SISTEMAS E REDES MULTISERVIÇO

Chapter 5

Data Center architectures, monitoring, and performance evaluation

Chapter Summary

Data Center Architectures

- Characterization
- Servers
- Storage
- SAN
- HCI

Network Assessment and Availability

Monitoring

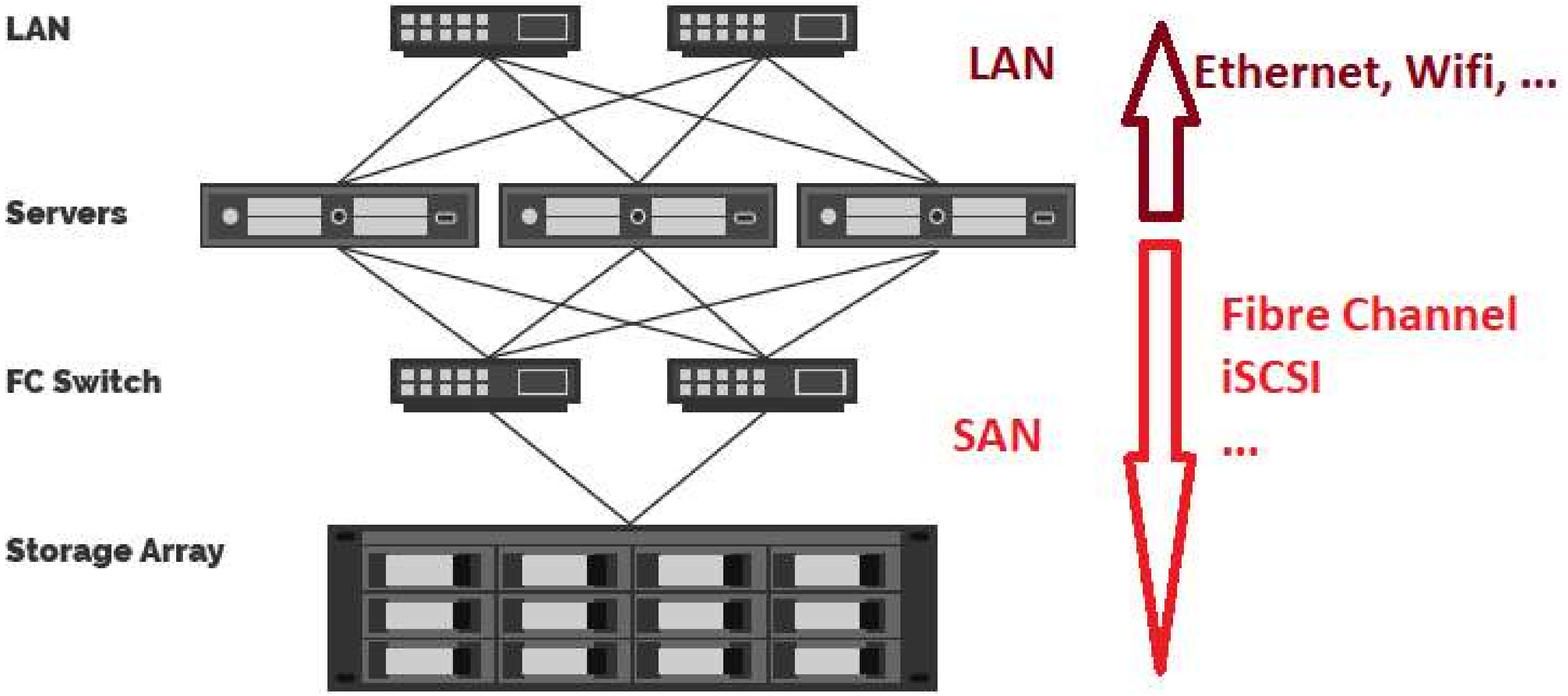
Data Center

- Resource consisting of computers and networked storage to manage, process, store and disseminate large amounts of data. Consisting of:
  - Processing and memory capacity to create servers
  - Storage
  - Infrastructures - building, energy, air conditioning, data network, closets, cables, etc. Management software

Data Center evolution

- '90s
  - A physical server for each application with dedicated storage
  - Lots of physical space and energy consumption!
  - Capabilities of underutilized servers
- ’00s
  - Sharing compute resources (by Virtualization) and storage – reducing the need for hardware
  - SAN - Strorage Area Network - for connecting servers to shared storage
- Current trends
  - Speed, availability, capacity and economy
  - Hyperconvergence – swapping SAN with integrated computing and storage systems
  - Software Defined Data Center

Typical Architecture



LAN

Servers

FC Switch

Storage Array

LAN

Ethernet, Wifi, ...

SAN

Fibre Channel

iSCSI

...

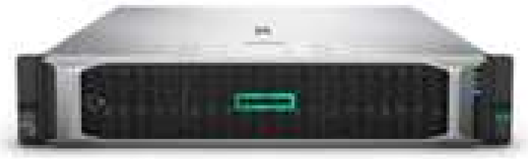
Servers

- Servers - Computers with high processing capacity and memory suitable for:
  - Host apps
  - Manage Files
  - Process data
- They can be:
  - Rack
  - Blades
  - Mainframes

Servers

Rack Servers

- Advantages:
  - Mounted in closets racks
  - Easy accommodation
  - Standard equipment (independence from manufacturers)
- Difficulties:
  - Independent wiring for power, network and storage connection



Servers

Servers in Blades

- Advantages
  - Modular component that fits a chassis
  - Power supply and connection to the network and storage is common to all servers on the same chassis
  - Higher capacity than Rack servers in less busy space
- Difficulties
  - Proprietary chassis –
  - all servers (blades) from the

  same manufacturer

  More expensive than rack

Servers

- Mainframe Servers
  - – Dedicated high performance equipment
  - – Powerful Extremes
  - – Example: IBM with 12 million encrypted transactions per day
- Difficulties
  - – Very expensive
  - – They can take up a lot of space

Server sizing

- They should be adequate to ensure the provision of the service without failures or delays.
  - Hardware:
    - CPU – quantity, type and speed;
    - Memory - Cache, RAM, Flash;
    - Storage - SSD, HDD; RAID; …
  - Software:
    - Operating System;
    - Application service support software.

Server Sizing

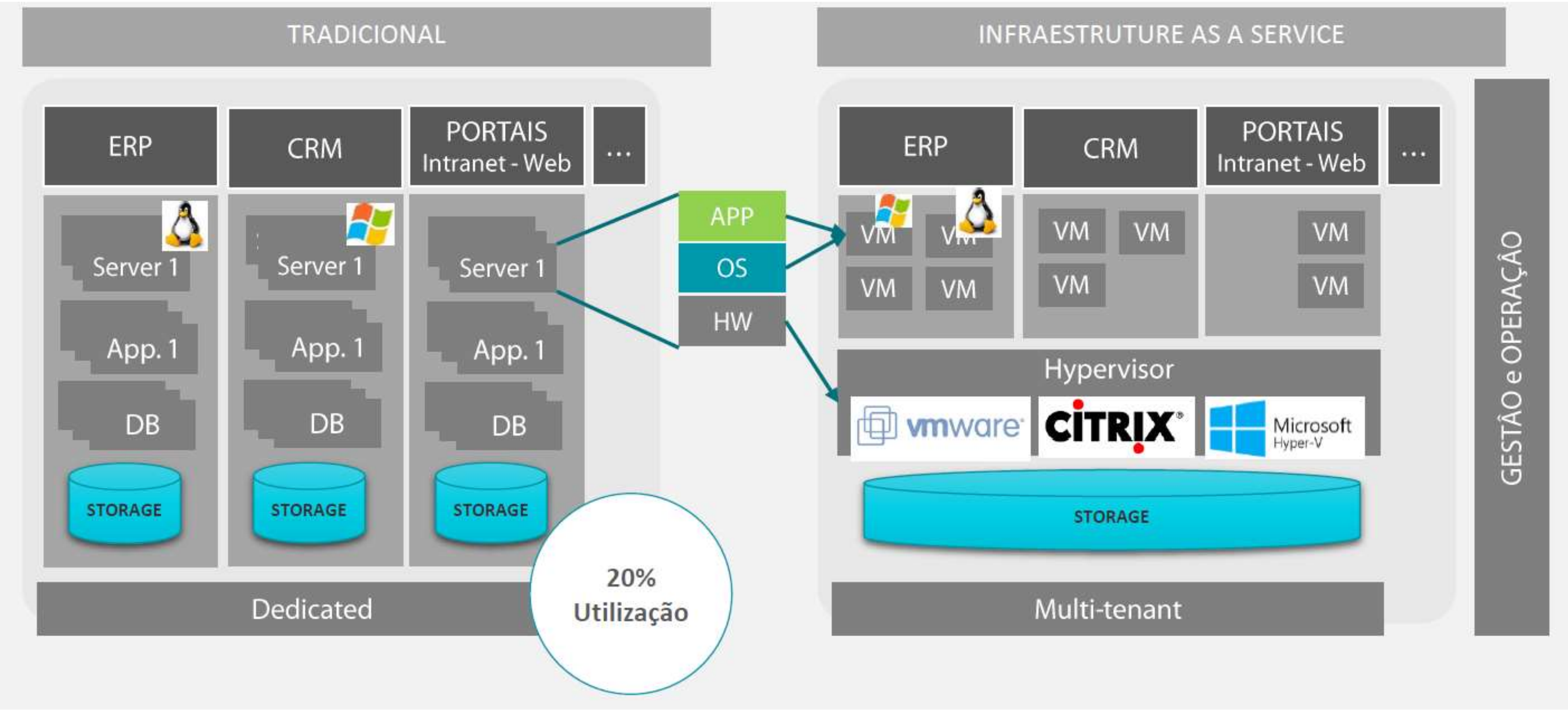
– In sizing, the type of service and the charge expectations should be considered, namely the consumption by each connected customer and the maximum of expected related customers.

Currently, there is no physical server for each application. With Virtualization, servers are created and managed on virtual machines in shared computing and storage resources.

Virtualization

- Technology that allows you to create a hardware platform through a software component
  - The software creates a virtual machine that emulates a computer where you can install an operating system.
  - Easier management of machines for changes, backups, mobility, etc...
  - Fundamental technology for Cloud Computing (BUT NOT THE SAME THING!) because it allows you to share a computer platform into independent pieces that can be managed by different entities

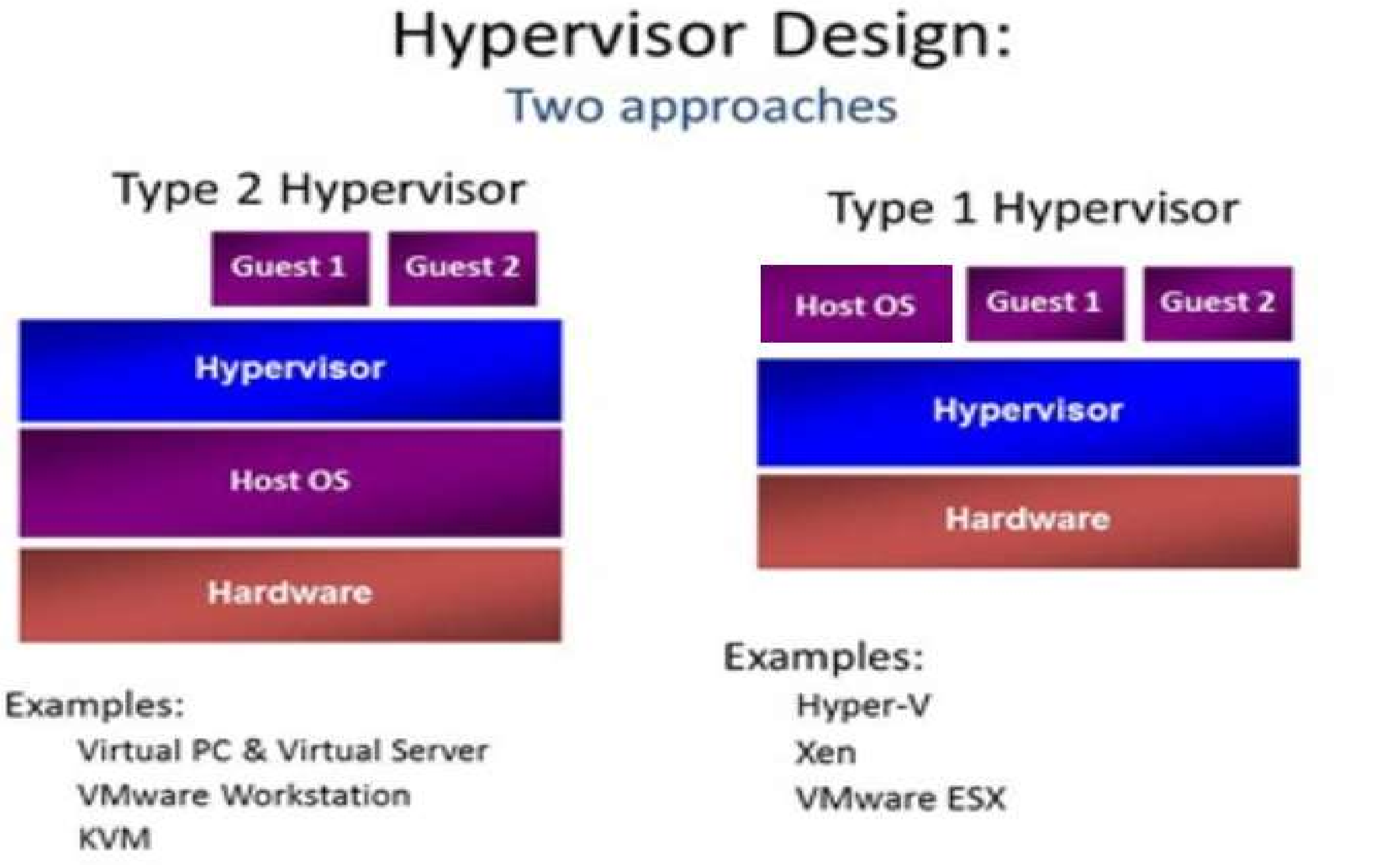
Virtualization



Virtualization

- Virtualization components
  - Physical support hardware (host or host)
    - Limits the computational capacity of the virtual machines it supports;
    - Responsible for the actual network connection interfaces;
  - Hypervisor
    - Software layer that acts between hardware and operating system and emulates virtual machines using host resource sharing;
    - Manage host resources and assign them to Virtual Machines;
    - Manage the resources of multiple physical machines (example: virtualization storage);
  - Virtual Machine
    - Independent systems that act as a computer

Virtualization



Hypervisor Design:

Two approaches

Type 2 Hypervisor

Examples:

- Virtual PC & Virtual Server
- VMware Workstation
- KVM

Type 1 Hypervisor

Examples:

- Hyper-V
- Xen
- VMware ESX

Virtualization

- Advantages of machine virtualization
  - Better use of resources
  - Faster setting up computers or servers
  - Possibility to treat a computer or server as a file that can be easily transported
  - Easier to create backups and disaster recovery architectures
  - Energy saving - fundamental!

Storage – Disc types

- Evaluated by capacity, latency (time it takes to start a task) number of read/write operations (IOPS) and data transfer speed
- For many years, mechanical discs (HDD)
  - The speed is limited by disc rotation – a good disc reaches 200 to 400 IOPS
  - Latency is also affected by nature mechanics of data access - in the milliseconds order
  - discs SAS (**Serial Attached SCSI)**

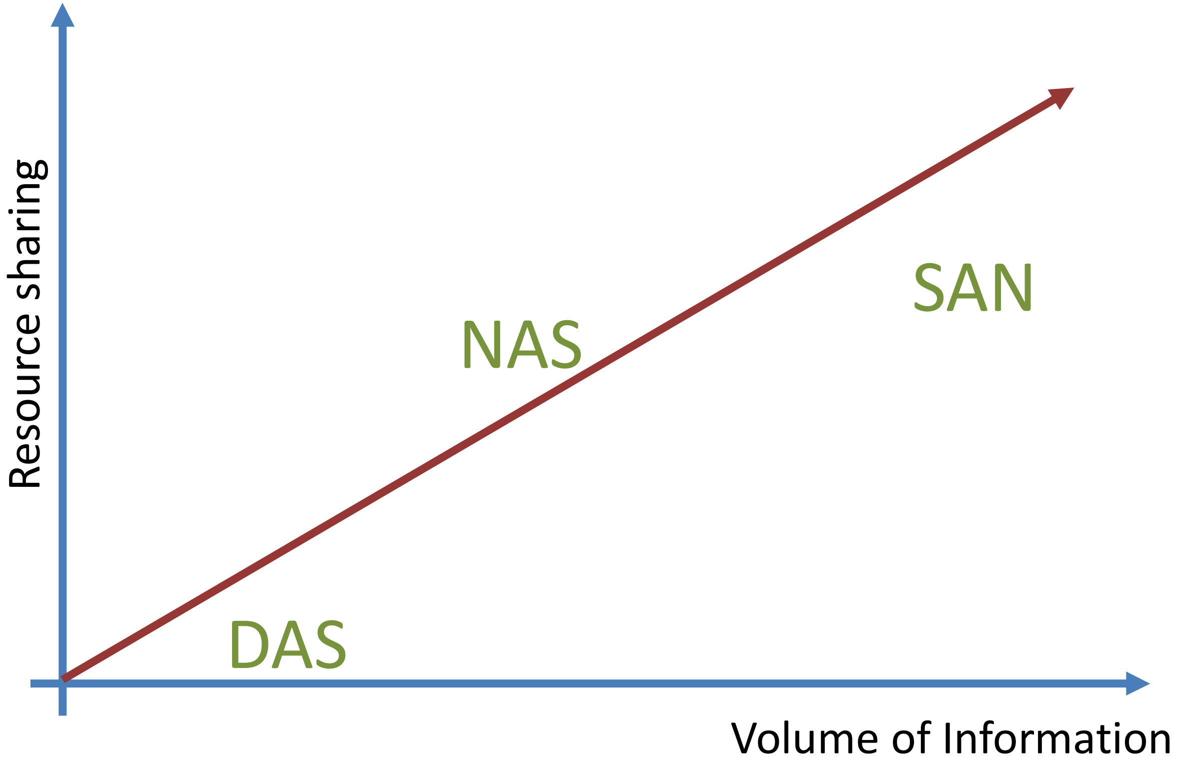
and SATA (*Serial Advanced Technology Attachment*

Storage – Disc types

- Disk types for Storage
  - Recently, Solid State Drive (SSD) discs
    - There are no mechanical components - information stored in nonvolatile memory (memory chips)
    - Lower latency (in the order of microseconds)
    - More IOPS (can reach more than 100,000 IOPS)
    - Lower energy consumption
    - Less prone to breakdowns
    - More expensive but in the process of reducing!
    - For now, lower-capacity discs

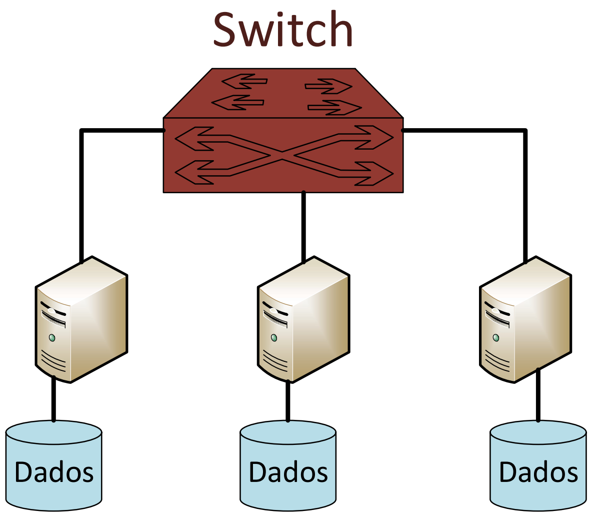
Storage

- How to manage storage?
  - DAS
  - NAS
  - SAN



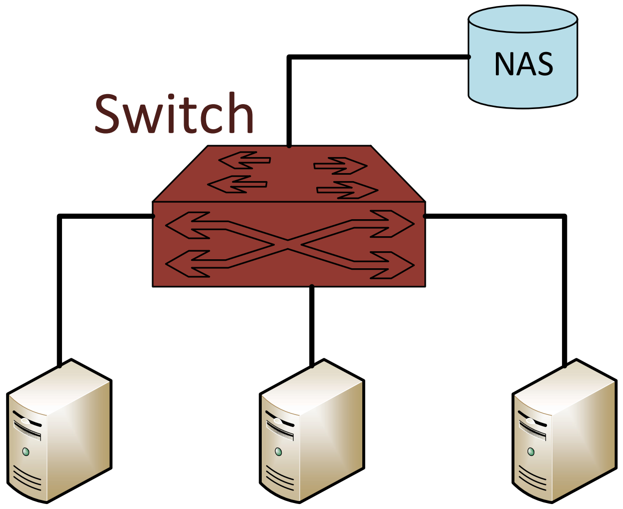
Storage

- DAS – Direct Attached Storage
  - The storage unit is connected directly to the system (e.g. server) that uses it without going over the network;
  - Traditional method used when a server's disk capacity was exceeded;
  - Solution for low volume needs where you do not need to share storage;
  - Storage is only used by the server to which it is connected



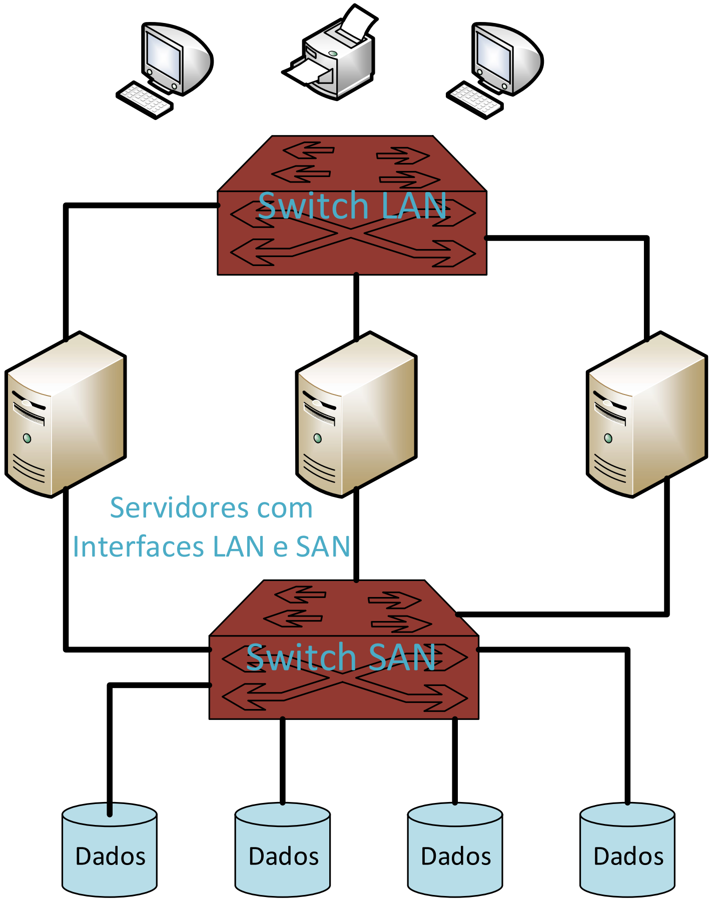
Storage

- NAS – Network Attached Storage
  - The storage unit is connected to the LAN network;
  - It is connected via TCP/IP, like any network device, and typically configured by Web Browser;
  - The information is accessed by File Share (e.g. NFS - Network File System) and can work p.e. as a multimedia server;
  - Most common method in small enterprises;
  - Any network system can access information even at the same time.



SAN –Storage Area Networks

- SAN – Storage Area Network
  - Technology, based on Switches, that connects multiple Physical Servers, Virtual Machines, and storage systems, typically in DataCenters;
  - There is a dedicated network for connecting servers and storage, which does not have the same LAN rules; - prevents LAN congestion from affecting servers;
  - Requires financial investment and the ability to manage it;
  - There are different technologies.



SAN – Storage Area Network

- Dominant network technologies
  - – Fibre Channel
    - Older technology in SANs
    - Distinct from Ethernet/IP operation
    - Physical interface with Host Bus Adapter (HBA)
    - Higher debits but greater complexity and cost
    - Requires own equipment (switches, server network interfaces and storage units)
    - Multiple 4Gb debits (typical 8, 16 or 32Gbps; current max 128Gbps, roadmap for 512Gb)

SAN – Storage Area Network

- Dominant Technologies
  - iSCSI - Small Computer Systems Interface (SCSI) over IP
    - SAN technology developed to connect scsi interfaces (most of the storage) in Ethernet/IP
      - SCSI protocol encapsulated in TCP/IP
      - Connectivity is provided through iSCSI (HBAs) or STORAGE NIC host bus;
      - It already has fibre channel like debits but with lower costs
      - Typical 1Gb and 10Gb debits; maximum 100Gbps, roadmap for 400Gb

SAN – Storage Area Network

- Dominant Technologies
  - Fibre Channel over Ethernet (FCoE)
    - Evolution of Fibre Channel networks to encapsulate FC packets in Ethernet frames so that they can be worked out by cheaper Switches and Routers;
    - Requires converged network adapters (CNA) that pass Ethenet or FCoE frames
    - Having a lot of success by adding the advantages of FC with Ethernet equipment costs

Evolution - HCI

- Hyperconverged infrastructure (HCI)
  - SSD is changing the Data Center architecture. It is faster to have storage accessed directly than through an SAN...
  - The various components (processing, storage,network connection) are assembled in the same rack (node)!
  - Scalability adding more nodes.
  - The HCI solution includes the rack, pre-made cabling, nodes, and, very importantly, the management software that includes Hypervisor and the ability to manage all hardware and software in a fully and shared way (Defined DataCenter Software).

Evolution - HCI

astio

- Software Defined DataCenter
  - The software makes hardware abstraction;
  - Allows the creation and configuration of resources automatically (automation) - p.e. Automatic configuration of a standard station
  - Simplifies processes for the user

Chapter Summary

- Data Center Architectures
- Network Assessment and Availability
  - Performance assessment
  - Business Continuity Plan (BCP)
  - Disaster Recovery (DR)
  - High Availability
    - Redundancies
    - Load Balancing
- Monitoring

Performance Assessment

- Computer networks and systems can be evaluated by:
  - Link debits
  - Packet loss rate
  - Delay and delay variation
  - Response time to application requests -> implications for server scaling
  - Availability (uptime time vs downtime time)

PERFORMANCE EVALUATION

- Availability - measure of evaluation of networks or systems that takes into account the time that services have been available.

Availability (%)	*Downtime*/year	*Downtime*/month
95%	18 days 6:00:00	1 days 12:00:00
96%	14 days 14:24:00	1 days 4:48:00
97%	10 days 22:48:00	0 days 21:36:00
98%	7 days 7:12:00	0 days 14:24:00
99%	3 days 15:36:00	0 days 7:12:00
99,9%	0 days 8:45:35.99	0 days 0:43:11.99
99,99%	0 days 0:52:33.60	0 days 0:04:19.20
99,999%	0 days 0:05:15.36	0 days 0:00:25.92

- Time is money!

Performance Assessment

- For greater Availability -> Greater investment in hardware and software!
- Typically organizations seek a compromise between the availability rate and the cost of solutions.
- Two related parameters:
  - MTBF - Mean time between failures
  - MTTR - Mean time to repair

  Availability = MTBF / (MTBF + MTTR)

Availability of Services

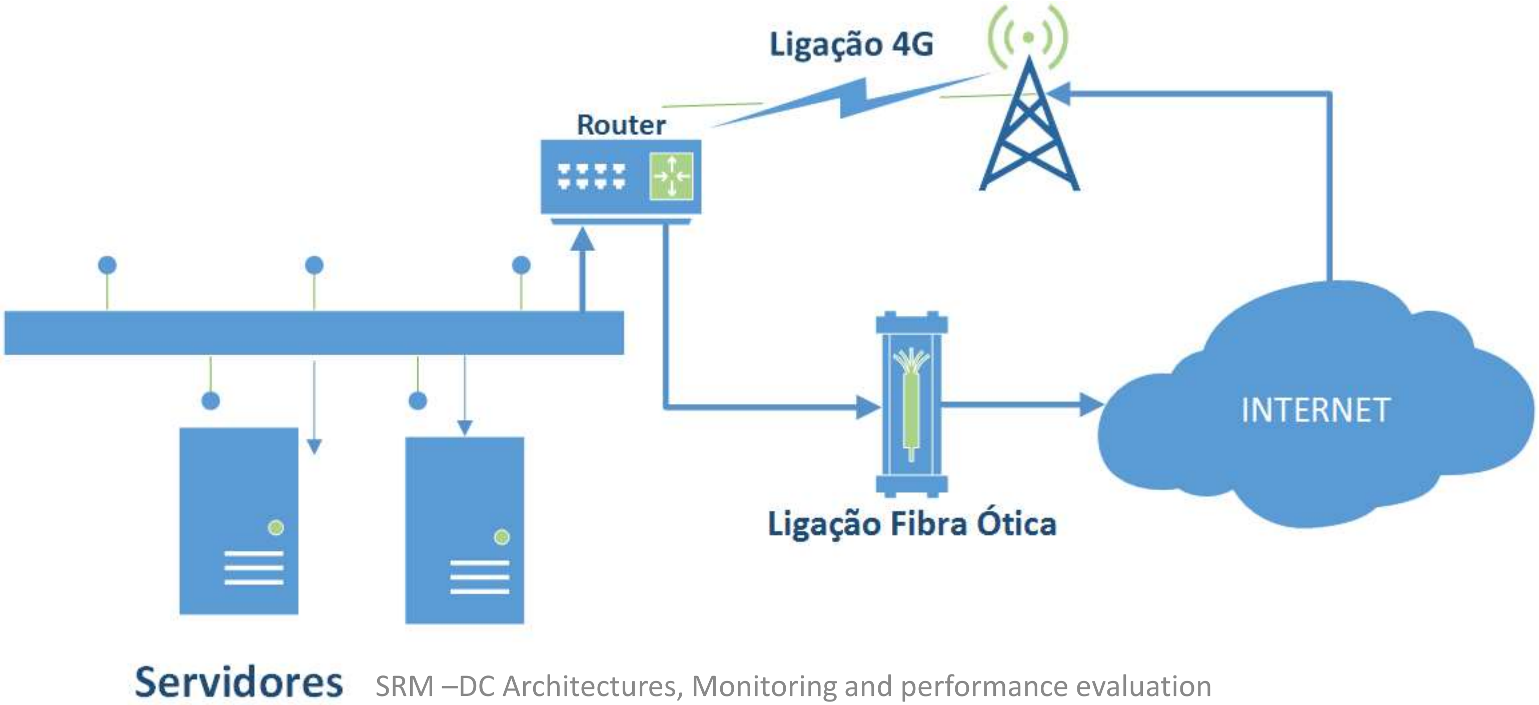
- When a service is critical, requiring a great availability, high availability systems are used:
  - Redundant solutions including alternative systems that ensure service operation when the main system fails.
  - It involves Hardware, Software, Energy and Security (even physics).

Availability of Services

- High Availability involves:
  - Keep Energy available
    - UPS – can be online (energy is constantly feeding them and they are the ones that produce internal energy and support it in case of failure) and offline (only act when power fails);
    - Redundant electrical power strokes in separate paths;
    - Alternative generators - e.g. diesel generators.

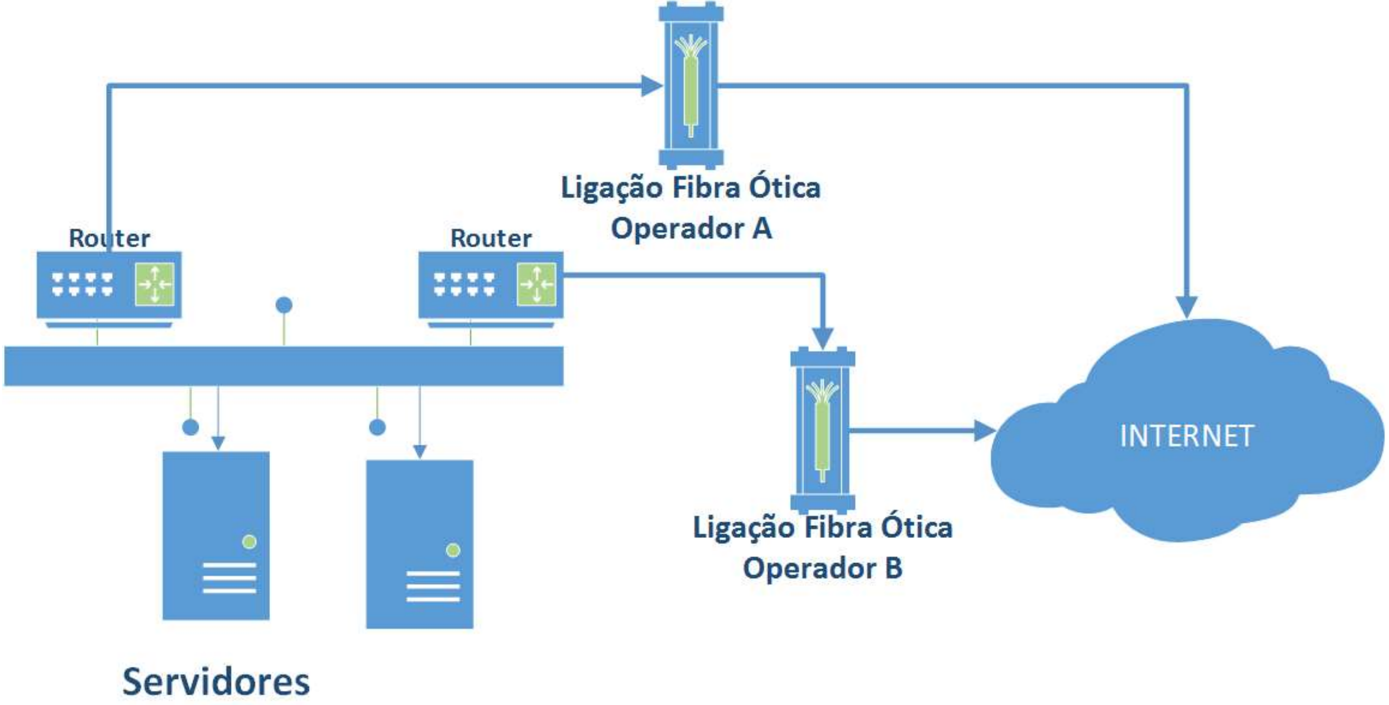
Availability of Services

- High Availability involves:
  - Keep LAN and WAN Networks available
    - LAN with redundant paths;
    - Internet connection duplicated by another operator and/or technology (e.g. Fiber and 4G);
    - In the same operator, there may be redundancy of public IP's.



Availability of Services

- High Availability involves:
  - Keep LAN and WAN Networks available
    - More redundant systems with router duplication, alternate paths and operators:
    - In the same operator, there may be redundancy of public IP's



Availability of Services

- High Availability involves:
  - Ensure availability on Servers
    - Duplication of equipment, in different locations and connected by redundant access;
    - Redundant parts (motherboard, power supply, discs, etc.);
  - Ensure the availability of information
    - Backups, Backups, Backups and more Backups – preferably outside the building where the main equipment is located, e.g. in Cloud;
  - Celebrate Service Level Agreement (SLA) with suppliers
  - Contract that clearly sets the response time to the various possible failures!

Availability of Services

- Plans needed to define and ensure Availability:
  - Business Continuity Plan (BCP)
    - Document that defines the critical information of an organization, that is, the one that if it fails, interrupts the activity of the organization!
  - Disaster Recovery (DR)
    - Recovery plan after an event that generated the complete destruction of information and main equipment (e.g. fires, floods, earthquakes, terrorist attacks, etc.);

Availability of Services

- Business Continuity Plan (BCP)
  - Document that defines the critical information of an organization, that is, the one that if it fails, interrupts the activity of the organization!
  - It is a proactive process that aims to mitigate the risks of information loss;
  - Involves:
    - Systems
    - Processes

Availability of Services

- Business Continuity Plan (BCP)
  - What should be part of an BCP:
    - Define critical information for the company;
    - How this information exists and is mantained;
    - Who are the people responsible for their maintenance;
    - What is the process of maintenance and recovery in case of loss;
    - What are the costs of these processes.
  - It is a succinct and precise document, constantly evolving and improving.

Service Availability
Disaster Recovery

- Disaster Recovery Plan (DR) – Defines how the recovery is made after an event that generated the complete destruction of information and main equipment (e.g. fires, floods, earthquakes, terrorist attacks, computer attacks, etc.);
- It is a reactive process that is supported in BCP.
- Metrics:
  - RTO - Recovery Time Objective - time from disaster until services are available;
  - RPO - Recovery Point Objective - Sets the information assumed to be lost in case of disaster; defines the backup interval; at the limit, the information that is lost is that produced between the last Backup and the moment of the disaster.

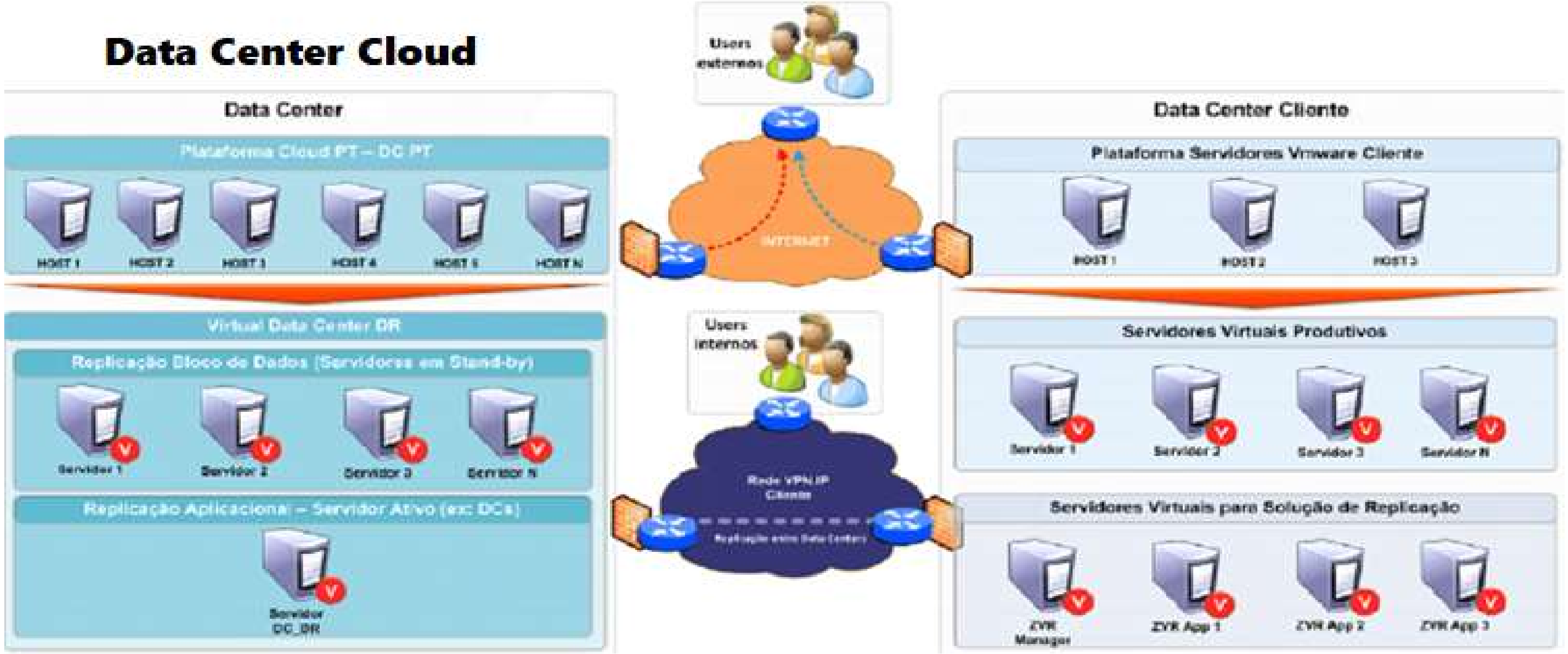
Availability of services
Disaster Recovery

- How to implement Disaster Recovery (DR)
  - Nowadays organizations servers are virtualized, they are software...
  - It's relatively simple to copy, move...
  - Several options:
    - Keep up-to-date copies of servers in location outside the company
    - Duplicate Hardware and servers on the LAN at a point away from the Home DataCenter
    - Create a virtual Data Center in the Cloud that replicates the Primary Data Center
  - Example of permanent server duplication applications:
    - Zerto: https://www.zerto.com/
    - Veeam: https://www.veeam.com/

Example of DR

Supported DR in Cloud:

- Images of virtual servers in a Cloud Data Center
- Backend connections (via VPN on the operator's network) to the Data Center with guaranteed debit in a secure environment;
- Short times for RPO - updating server images;
- Public IP addresses replicated by the Data Center (decreases the RTO).



Load balancing

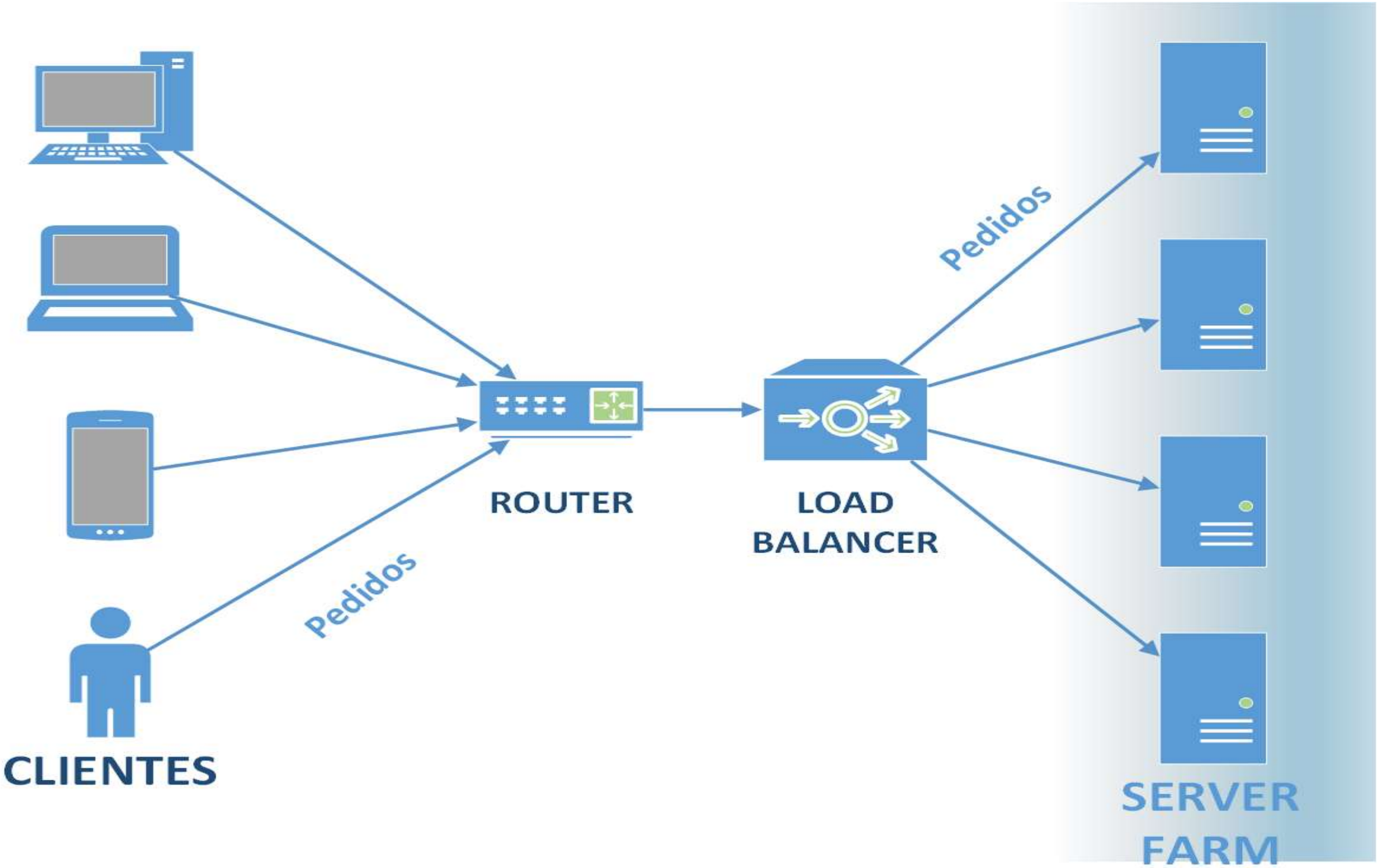
- When a service is only secured by a unique server, it becomes a "Single point of failure":
  - If the server fails, the service fails!
  - Solution: Scale to multiple servers and do Load balancing – split the service provided by a set of servers to maximize performance and ensure redundancy in the event of failure.
  - Fundamental in Data Center service providers.

Load balancing

- Implementation can be made:
  - Proprietary business solutions:
    - Example: Windows Load Balancing Service (WLBS), Network Load Balancing (NLB) or Component Load Balancing (CLB) from Microsoft.
  - Build a server farm (or cluster) – two or more servers that act as if they were one with the intervention of a load balancer that distributes the load.
    - Each server must be able to access the disk(s) of the other(s) server(s);

Load balancing

Build a server farm (or cluster)



Load balancing

- In the farm system, load balancing divides work between servers as evenly as possible to optimize performance and avoid congestion.
  - Basic method: select randomly, sequentially or otherwise, the server handling each request; The server forwards each request alternately to one of the servers.

Load balancing

- Static Methods: The balancer does not know the current state of the servers, only their capacity, and assigns the requests to servers based on this information;
  - Applicable in small DataCenters;
  - Examples: Round-Robin, Threshold Algorithm, etc.
- Dynamic Methods: The balancer records the number of connections already forwarded and still active for each server, and chooses the one that has the least load at the moment.
  - More complex but more efficient in large DataCenters.
  - Example: Least-Connect

Load balancing

- Examples of Load Balancing Appliances:
  - F5 (https://www.f5.com/solutions/traffic-management/load-balancing)
  - Citrix NetScaler (https://www.citrix.com/blogs/2018/06/11/load-balancing-citrix-storefront-ltsr-with-netscaler-and-disa-stigs/)
  - Amazon Elastic Load Balancing (ELB) (https://aws.amazon.com/pt/elasticloadbalancing/)

Chapter Summary

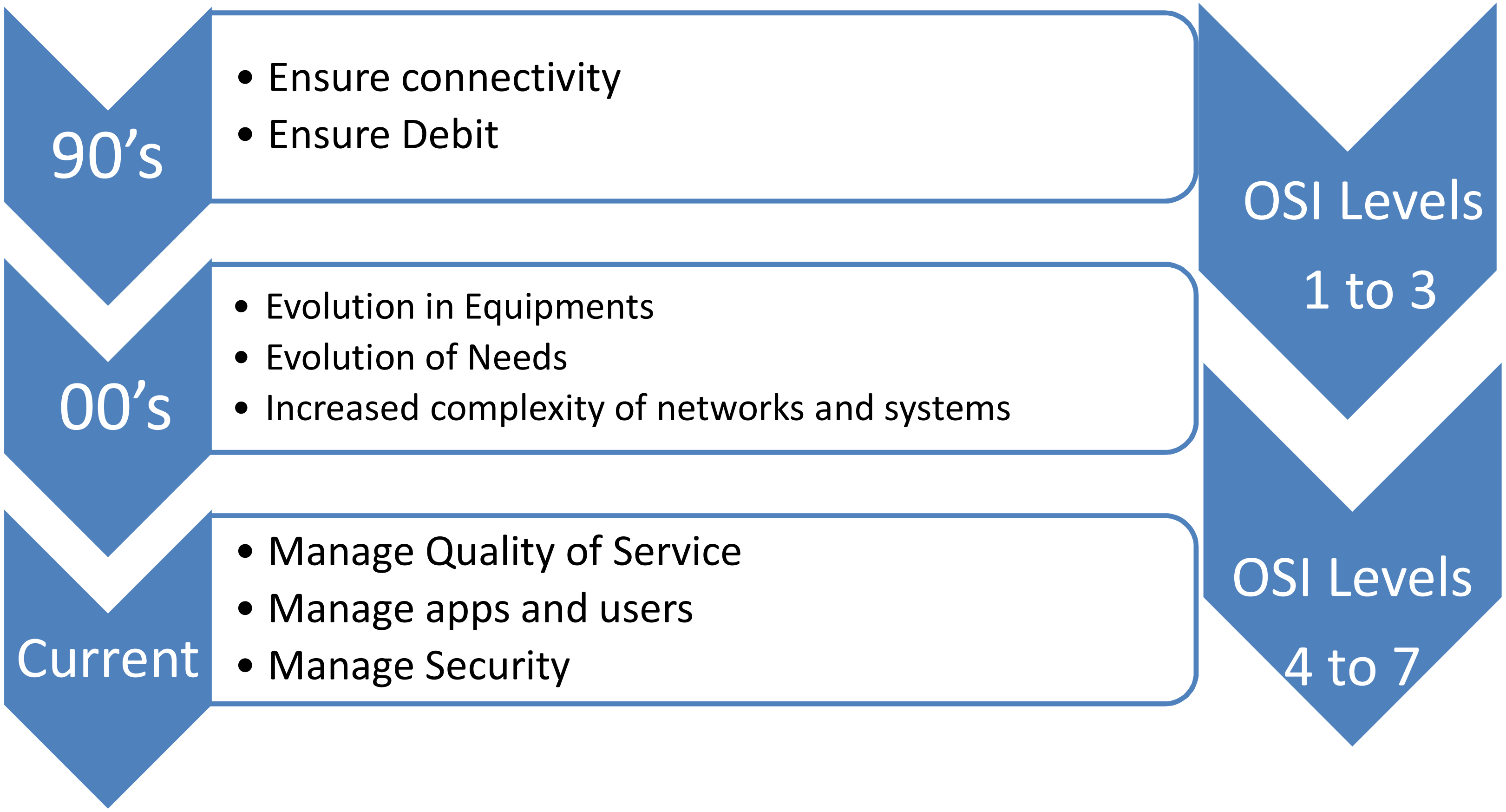
- Data Center Architectures
- Network Assessment and Availability
- Monitoring
  - Network and Systems Monitoring
  - SNMP Architecture
  - WMI Architecture
  - Monitoring tools

Monitoring

- MONITORING is essential for effective management of networks and sistems.
- His motivation derives from the need that the network manager has to know, evaluate, measure and predict the performance of all elements.
- Network KNOWLEDGE, vulnerabilities and threats is a tool that anticipates problems and allows users to experience improved services they need.

Monitoring

- Network management needs have evolved:



90’s

- Ensure connectivity
- Ensure Debit

00’s

- Evolution in Equipments
- Evolution of Needs
- Increased complexity of networks and systems

Current

- Manage Quality of Service
- Manage apps and users
- Manage Security

OSI Levels

1 to 3

OSI Levels

4 to 7

Monitoring

- Some monitoring activities on a computer network:
  - Connectivity of equipment;
  - Service performance;
  - Measurement of parameters;
  - Analysis of traffic and protocols;
  - Detection of intrusions;
  - Technical support to users;
  - …

Monitoring

- NETWORK MONITORING includes a set of tasks and features that are very useful in network management:
  - Detection of breakdowns – by sending alerts or notifications to the manager;
  - Proactive management - detection and correction of anomalies
  - Documentation or inventory of the network;
  - Access to graphic tools about the status of networks, equipment, services and traffic;
  - Measurements and performance evaluation taking into account required service levels.

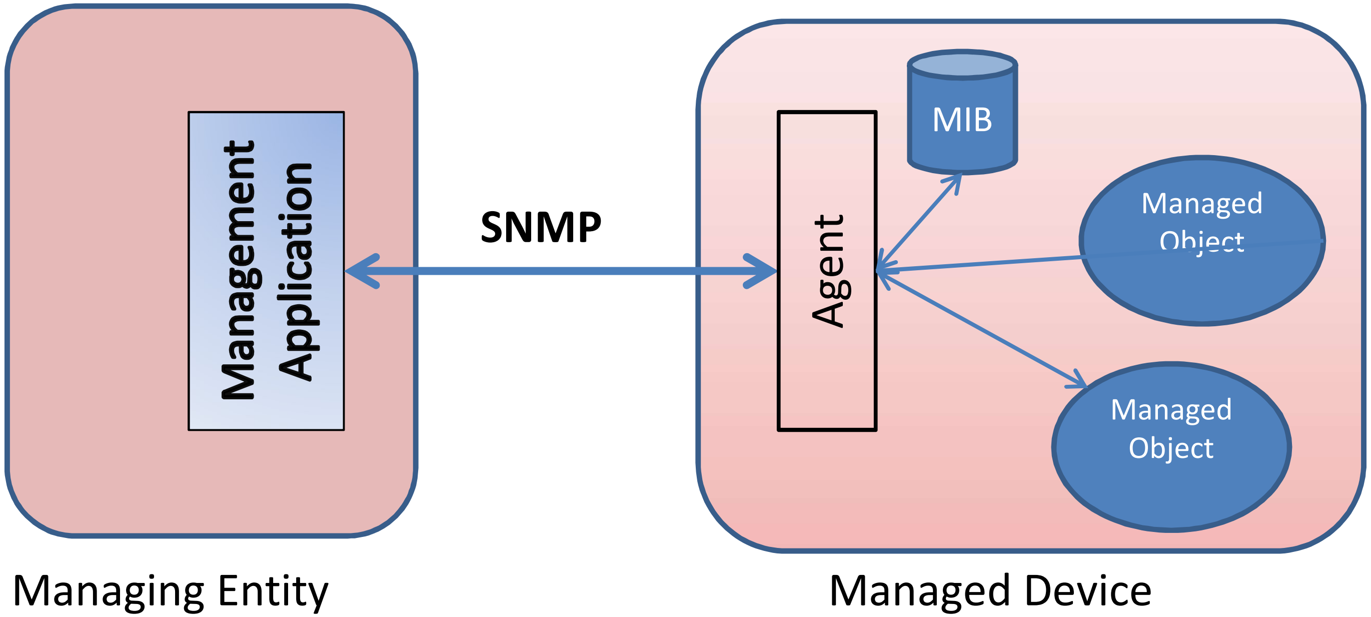
SNMP Architecture

- The most commonly used architecture is the SNMP – Simple Network Menagement Protocol
  - Normalized by IETF in 1990 and is now in the SNMPv3 version; https://searchnetworking.techtarget.com/feature/The-fundamentals-of-availability-monitoring-tools
  - Components:
    - One or more coordinated management entities - MIB RMON;
    - Management Agents;
    - MIB
  - Modular architecture
    - SMI language - defines how information is structured in MIB
    - Definition of the type of information to store
    - SNMP protocol for communication
    - Information security features

SNMP Architecture

- Network management components:
  - Managing entity - application that centralizes information and alerts about network activity and allows the management of devices;
  - Managed device (menaged devices) – any device on the network and its software. Contains one or more managed objects (interfaces, software, etc.) whose information is stored in an MIB – management information base. On each device runs a process called agent that is in charge of communicating with the managing entity.
  - Management Protocol - form of communication between the managing entity and the agents.

SNMP Architecture



Exemplos:
Management Application: NAGIOS, MRTG, Spiceworks, etc.
Managed Object: Network Card, CPU, Memory, etc.

SNMP PROTOCOL

- Regulates communication between the managing entity and the agents located on the managed objects/devices;
- Seven types of messages (PDU, use port 161)
  - GetRequest, GetNextRequest, GetBulkRequest – from management entity to agents to ask for information;
  - SetRequest – from management entity to agents to change information;
  - InformRequest – exchange of information between managers
  - Trap – alert sent by the agent
  - ResponsePDU – agent's response to GET and SET.

MIB

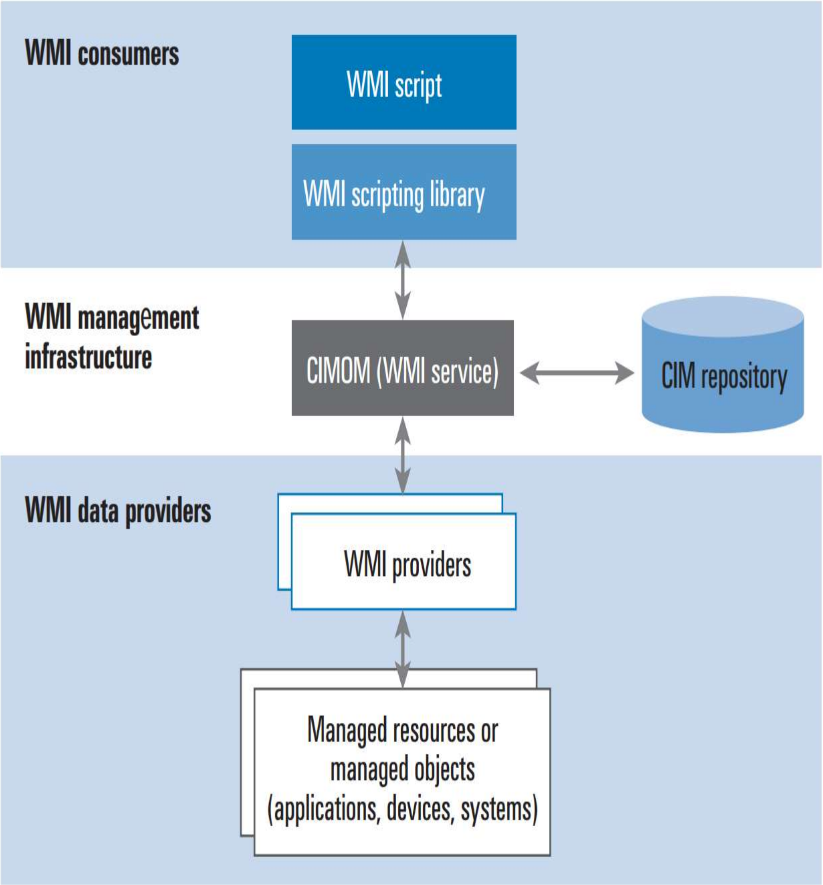
- MIB – *Menagement Information Base*
  - MIB modules gather information from the objects to be monitored on a network;
  - It is an ASCII File with the formal description of objects on a device. The managing entity must compile this file in order to interpret it.
  - Each object includes an identifier (OID) in hierarchical format
  - To identify objects, it uses a specific language for the structure of the data (SMI - Structure of Management Information)

WMI

- WMI - Windows Management Instrumentation
  - On Windows systems, WMI is the structure typically used for monitoring
  - Allows you to obtain data from Windows equipment (PC's, Servers, etc.) with more information than via SNMP.
  - Through WMI you can manage computers locally or remotely (as long as you have the necessary permissions) by collecting data and changing the state of the corresponding objects and physical entities, whether they are hardware or software (services, accounts of users...).

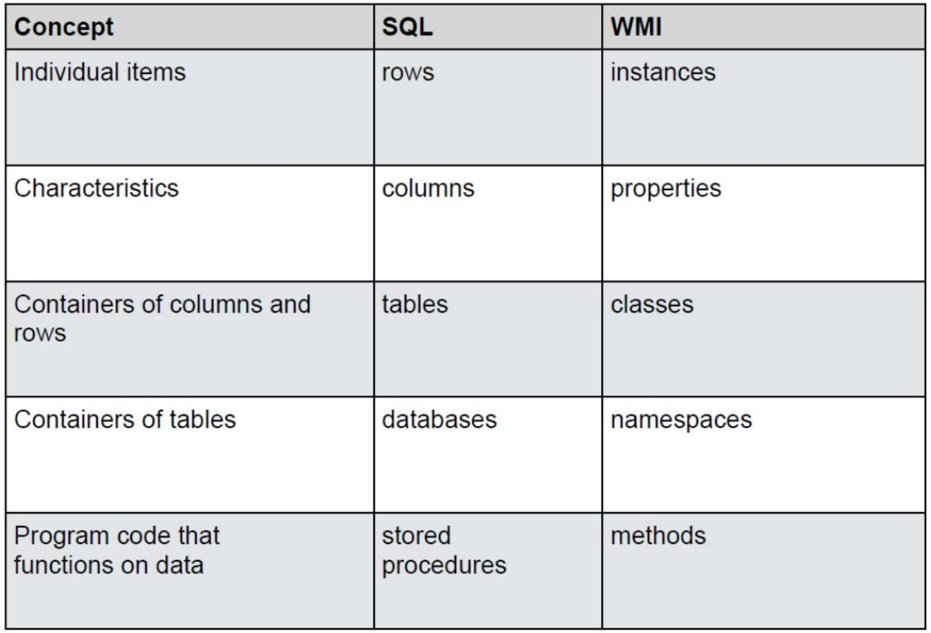
WMI Architecture

- WMI Architecture:
  - Consumers: system that receives and treats information - e.g. monitoring software
    - Access to monitoring information is done through scripts in any language that allows the control of Microsoft ActiveX objects (e.g. C, C++, Python, VB Scripts, etc.).



WMI Architecture

- WMI Architecture:
  - Data Providers: system that reads the information of managed resources.
  - Information is organized in the Windows Query Language (WQL) language that follows a framework similar to SQL:



Concept	SQL	WMI
Individual items	rows	instances
Characteristics	columns	properties
Containers of columns and rows	tables	classes
Containers of tables	databases	namespaces
Program code that functions on data	stored procedures	methods

WMI Architecture

- WMI Architecture:
  - WMI Infrestructure
    - Windows OS component that controls and defines communication between consumers and providers
    - This is where classes are defined, for example.

Impact on network infrastructure

- The activation of monitoring systems have impacts on network infrastructures that should not be neglected:
  - Bandwidth consumption, in particular in network scans;
  - Enabling features on devices that involve opening ports that can be used by third parties to access user and system information.
  - Be careful to configure firewalls to allow communication of monitoring protocols.

MONITORING SYSTEMS

- They should not only allow them to verify connectivity but also performance and availability of services.
- Analysis of existing solutions
  - Commercial products – comprehensive in functionalities, with significant costs and adapted to homogeneous means.
  - Examples: HP BTO (Business Technology Optimization) , CiscoWorks, IBM Tivoli e outras

MONITORING SYSTEMS

- Open Source Offer:
  - Set of tools available independent of manufacturers.

  Most common examples:
  - MRTG – measures performance and traffic on the network
  - NAGIOS – inventory and management platform
  - Spiceworks ou PRTG – examples of opensource inventory and monitoring platforms with web interface

spiceworks

PRTG NETWORK MONITOR

Chapter 5

Doubts?