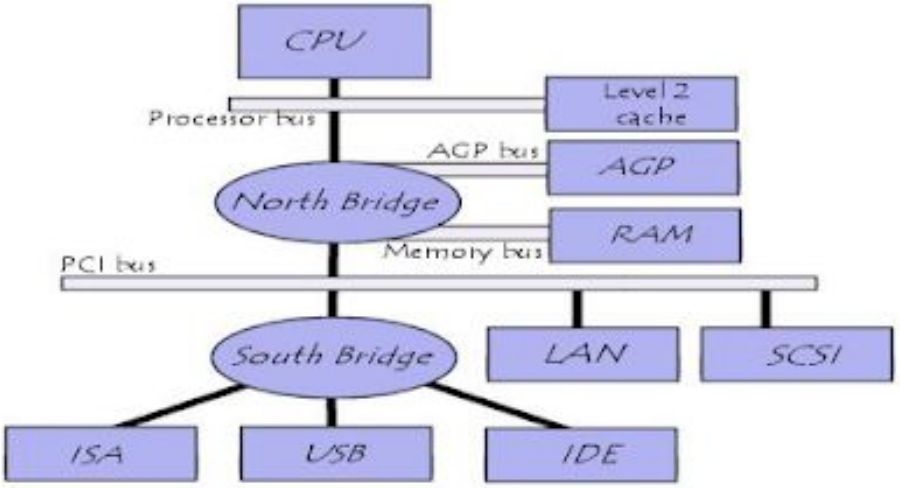
- **PC and Server Architecture**

PC Architecture



Architecture

In reality, each bus is generally constituted of 50 to 100 distinct physical lines, divided into three subassemblies:

- The **address bus** (sometimes called the *memory bus*) transports memory addresses which the processor wants to access in order to read or write data. It is a unidirectional bus.
- The **data bus** transfers instructions coming from or going to the processor. It is a bidirectional bus.
- The **control bus** (or *command bus*) transports orders and synchronisation signals coming from the control unit and travelling to all other hardware components. It is a bidirectional bus, as it also transmits response signals from the hardware.

The primary buses

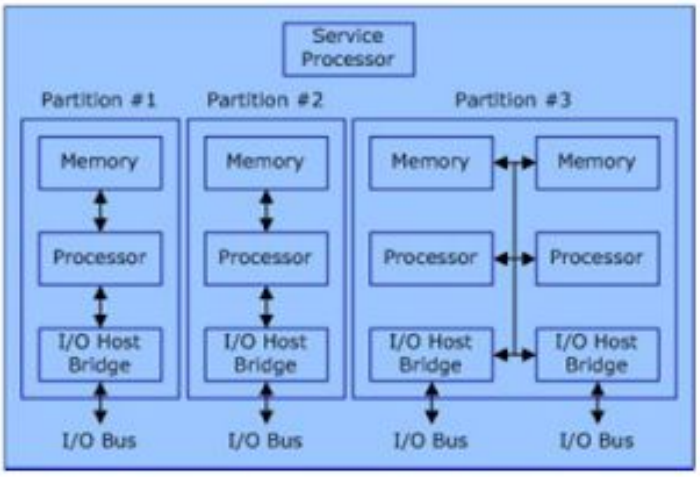
There are generally two buses within a computer:

- The **internal bus** (sometimes called the *front-side bus*, or *FSB* for short). The internal bus allows the processor to communicate with the system's central memory (the RAM).
- **The expansion bus** (sometimes called the *input/output bus*) allows various motherboard components (USB, serial, and [contents/415-serial-port-and-parallel-port parallel ports], cards inserted in PCI connectors, hard drives, CD-ROM and CD-RW drives, etc.) to communicate with one another. However, it is mainly used to add new devices using what are called **expansion slots** connected to the input/output bus.

Chipset

A **chipset** is the component which routes data between the computer's buses, so that all the components which make up the computer can communicate with each other. The **chipset** originally was made up of a large number of electronic chips, hence the name.

Server Architecture



A hardware partitionable server can be configured into one or more isolated hardware partitions. A hardware partition consists of one or more partition units. A partition unit can be a processor, a memory module, or an I/O host bridge.

In the previous figure, the server has a total of 12 partition units: four memory modules, four processor modules, and four I/O host bridge modules. Each of these partition units is assigned to one of three hardware partitions. Each hardware partition is completely isolated from the other hardware partitions. The service processor is responsible for the configuration of the hardware partitions. It controls the mapping of the partition units to the hardware partitions and creates isolation between the hardware partitions.

OPERATING SYSTEM ADMINISTRATION

UNIX

- Early 70s --> AT&T System V Unix (and C developed)--> BSD Unix (U. Cal-Berkley)
- Today - many variants. Portable and Scalable.

  HP - HP/UX

  IBM - AIX

  Silicon Graphics - Irix

  Sun Microsystems - SunOS/Solaris
- 1982 - Sun Microsystems founded.
- PC Based Unix - solaris, SCO Unix, FreeBSD, NetBSD
- Linux - Linus Torvalds (Finland) 1991. Free/Open.
  - (Red Hat Linux – Commercial Version)

- Debian, another popular version of Linux (freeware)

WINDOWS

- 1975 - Microsoft Formed
- 1980 - Xenix released by Microsoft
- 1981 - MS-DOS 1.0 released with new IBM PC
- 1985 - Windows 1.0 released
- 1992 - Windows 3.1 released
- 1993 - Windows NT 3.1 released (over 6 million lines of code)
- **1995** - Windows NT 3.5.1 released
- Windows 95 released
- **1996** - Windows NT 4.0 released
- **1998** - Windows 98 released
- **1998** - Microsoft announces Windows NT 5.0 will be renamed Windows 2000
- **2000** - release of windows 2000 (aka NT 5.0)
- **2001** - release of windows XP (aka NT 5.1)
- **2003** - release of windows 2003 server

MAC-OS

- Mac OS is a series of graphical user interface-based operating systems developed by Apple Inc. for their Macintosh line of computer systems.
- Mac OS was designed only to run on Apple Computers.
- In 1984, Apple introduced the Macintosh PC with the Macintosh Operating System.
- Apple names its OS as "Mac OS", beginning in 1997 which was previously known as "System".

MAC-OS Versions

Various Versions of Mac OS X

Version	Codename	Release Date
MAC OS X 10.0	Cheetah	March 24, 2001
MAC OS X 10.1	Puma	September 25, 2001
MAC OS X 10.2	Jaguar	August 24, 2002
MAC OS X 10.3	Panther	October 24, 2003
MAC OS X 10.4	Tiger	April 29, 2005
MAC OS X 10.5	Leopard	October 26, 2007
MAC OS X 10.6	Snow Leopard	August 28, 2009
MAC OS X 10.7	Lion	July 20, 2011
MAC OS X 10.8	Mountain Lion	July 25, 2012
MAC OS X 10.9	Mavericks	October 22, 2013
MAC OS X 10.10	Yosemite	June 2, 2014

Centralization Authentication

Centralized administration means having one point for control and policy. For example each site might have its own pair of DNS servers, but the data on these servers might be completely, partially (e.g., domain names but not host names, or a top-level domain name but not sub-domain names or host names), or not at all controlled (allow each site to create domain and host names) by central administration.

How much *centralization* or *decentralization* to have in a large organization? There is no best answer to this question. As the SA for a larger organization, you will likely have to understand what parts of the system are centralized and which (if any) are not. In a smaller organization, the SA may be asked for an opinion on policy and procedures, and will need to decide what services should be under a single, central control and which should not.

Note that this decision isn't all or nothing! Centralization is a spectrum, with total control by a central authority at one extreme and no central control or policy at all at the other. Furthermore it is likely that some services will be more centralized than others. Most services will have control policies somewhere in the middle.

Factors to consider when creating policies or procedures (when deploying a new service) include availability of local expertise and training costs, budgeting issues, and organization management structure and politics.

Benefits of Centralization

- Centralization can often improve efficiency and reduce costs. (At HCC software licenses were too expensive per class or even per campus, but per college we got great terms!)
- Centralization usually means consistent policies and procedures across the enterprise, always a good thing.
- Centralization or partial centralization works well for well understood or *commodity* services such as printing, file services, and email.

Reasons for Decentralization

A poorly run central administration means slow response times and often a worse service than a local "do it ourselves" admin service can provide. It can even drive up

costs with bureaucratic overhead such as needless levels of management. Other problems can include inability to communicate directly with required people, time wasted with pointless reporting, micromanagement, inflexibility, etc.
(HCC story: IMAP mail server when down but web mail service remained up. Rather than report to the SA in charge of that server, I was forced to report to my dean, who was forced to report to some V.P., who called the manager of our out-sourced admin service, who called the help desk, who entered a trouble-ticket, which was eventually sent to the SA in charge of the mail server. Of course none of these management people knew what IMAP was so the problem was never reported correctly.)
Decentralization usually works better when deploying new technology, or if various users will have special requirements (*one size fits all* is a motto that will doom many projects).
Decentralization can improve response time and lower overhead and other costs.

Problems with Decentralization

If poorly managed decentralization can lead to higher costs, and no recourse if no local expertise is available (which may be needed in many areas!). Local politics and personality conflicts can lead to very poor quality of service, as well as poor recognition for local SAs, just because some local manager doesn't budget correctly, or automatically says no to any upgrade or change. (This happens more often than you might think!)
Decentralization can cause inconsistent policies and procedures. Central budgeting can cause local service to suffer scarce budgets

Central Authentication Service

The Central Authentication Service (CAS) is a single sign-on protocol for the web. Its purpose is to permit a user to access multiple applications while providing their credentials (such as userid and password) only once. It also allows web applications to authenticate users without gaining access to a user's security credentials, such as a password. The name CAS also refers to a software packagethat implements this protocol.

The CAS protocol involves at least three parties: a client web browser, the web application requesting authentication, and the CAS server. It may also involve a back-end service, such as a database server, that does not have its own HTTP interface but communicates with a web application.

When the client visits an application requiring authentication, the application redirects it to CAS. CAS validates the client's authenticity, usually by checking a username and password against a database (such as Kerberos, LDAP or Active Directory).

If the authentication succeeds, CAS returns the client to the application, passing along a service ticket. The application then validates the ticket by contacting CAS over a secure connection and providing its own service identifier and the ticket. CAS then gives the application trusted information about whether a particular user has successfully authenticated.

CAS allows multi-tier authentication via proxy address. A cooperating back-end service, like a database or mail server, can participate in CAS, validating the authenticity of users via information it receives from web applications. Thus, a webmail client and a webmail server can all implement CAS.

Active Directory

Active Directory (AD) is a directory service that Microsoft developed for Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services. Initially, Active Directory was only in charge of centralized domain management. Starting with Windows Server 2008, however, Active Directory became an umbrella title for a broad range of directory-based identity-related services.

A server running Active Directory Domain Services (AD DS) is called a domain controller. It authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software. For example, when a user logs into a computer that is part of a Windows domain, Active Directory checks the submitted password and determines whether the user is a system administrator or normal user.[4] Also, it allows management and storage of information, provides authentication and authorization mechanisms, and establishes a framework to deploy other related

services: Certificate Services, Federated Services, Lightweight Directory Services and Rights Management Services.[5]

Active Directory uses Lightweight Directory Access Protocol (LDAP) versions 2 and 3, Microsoft's version of Kerberos, and DNS

Active Directory provides the following network services:

1. Lightweight Directory Access Protocol (LDAP) – An open standard used to access other directory services
2. Security service using the principles of Secure Sockets Layer (SSL) and Kerberos-based authentication
3. Hierarchical and internal storage of organizational data in a centralized location for faster access and better network administration
4. Data availability in multiple servers with concurrent updates to provide better scalability

Active Directory is internally structured with a hierarchical framework. Each node in the tree-like structure is referred to as an object and associated with a network resource, such as a user or service. Like the database topic schema concept, the Active Directory schema is used to specify attribute and type for a defined Active Directory object, which facilitates searching for connected network resources based on assigned attributes. For example, if a user needs to use a printer with color printing capability, the object attribute may be set with a suitable keyword, so that it is easier to search the entire network and identify the object's location based on that keyword.

Active Directory versus Workgroup

Workgroup is another Microsoft program that connects Windows machines over a peer-to-peer network. Workgroup allows these machines to share files, internet access, printers and other resources over the network. Peer-to-peer networking removes the need for a server for authentication.

Lightweight Directory Access Protocol (LDAP)

LDAP (Lightweight Directory Access Protocol) is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet. LDAP is a "lightweight" (smaller amount of code) version of Directory Access Protocol (DAP), which is part of X.500, a standard for directory services in a network. LDAP is lighter because in its initial version it did not include security features. LDAP originated at the University of Michigan and has been endorsed by at least 40 companies. Netscape includes it in its latest Communicator suite of products. Microsoft includes it as part of what it calls Active Directory in a number of products including Outlook Express. Novell's NetWare Directory Services interoperates with LDAP. Cisco also supports it in its networking products.

An LDAP directory is organized in a simple "tree" hierarchy consisting of the following levels:

- The root directory (the starting place or the source of the tree), which branches out to
  Countries, each of which branches out to
- Organizations, which branch out to
- Organizational units (divisions, departments, and so forth), which branches out to (includes an entry for)
- Individuals (which includes people, files, and shared resources such as printers)

four models are defined:
1. Information model
The information model provides the structures and data types necessary for building an LDAP directory tree. An entry is the basic unit in an LDAP directory. You can visualize an entry as either an interior or exterior node in the
Directory Information Tree (DIT). An entry contains information about an instance of one or more objectClasses. These objectClasses have certain required or optional attributes.
Attribute types have defined encoding and matching rules that govern such things as the type of data the attribute can hold and how to compare this data during a search. This information model will be covered extensively in the next chapter when we examine LDAP schema.

2. Naming model
The naming model defines how entries and data in the DIT are uniquely referenced. Each entry has an attribute that is unique among all siblings of a single parent. This unique

attribute is called the relative distinguished name (RDN). You can uniquely identify any entry within a directory by following the RDNs of all the entries in the path from the desired node to the root of the tree. This string created by combining RDNs to form a unique name is called the node's distinguished name (DN).
3. Functional model
The functional model is the LDAP protocol itself. This protocol provides the means for accessing the data in the directory tree. Access is implemented by authentication operations (bindings), query operations (searches and reads),
and update operations (writes).
4. Security model
The security model provides a mechanism for clients to prove their identity (authentication) and for the server to control an authenticated client's access to data (authorization). LDAPv3 provides several authentication methods not
available in previous protocol versions. Some features, such as access control lists, have not been standardized yet, leaving vendors to their own devices.

RAID

RAID (**redundant array of independent disks**) is a data storage virtualization technology that combines multiple physical disk drive components into a single logical unit for the purposes of data redundancy, performance improvement, or both.

Data is distributed across the drives in one of several ways, referred to as RAID levels, depending on the required level of redundancy and performance. The different schemes, or data distribution layouts, are named by the word "RAID" followed by a number, for example RAID 0 or RAID 1. Each schema, or RAID level, provides a different balance among the key goals: reliability, availability, performance, and capacity. RAID levels greater than RAID 0 provide protection against unrecoverable sector read errors, as well as against failures of whole physical drives.

RAID Levels

RAID 0 consists of striping, without mirroring or parity. The capacity of a RAID 0 volume is the sum of the capacities of the disks in the set, the same as with a spanned value. There is no added redundancy for handling disk failures, just as with a spanned volume. Thus, failure of one disk causes the loss of the entire RAID 0 volume, with reduced possibilities of data recovery when compared with a broken spanned volume. Striping distributes the contents of files roughly equally among all disks in the set, which makes concurrent read or write operations on the multiple disks almost inevitable and results in performance improvements. The concurrent operations make the throughput of most read and write operations equal to the throughput of one disk multiplied by the number of disks. Increased throughput is the big benefit of RAID 0 versus spanned volume at the cost of increased vulnerability to drive failures.

RAID 1 consists of data mirroring, without parity or striping. Data is written identically to two drives, thereby producing a "mirrored set" of drives. Thus, any read request can be serviced by any drive in the set. If a request is broadcast to every drive in the set, it can be

serviced by the drive that accesses the data first improving performance. Sustained read throughput, if the controller or software is optimized for it, approaches the sum of throughputs of every drive in the set, just as for RAID 0. Actual read throughput of most RAID 1 implementations is slower than the fastest drive. Write throughput is always slower because every drive must be updated, and the slowest drive limits the write performance. The array continues to operate as long as at least one drive is functional.

RAID 2 consists of bit-level striping with dedicated Hamming-code parity. All disk spindle rotation is synchronized and data is striped such that each sequential bit is on a different drive. Hamming-code parity is calculated across corresponding bits and stored on at least one parity drive. This level is of historical significance only; although it was used on some early machines as of 2014 it is not used by any commercially available system.

RAID 3 consists of byte-level striping with dedicated parity. All disk spindle rotation is synchronized and data is striped such that each sequential byte is on a different drive. Parity is calculated across corresponding bytes and stored on a dedicated parity drive. Although implementations exist, RAID 3 is not commonly used in practice.

RAID 4 consists of block-level striping with dedicated parity. This level was previously used by NetApp, but has now been largely replaced by a proprietary implementation of RAID 4 with two parity disks, called RAID-DP. The main advantage of RAID 4 over RAID 2 and 3 is I/O parallelism: in RAID 2 and 3, a single read I/O operation requires reading the whole group of data drives, while in RAID 4 one I/O read operation does not have to spread across all data drives. As a result, more I/O operations can be executed in parallel, improving the performance of small transfers.

RAID 5 consists of block-level striping with distributed parity. Unlike RAID 4, parity information is distributed among the drives, requiring all drives but one to be present to operate. Upon failure of a single drive, subsequent reads can be calculated from the distributed parity such that no data is lost. RAID 5 requires at least three disks. RAID 5 implementations are susceptible to system failures because of trends regarding array rebuild time and the chance of drive failure during rebuild (see "Increasing rebuild time and failure probability" section, below). Rebuilding an array requires reading all data from all disks, opening a chance for a second drive failure and the loss of the entire array. In August 2012, Dell posted an advisory against the use of RAID 5 in any configuration on Dell EqualLogic arrays and RAID 50 with "Class 2 7200 RPM drives of 1 TB and higher capacity" for business-critical data.

RAID 6 consists of block-level striping with double distributed parity. Double parity provides fault tolerance up to two failed drives. This makes larger RAID groups more practical, especially for high-availability systems, as large-capacity drives take longer to restore. RAID 6 requires a minimum of four disks. As with RAID 5, a single drive failure results in reduced performance of the entire array until the failed drive has been replaced. With a RAID 6 array, using drives from multiple sources and manufacturers, it is possible to mitigate most of the problems associated with RAID 5. The larger the drive capacities and the larger the array size, the more important it becomes to choose RAID 6 instead of RAID 5. RAID 10 also minimizes these problems.

Network Attached Storage

A Network Attached Storage (NAS) device is a **storage device connected to a network that allows storage and retrieval of data from a centralised location for authorised network users and heterogeneous clients**. NAS devices are flexible and scale-out, meaning that as you need additional storage, you can add on to what you have.

A NAS is like **having a private cloud in the office. It's faster, less expensive and provides all the benefits of a public cloud onsite, giving you complete control**.

NAS devices are perfect for small businesses because they are:

- Simple to operate, a dedicated IT professional is often not required
- Lower cost
- Easy to use for back up of data, so it's always accessible when you need it
- Good at centralising data storage in a safe, reliable way

Network-attached storage (NAS) is a type of dedicated file storage device that provides local-area network local area network (LAN) nodes with file-based shared storage through a standard Ethernet connection.

NAS devices, which typically do not have a keyboard or display, are configured and managed with a browser-based utility program. Each NAS resides on the LAN as an independent network node and has its own IP address.

An important benefit of NAS is its **ability to provide multiple clients on the network with access to the same files.** Prior to NAS, enterprises typically had hundredsK or even thousands of discrete file servers that had to be separately configured and maintained. Today, when more storage capacity is required, NAS appliances can simply be outfitted with larger disks or clustered together to provide both vertical scalability and horizontal scalability. Many **NAS vendors partner with cloud storage providers to provide customers with an extra layer of redundancy for backing up files.**

Advantages of NAS (Network Attached Storage)

Following are the advantages of NAS:
• It is used for low volume access to a large amount of storage by many users.
• Heterogeneous environment
• Centralized Storage

Disadvantages of NAS

Following are the disadvantages of NAS:
• Low Performance
• Limited scalability
• Network Congestion during backups & Restore
• Ethernet Limitations

storage area network (SAN)

A storage area network (SAN) is a secure high-speed data transfer network that provides access to consolidated block-level storage. An SAN makes a network of storage devices

accessible to multiple servers. SAN devices appear to servers as attached drives, eliminating traditional network bottlenecks.

Introduced in the early 2000s, SANs were initially limited to enterprise class computing. Today, high-speed disk costs have gradually dropped and SANs have become a mainstay for greater organizational storage.

SAN implementation simplifies information life cycle management and plays a critical role in delivering a consistent and secure data transfer infrastructure.

SAN solutions are available as two types:

- Fiber Channel (FC): Storage and servers are connected via a high-speed network of interconnected fiber channel switches. This is used for mission-critical applications where uninterrupted data access is required.
- Internet Small Computer System Interface (iSCSI) Protocol: This infrastructure gives the flexibility of a low-cost IP network.
  Both provide advantages based on business requirements.

  The advantages of SAN include:

- Storage Virtualization: Server capacity is no longer linked to single storage devices, as large and consolidated storage pools are now available for software applications.
- High-Speed Disk Technologies: An example is FC, which offers data retrieval speeds that exceed 5 Gbps. Storage-to-storage data transfer is also available via direct data transmission from the source to the target device with minimal or no server intervention.
- Centralized Backup: Servers view stored data on local disks, rather than multiple disk and server connections. Advanced backup features, such as block level and incremental backups, streamline IT system administrator responsibilities.
- Dynamic Failover Protection: Provides continuous network operation, even if a server fails or goes offline for maintenance, which enables built-in redundancy and automatic traffic rerouting.

SAN is offered by server manufacturers, such as IBM and HP. Server-independent SAN providers include EMC and Network Appliance.

Direct-attached storage (DAS)

Direct-attached storage (DAS) is computer storage that is connected to one computer and not accessible to other computers. For an individual computer user, a hard drive or solid-state drive (SSD) is the usual form of direct-attached storage. In the enterprise, individual disk drives in a server are called direct-attached storage, as are groups of drives that are external to the server but are directly attached through Small Computer System Interface (SCSI), Serial Advanced Technology Attachment (SATA), Serial-Attached SCSI (SAS), Fibre Channel (FC) or iSCSI.

DAS can be deployed as disks -- hard disk drives (HDDs) or SSDs -- inside a server chassis, for example, or as an external storage enclosure or enclosures directly connected to a card

plugged into the internal bus of a server. It can also be an individual drive in a desktop or laptop computer.

A direct-attached storage device is not networked. There is no connection through Ethernet or FC switches that connect network-attached storage (NAS) devices and storage area networks (SANs).

Other types of storage, such as optical devices and tape, are technically DAS as they are directly attached to a system. However, when one refers to DAS, it is usually in regard to internal or external primary or secondary storage in the form of HDDs and SSDs.

DAS advantages include:

- High availability.
- High access rate due to Storage Area Network (SAN) absence.
- Elimination of network setup complications.
- Storage capacity expansion.
- Data security and fault tolerance.

DAS drawbacks include:

- Data not accessible by diverse user groups.
- Allows only one user at a time.
- High administrative costs.

feature	DAS	NAS	SAN
Full Name	Direct Access Storage	Network Attached Storage	Storage Area Network
Storage type	Sectors	Shared files	Blocks
Data Transmission	IDE/SCSI	TCP/IP, Ethernet	Fiber Channel, IP
Access Mode	Clients or servers	Clients or servers	Servers
Capacity in Bytes	10^9	10^9 to 10^{12}	> 10^{12}
Complexity	Easy	Moderate	Difficult
Management cost (per GB)	High	Moderate	Low

Data integrity

Data integrity is the assurance that digital information is uncorrupted and can only be accessed or modified by those authorized to do so. Integrity involves maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle.

To maintain integrity, data must not be changed in transit and steps must be taken to ensure that data cannot be altered by an unauthorized person or program. Such measures include implementing user access controls and version control to prevent erroneous changes or accidental deletion by authorized users. Other measures include the use of checksums and cryptographic checksums to verify integrity. Network administration measures to ensure data integrity include documenting system administration procedures, parameters and maintenance activities, and creating disaster recovery plans for occurrences such as power outages, server failure or security attacks. Should data become corrupted, backups or redundancies must be available to restore the affected data to its correct state.

Measures must also be taken to ensure integrity by controlling the physical environment of networked terminals and servers because data consistency, accuracy and trustworthiness can also be threatened by environmental hazards such as heat, dust or electrical problems. Some means must be in place to detect any changes in data that might occur as a result of non-human-caused events such as an electromagnetic pulse (EMP) or server crash. Practices followed to protect data integrity in the physical environment include keeping transmission media (such as cables and connectors) covered and protected to ensure that they cannot be tapped, and protecting hardware and storage media from power surges, electrostatic discharges and magnetism.

Data Backup and Recovery Methods

Backup and recovery refers to the process of backing up data in case of a loss and setting up systems that allow that data recovery due to data loss. Backing up data requires copying and archiving computer data, so that it is accessible in case of data deletion or corruption. Data from an earlier time may only be recovered if it has been backed up.

Data backup is a form of disaster recovery and should be part of any disaster recovery plan.

Data backup methods

- **Disks or tape backup**. These are the oldest of the backup methods we're discussing. Traditional tape backups have their benefits (fairly inexpensive), but also have their drawbacks (slower backup and recovery times, and management of physical tapes). With tape, you're sequentially backing up your data on a physical device. Hard disks offer a faster backup and recovery process than tape, and include additional benefits such as deduplication and data compression. Backing up to a physical device has its merits, but the key is finding a way to do it efficiently and economically.
- **Hybrid cloud backup**. With a hybrid cloud backup solution you're essentially backing up data on a local device and in a secure offsite data center for redundancy. You always have a secure local copy of your data, but you also have it stored offsite. Also, your machines are backed up to the local device first, so you don't have to worry about the replication to the cloud affecting the performance of machines or your Internet connection. The best practice in this case would be to back up from the local device to a secure offsite data center after business hours (automatically of course).
- **Direct-to-cloud backup**. With direct-to-cloud backups, you send your data directly to the cloud, bypassing the need for a local device. In this case, you're backing up your data in a remote data center, without the local copy in your office. Depending on your Internet speeds and specs of your machines, these backups could take much longer. Direct-to-cloud

backups may make sense for SaaS data because you're essentially doing a backup of data that already lives in the cloud!

Data recovery methods

- **Recover from your local** *device*. This only works if you have a device locally (like in the hybrid cloud backup method mentioned above). Some solutions actually allow you to spin up a virtual machine right from the device, so your business operations (applications, settings, files, folders) can all run from the device. This may be a great option if you've experienced server failure, or a machine has had a security compromise. And because you're recovering from your local device, it happens quickly.
- **Recover from the cloud**. Other solutions require you to download your backed-up data from the cloud. This involves transferring gigabytes or even terabytes of data over your Internet connection (in most cases) which could result in hours or even days of downtime. If this is the route you take, it's imperative you find a solution that can recover from the cloud in a few minutes.
- **Recover right in the cloud.** If your local device is damaged, some providers can spin up a virtual machine for you right in the cloud, also known as "disaster recovery as a service" or DRaaS. In other words, you can continue to run these important applications right from the cloud!