systems

Threat: A type of action that can harm the overall system

Vulnerabilities: The level of exposure

Countermeasure: Action taken to prevent the threat

We can relate these as

$$Risk = \frac{Threat\ x\ vulnerability}{Contermeasure}$$

Intrusion: The modern infrastructure facility allows the virtual connection to access source from anywhere and anytime and may allow carrying outside a part of the information from company's secured infrastructure. This introduces the chances of intrusion

- **Access control** and User rights: to be well defined and are essential steps to be introduced.
- **Risk Analysis**: It is essential to know all the components of the company that needs to be protected all such risk

Vulnerabilities

- A vulnerability is a security weakness in the design, implementation, operation, or internal control of a computer or system
- Most of the vulnerabilities that have been discovered are documented in the **Common Vulnerabilities and Exposures** (CVE)* database.
- An ***exploitable* vulnerability** is one for which at least one working attack or *exploit* exists.
- Vulnerabilities can be researched, reverse-engineered, hunted, or exploited using automated tools or customized scripts
- Various people or parties are vulnerable to cyber attacks; however, different groups are likely to experience different types of attacks more than others

* "About the CVE Program". *www.cve.org*

Vulnerabilities – A report from UK

- In April 2023, the United Kingdom Department for Science, Innovation & Technology released a report on cyber attacks over the last 12 months.
- They surveyed 2,263 UK businesses, 1,174 UK registered charities and 554 education institutions.
- The research found that 32% of businesses and 24% of charities overall recall any breaches or attacks from the last 12 months.
- These figures were much higher for medium businesses (59%), large businesses (69%) and high-income charities with £500,000 or more in annual income (56%).
- Medium or large businesses are more often the victims, but larger companies have generally improved their security over the last decade.
- Small and Midsize Businesses (SMBs) have also become increasingly vulnerable as they often "do not have advanced tools to defend the business".
- SMBs are most likely to be affected by malware, ransomware, phishing, man-in-the-middle attacks, and Denial-of Service (DoS) Attacks.

Classification of Threats that leads to attacks

- Backdoor
- Denial-of-service attack (DoS)
- Direct-access attacks
- Eavesdropping
- Malware (malicious software)
- Man-in-the-middle attacks
- Multi-vector, polymorphic attack
- Phishing
- Privilege escalation
- Side-channel attack
- Social engineering
- Spoofing
- Tampering
- HTML smuggling

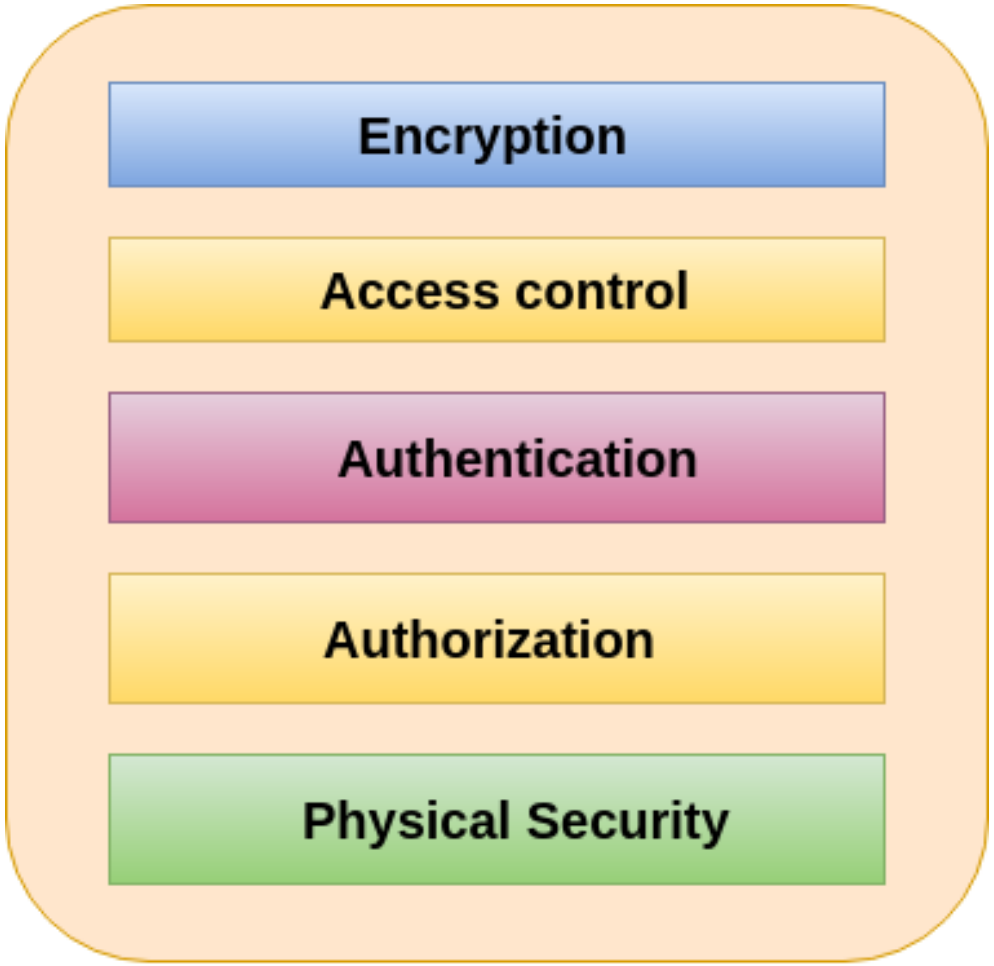
Security Goals

- C.I.A

Confidentiality

- Confidentiality is roughly equivalent to privacy and avoids the unauthorized disclosure of information.
- It involves the protection of data, providing access for those who are allowed to see it while disallowing others from learning anything about its content.
- It prevents essential information from reaching the wrong people while making sure that the right people can get it.
- Data encryption is a good example to ensure confidentiality.

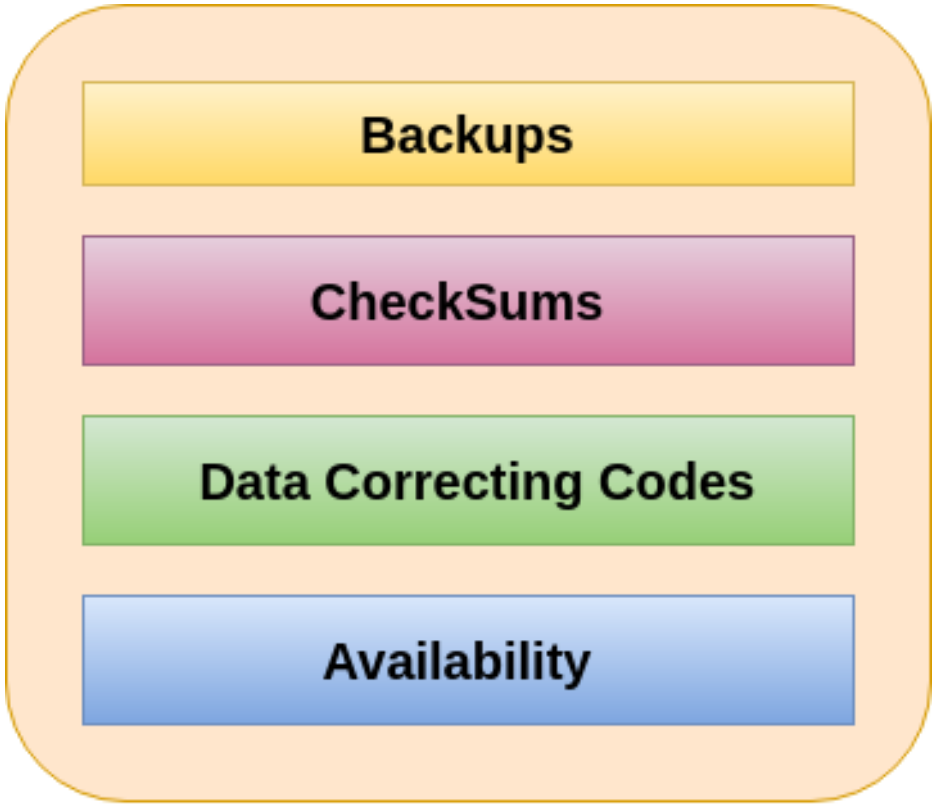
Tools for Confidentiality



Confidentiality Tools

Integrity

- Integrity refers to the methods for ensuring that data is real, accurate and safeguarded from unauthorized user modification.
- It is the property that information has not be altered in an unauthorized way, and that source of the information is genuine.



Integrity Tools

Availability

- Availability is the property in which information is accessible and modifiable in a timely fashion by those authorized to do so.
- It is the guarantee of reliable and constant access to sensitive data by authorized people only

Tools for Availability

- Physical Protections
- Computational Redundancies

Non-repudiation

- It ensures that the operation and activities involved (or performed) in the transaction processing cannot be denied by none of the parties at a later date

- To establish non-repudiation, e-commerce systems uses digital signature and encryption technology during transaction processing

Popular Security Mechanism

The mechanism that is built to identify any breach of security or attack on the organization

- **Encipherment (Encryption)** involves the use of algorithms to transform data into a form that can only be read by someone with the appropriate decryption key. Encryption can be used to protect data it is transmitted over a network, or to protect data when it is stored on a device.

- **Digital signature** is a security mechanism that involves the use of cryptographic techniques to create a unique, verifiable identifier for a digital document or message, which can be used to ensure the authenticity and integrity of the document or message.

- **Traffic padding** is a technique used to add extra data to a network traffic stream in an attempt to obscure/unclear the true content of the traffic and make it more difficult to analyze.

- **Routing control** allows the selection of specific physically secure routes for specific data transmission and enables routing changes, particularly when a gap in security is suspected.

Commonly used Security Services

Authentication is the process of verifying the identity of a user or device in order to grant or deny access to a system or device.

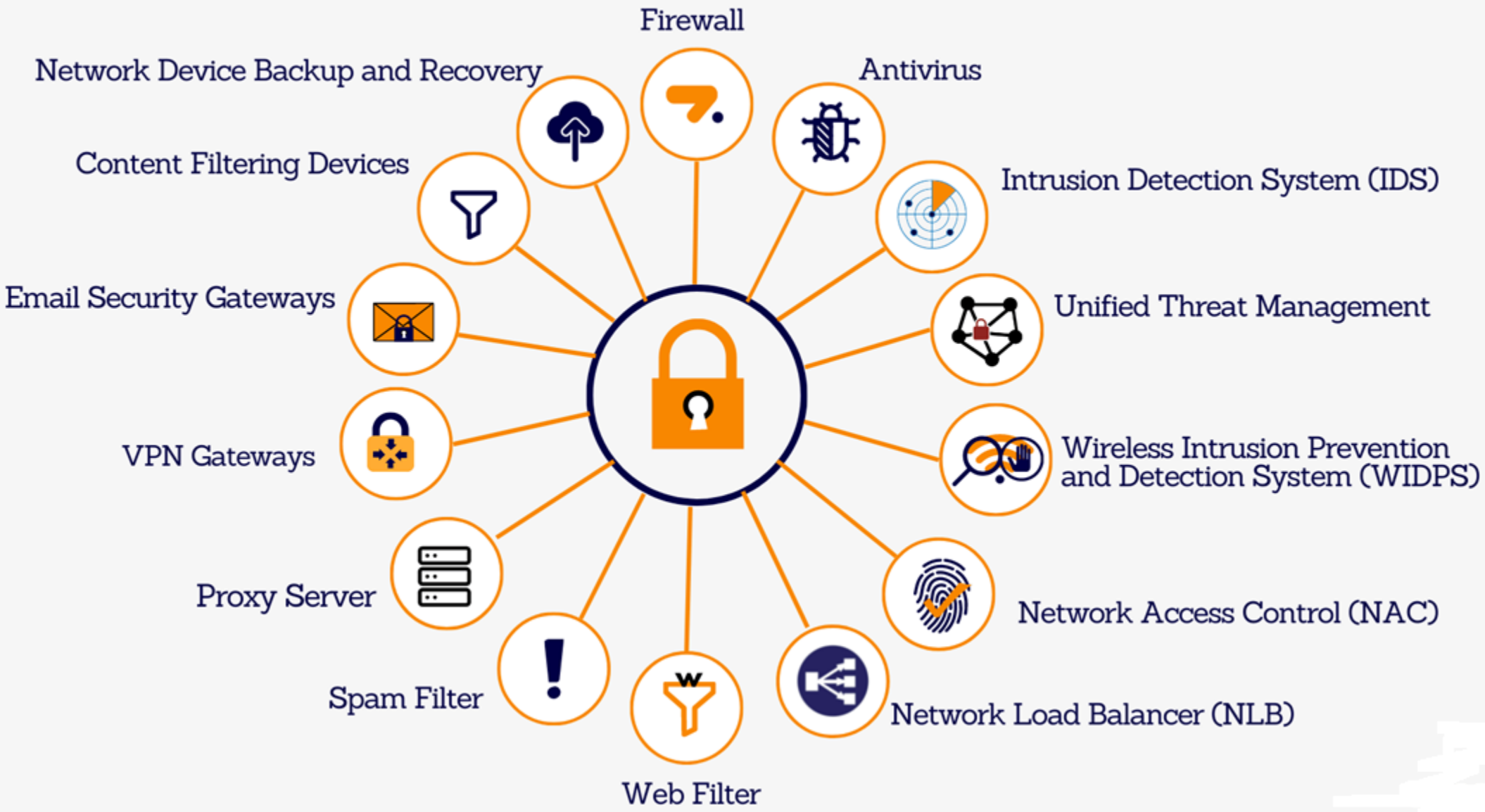
Access control involves the use of policies and procedures to determine who is allowed to access specific resources within a system.

Data Confidentiality is responsible for the protection of information from being accessed or disclosed to unauthorized parties.

Data integrity is a security mechanism that involves the use of techniques to ensure that data has not been tampered with or altered in any way during transmission or storage.

Non- repudiation involves the use of techniques to create a verifiable record of the origin and transmission of a message, which can be used to prevent the sender from denying that they sent the message.

WHAT ARE THE TYPES OF NETWORK SECURITY DEVICES



Security Techniques for Hackers and Crackers

- **Cryptography:** Converting plain text to cipher text at source (*encryption*) and revert at destination (decryption).Uses algorithms based on complex mathematical functions and keys in string of bits

- Categories of Cryptographic Algorithms
  - ✓**Secret Key Cryptography** (SKC): uses same key for encryption and decryption so requires key sharing
  - ✓**Public Key Cryptography** (PKC): Uses two keys – one public (used by sender) and one private key (used by recipient)
  - ✓**Hash Function (or message digests) :** One way encryption algorithm with no usage of any key
    - A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered.
    - It uses digital fingerprints of the file's content to ensure that the file has not been changed by an intruder or any type of virus
    - Many operating systems use hash functions to encrypt passwords
  - ✓**Digital Signature (DS)**: It uses asymmetric cryptography.
  - Make recipient to believe that the sender is a rightful claimant
  - Difficult to forge
  - Uses two different keys which are mathematically related – private key for DS creation and public key for DS verification

Security Techniques for Hackers and Crackers

❑ **Captcha**: Completely Automated Public Turing test to tell Computers and Humans Apart

- A computer program that can tell whether its user is a human or a computer
- Generates images that human can understand but a program can not.
- Captcha is basically a reverse Turing test i.e., administered by a machine and target to a human

- **Applications of Captcha** :
  Web registration, Preventing Spam, E-mail-worms and Spam,
  Dictionary attacks, Search Engine Robots, Online-Polls

Add to Tutorial 3 questions

Q. With example illustrate all the encryption-decryption algorithms
Q. State use of each of the above algorithms.

Internet Security

Layer			Protocol data unit (PDU)	Function[27]
Host layers	7	Application	Data	High-level protocols such as for resource sharing or remote file access, e.g. HTTP.
	6	Presentation		Translation of data between a networking service and an application; including character encoding, data compression and encryption/decryption
	5	Session		Managing communication sessions, i.e., continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes
	4	Transport	Segment, Datagram	Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing
Media layers	3	Network	Packet	Structuring and managing a multi-node network, including addressing, routing and traffic control
	2	Data link	Frame	Transmission of data frames between two nodes connected by a physical layer
	1	Physical	Bit, Symbol	Transmission and reception of raw bit streams over a physical medium

OSI Model

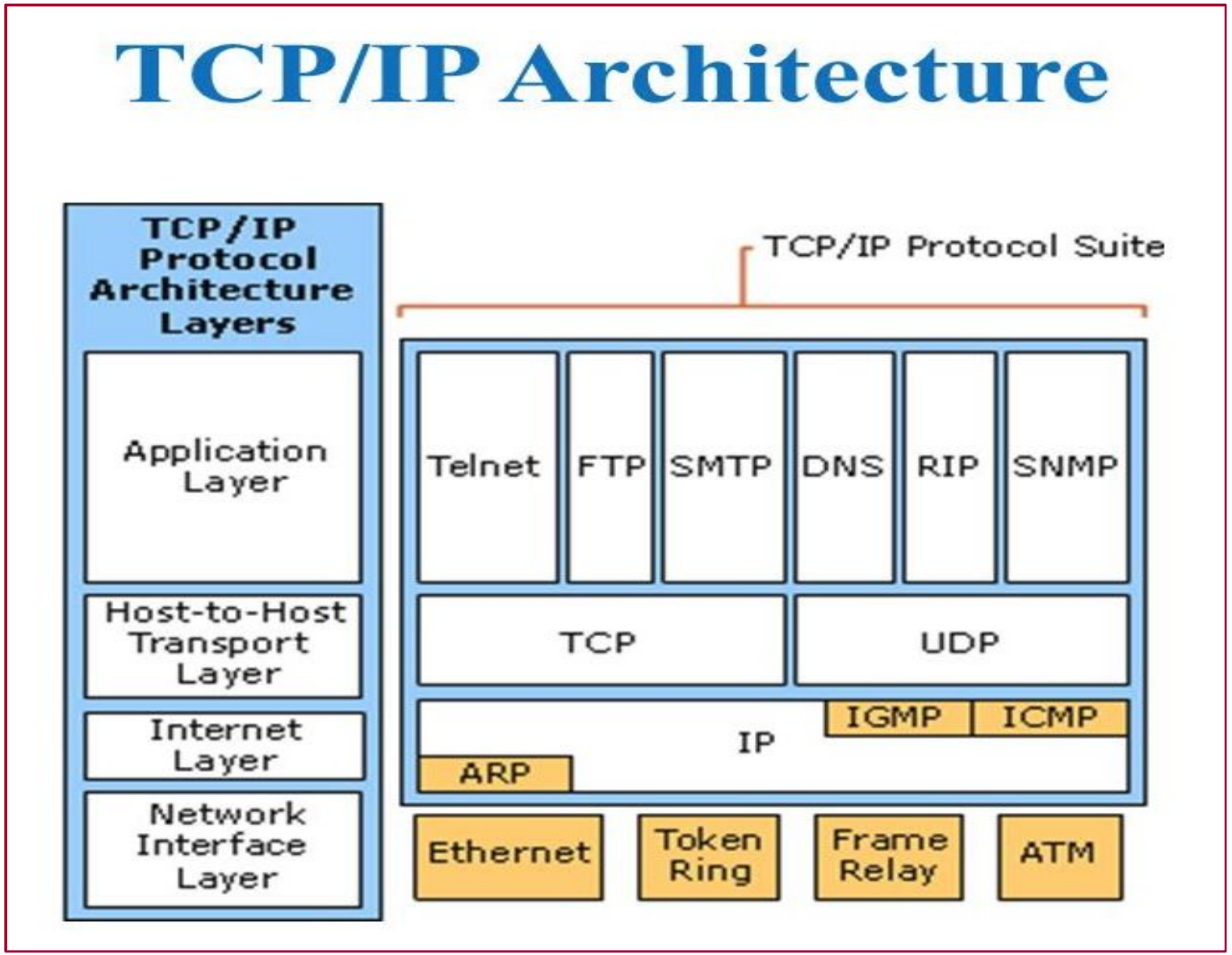
Security Mechanisms at each Layer of the OSI Model

LAYER	MECHANISM	DESCRIPTION
Physical Layer	**Physical Access Control**	Controls physical access to network devices, cables, and infrastructure. Examples include locked server rooms, biometric access controls, and security cameras
Data Link Layer	**MAC Address Filtering**	Filters incoming traffic based on MAC addresses. Only authorized devices with permitted MAC addresses are allowed to communicate
Network Layer	**Firewalls**	Firewalls filter traffic based on IP addresses, ports, and protocols. They prevent unauthorized access and protect against network-based attacks
Transport Layer	**Encryption (SSL/TLS)**	Encrypts data during transmission to ensure confidentiality. Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are commonly used protocols

Security mechanisms at each layer of the OSI model

LAYER	MECHANISM	DESCRIPTION
Session Layer	**Session Tokens**	Establishes and manages communication sessions. Session tokens prevent unauthorized session hijacking
Presentation Layer	**Data Compression and Encryption**	Compresses data for efficient transmission and encrypts it for security. Ensures data integrity and confidentiality
Application Layer	**Authentication and Authorization**	Verifies user identity (e.g., username/password, biometrics). Authorization: Determines access rights based on user roles (e.g., read-only, admin)

TCP/IP Reference Model



What security measures are in place to prevent TCP/IP protocol misuse?

Authentication:

- Strong authentication mechanisms such as username/password combinations, digital certificates, or biometric authentication can ensure that only authorized individuals or devices can access the network.

Encryption:

- Encryption techniques like Transport Layer Security (TLS) or Secure Socket Layer (SSL) can encrypt the transmitted data over the TCP/IP protocol.
- Prevents eavesdropping and ensures the confidentiality and integrity of the data.

Firewalls*: [techniques – packet filtering, application level gateway, circuit level gateway, proxy server]*

- Firewalls are a barrier between internal and external networks.
- Monitor incoming and outgoing network traffic, enforcing predefined security rules.
- Firewalls can block malicious traffic and prevent unauthorized TCP/IP protocol access.

Continue...

Intrusion Detection System (IDS) and Intrusion Prevention System (IPS):

- IDS and IPS monitor network traffic for suspicious activities or behavior.
- They can detect and respond to potential threats, such as denial-of-service attacks or unauthorized access attempts, to protect the TCP/IP protocol from misuse.

Access Control:

- Implementing strict access control policies helps prevent unauthorized TCP/IP protocol access.
- This can be achieved by using strong passwords, limiting user privileges, and employing role-based access control.

Regular Updates and Patches:

- Keeping the TCP/IP protocol and related software updated with the latest security patches is essential to prevent misuse.
- Regular updates and patches address known vulnerabilities and security flaws, ensuring that the protocol remains secure against potential attacks.

Network Segmentation:

- By dividing a network into smaller, isolated segments, it becomes more difficult for an attacker to gain unauthorized access to the TCP/IP protocol.
- Network segmentation helps contain potential security breaches and limits the impact of any successful attacks.

Security Audits and Penetration Testing:

- Regular security audits and penetration testing can help identify TCP/IP protocol vulnerabilities and its implementations.
- By proactively assessing the security posture of the protocol, any weaknesses can be addressed and mitigated to prevent misuse.

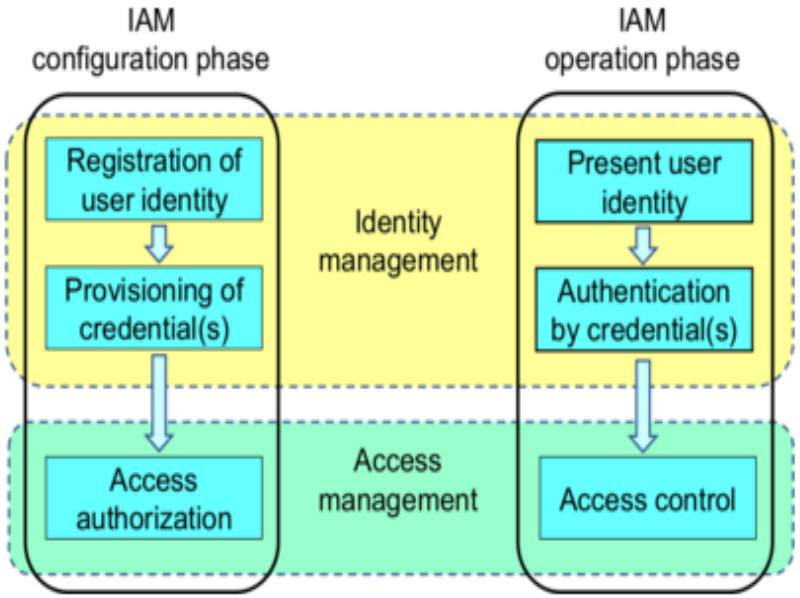
Incident Response Plan:

- A well-defined incident response plan ensures that any security incidents or breaches involving the TCP/IP protocol are promptly and effectively addressed.
- This includes containment, mitigation, and recovery steps to minimize misuse's impact.

Identity management (IdM) OR identity and access management (IdAM)

What is IdM or IdAM?

- A framework of policies and technologies to ensure that the right users (that are part of the ecosystem connected to or within an enterprise) have the appropriate access to technology resources
- Identity and access management systems not only identify, authenticate, and control access for individuals who will be utilizing IT resources but also the hardware and applications employees need to access
- It is the organizational and technical processes for first registering and authorizing access rights in the configuration phase, and then in the operation phase for identifying, authenticating and controlling individuals or groups of people to have access to applications, systems or networks based on previously authorized access rights



Functions of IdM

In the real-world context of engineering online systems, identity management can involve 5 basic functions:

1. **The pure identity function: Creation, management and deletion of identities without regard to access or entitlements.**
2. **The user access (log-on) function: For example: a smart card and its associated data used by a customer to log on to a service or services (a traditional view);**
3. **The service function: A system that delivers personalized, role-based, online, on-demand, multimedia (content), presence-based services to users and their devices.**
4. **Identity Federation: A system that relies on federated identity to authenticate a user without knowing their password.**
5. **Audit function: Monitor bottlenecks, malfunctions and suspect behavior.**