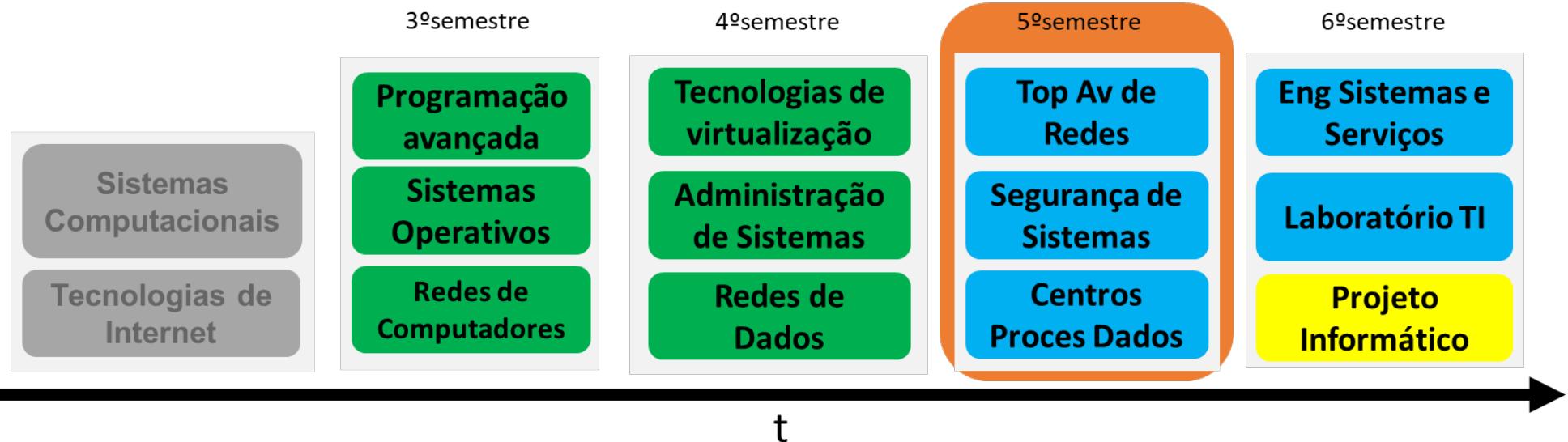


Apresentação e revisões

1. Funcionamento geral da comunicação TCP/IP
2. Tópicos fundamentais de redes de computadores
3. Tópicos fundamentais de administração de sistemas
4. Revisões

Roadmap



Put it all together!



Enquadramento

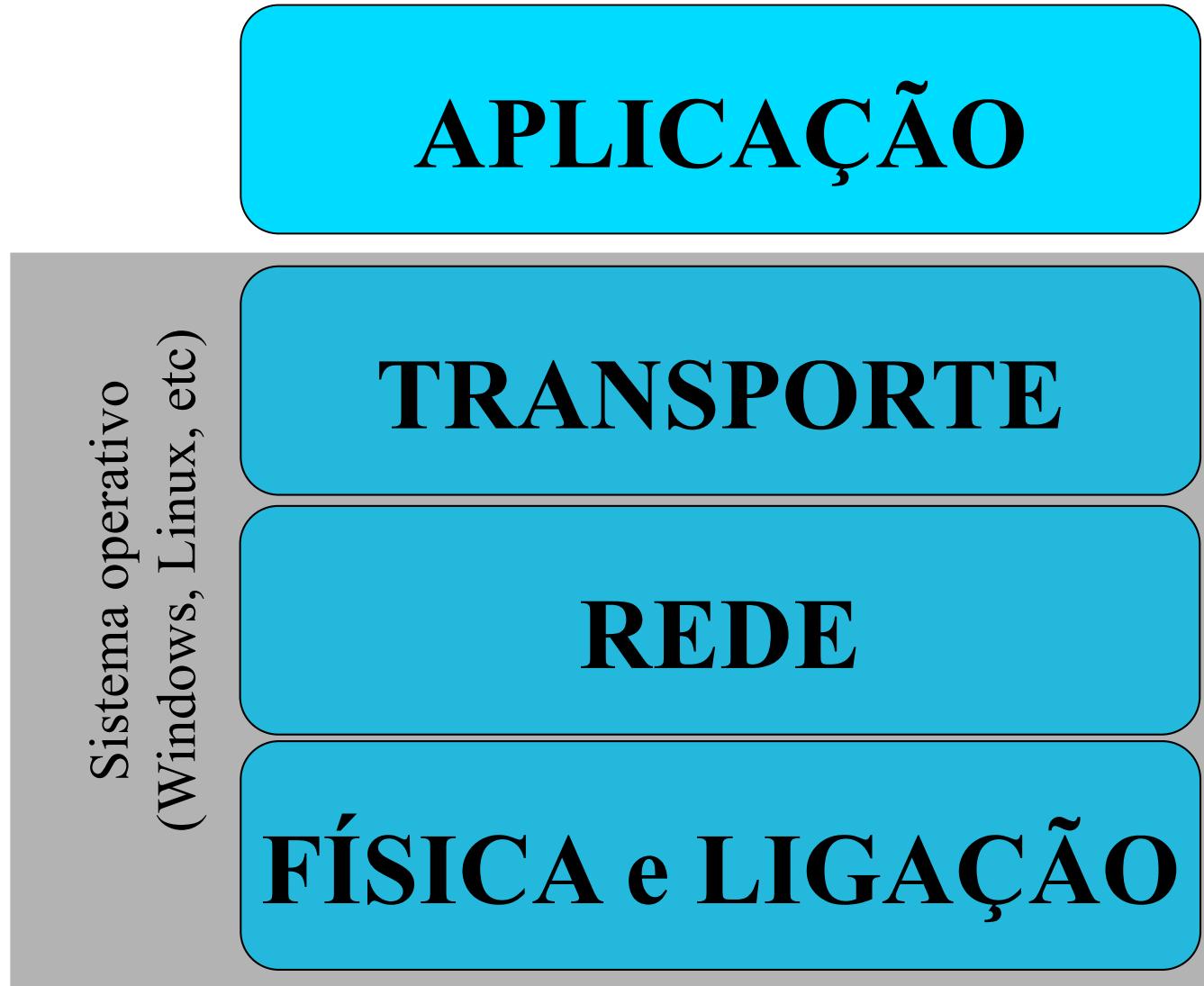
Sistemas
Operativos

Redes de
Computadores

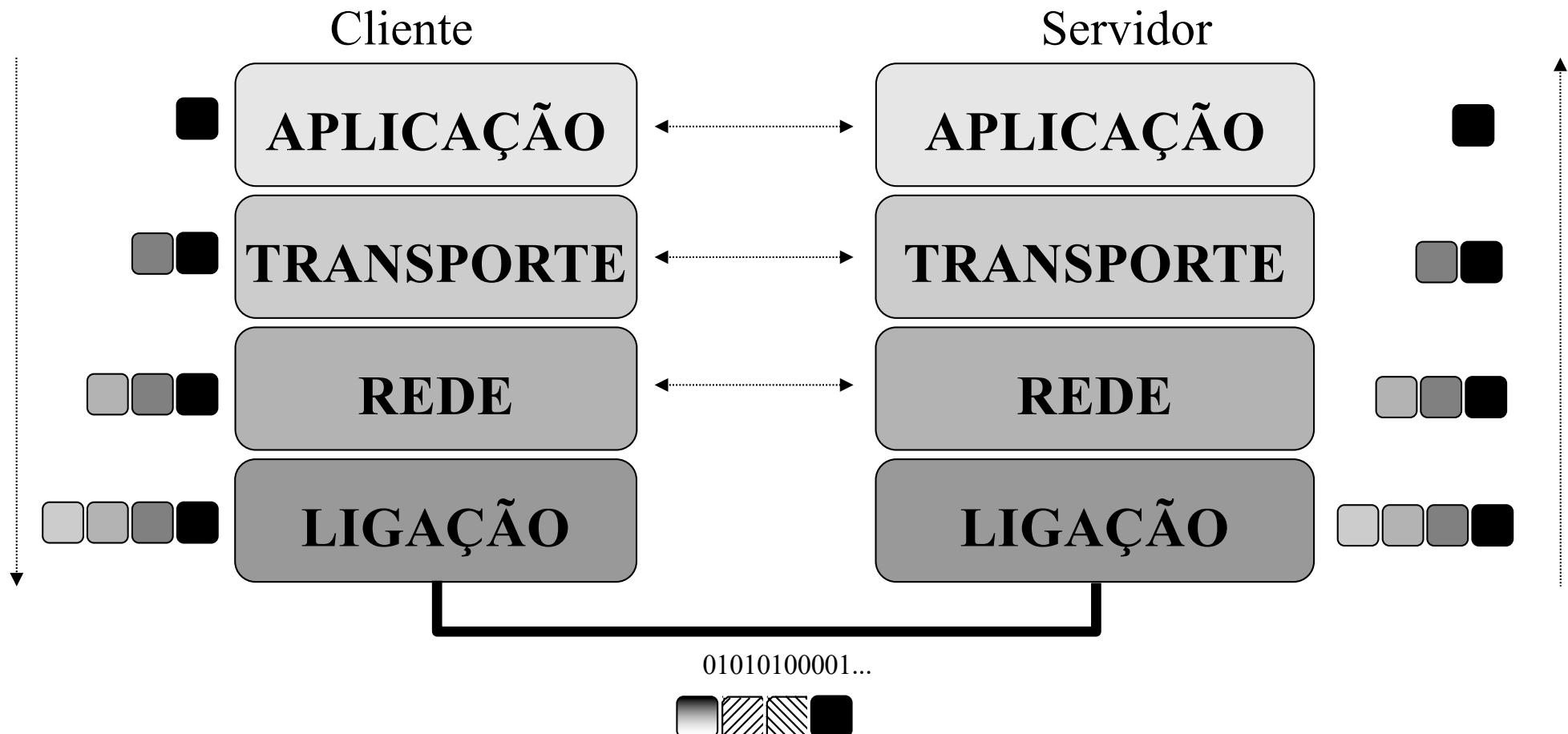
Administração de
Sistemas

Tecnologias de
Virtualização

Revisões – Redes de Computadores



Modelo de comunicação TCP/IP



Tópicos fundamentais de redes



- Funcionamento geral da Internet
- Encapsulamento TCP/IP e estrutura protocolar
- Controlo de erros e de fluxo
- Cablagem estruturada
- Tecnologia Ethernet
- Endereçamento MAC
- (Sub)endereçamento IP (v4|v6)
- Encaminhamento IP
- Fragmentação e agupamento IP

Tópicos fundamentais de redes



- Principais protocolos de transporte: TCP e UDP
- Noção de porto e socket
- Comunicação “cliente-servidor” e noção de 3WH
- Routing versus Switching
- Proxy versus NAT/PAT
- Configuração de NAT
- Noção de VLAN e encaminhamento Inter-VLAN
- Principais protocolos/serviços aplicacionais
- Configurar equipamentos Cisco IOS

Revisões – Sistemas operativos



- Noção de programa
- Noção de processo e subprocesso
- Noção de thread
- Estrutura da diretórias e ficheiros essenciais em Linux/Windows
- Servidores aplicacionais: iterativos, concorrentes, híbridos
- Comandos básicos e intermédios de administração
- Configuração e gestão de serviços

Revisões – Sistemas operativos



- Aplicações fundamentais:
 - netstat
 - ifconfig
 - nslookup
 - wireshark
 - tcpdump
- Troubleshooting

Revisões - Administração de Sistemas



OS	Users	Tasks	Processors
MS/PC DOS	S	S	1
Windows 3x	S	QM	1
Macintosh System 7.*	S	QM	1
Windows 95/98/ME	S	M*	1
AmigaDOS	S	M	1
Unix-like	M	M	<i>n</i>
VMS	M	M	<i>n</i>
NT-like	S/M	M	<i>n</i>
Windows 2000/XP	M	M	<i>n</i>
OS390 (zOS)	M	M	<i>n</i>

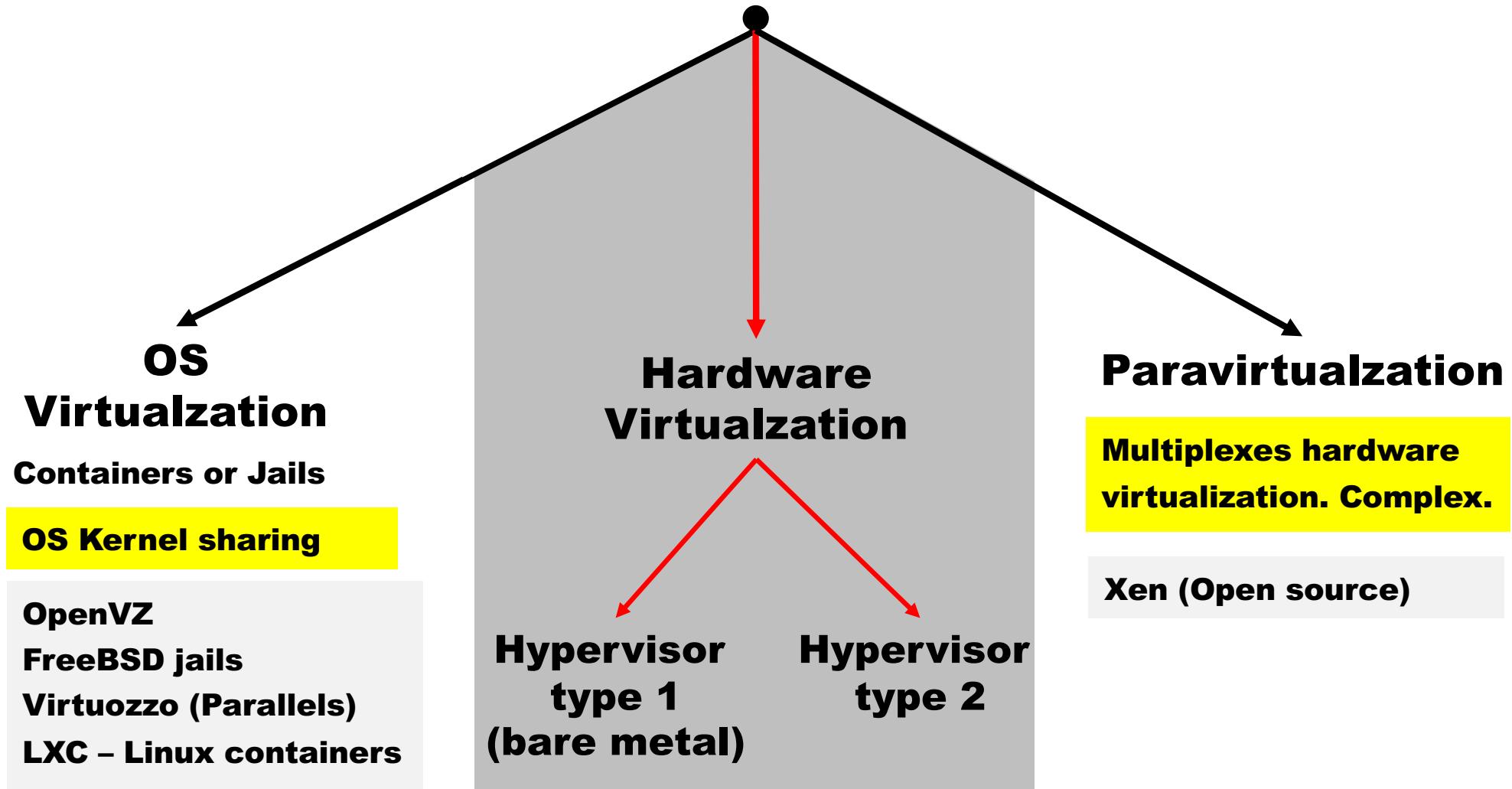
Unix-like OS	Manufacturer	Type
BSD	Univ. California Berkeley	BSD
SunOS (Solaris 1)	Sun Microsystems	BSD/Sys V
Solaris(2)	Sun Microsystems	Sys V/BSD
Tru64	DEC/Compaq/HP	BSD/Sys V
HPUX	Hewlett Packard	Sys V
AIX	IBM	Sys V / BSD
IRIX	Silicon Graphics	Sys V
GNU/Linux	GPL Free Software	Posix (Sys V/BSD)
MacOS X	Apple	BSD/Sys V
Unixware	Novell	Sys V



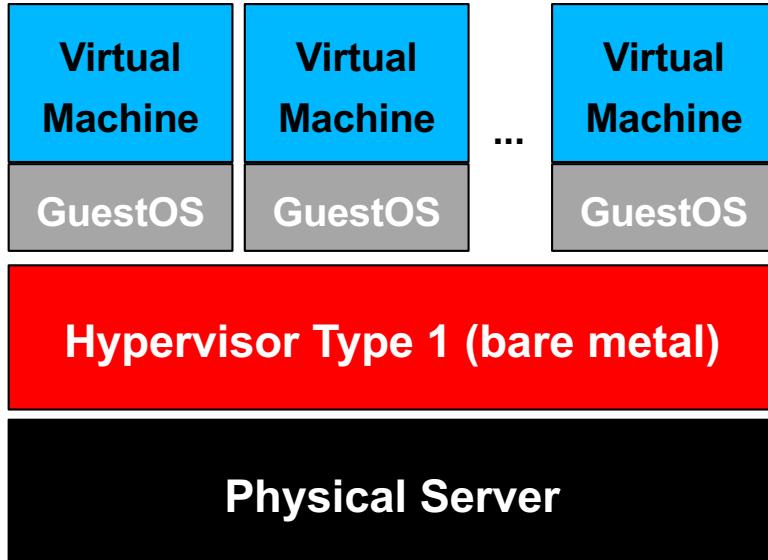
redhat.



Cloud technology - virtualization



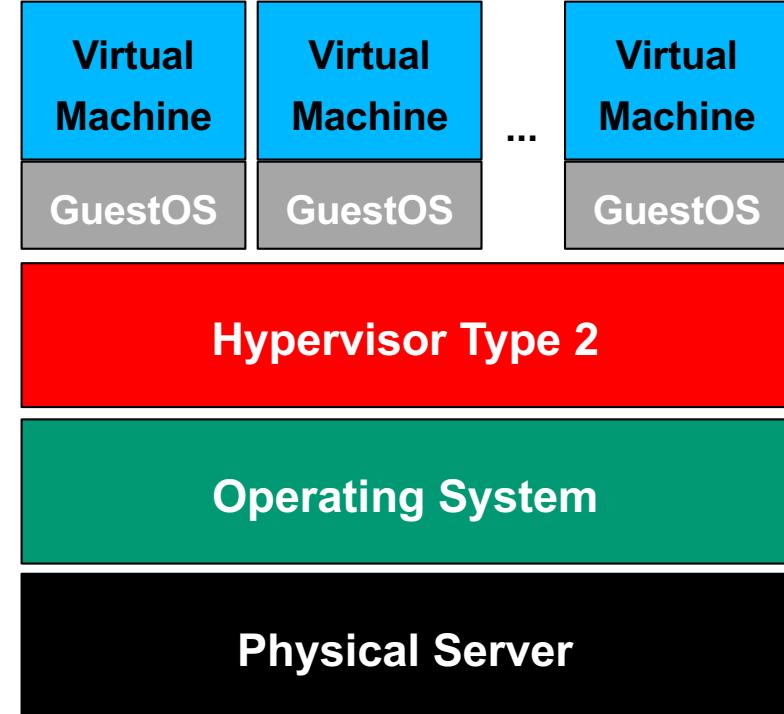
Revisões – Tecnologias de Virtualização



VMware ESX (vSphere)

Microsoft Hyper-V

Xen variants



VMware Workstation Player

Microsoft Virtual Player

Oracle VirtualBox

Revisões – Administração de Sistemas



Troubleshooting

Log analysis and monitoring applications

Business application servers

Networking services and ports

Disks

Partitions

Filesystems

Backups

Processes

CPU load

SWAP area

Virtual memory

Interfaces

Routing

IP config

Internet access

Storage management

CPU and memory

Networking

Install Kernel

Startup / Shutdown

Install software

Programming languages, scripting and CLI

Conceitos fundamentais



- Instalar sistema operativo
- Instalar aplicações
- Gerir contas e controlos de acesso
- Gerir partições, filesystems e ficheiros
- Configurar serviços fundamentais de rede
- Gerir logs
- Automatizar tarefas de administração
- Definir e desenvolver políticas de backups
- Escalonar temporalmente a execução de processos



- DNS
- SMTP
- HTTP
- SSH
- (...)

Conceitos fundamentais



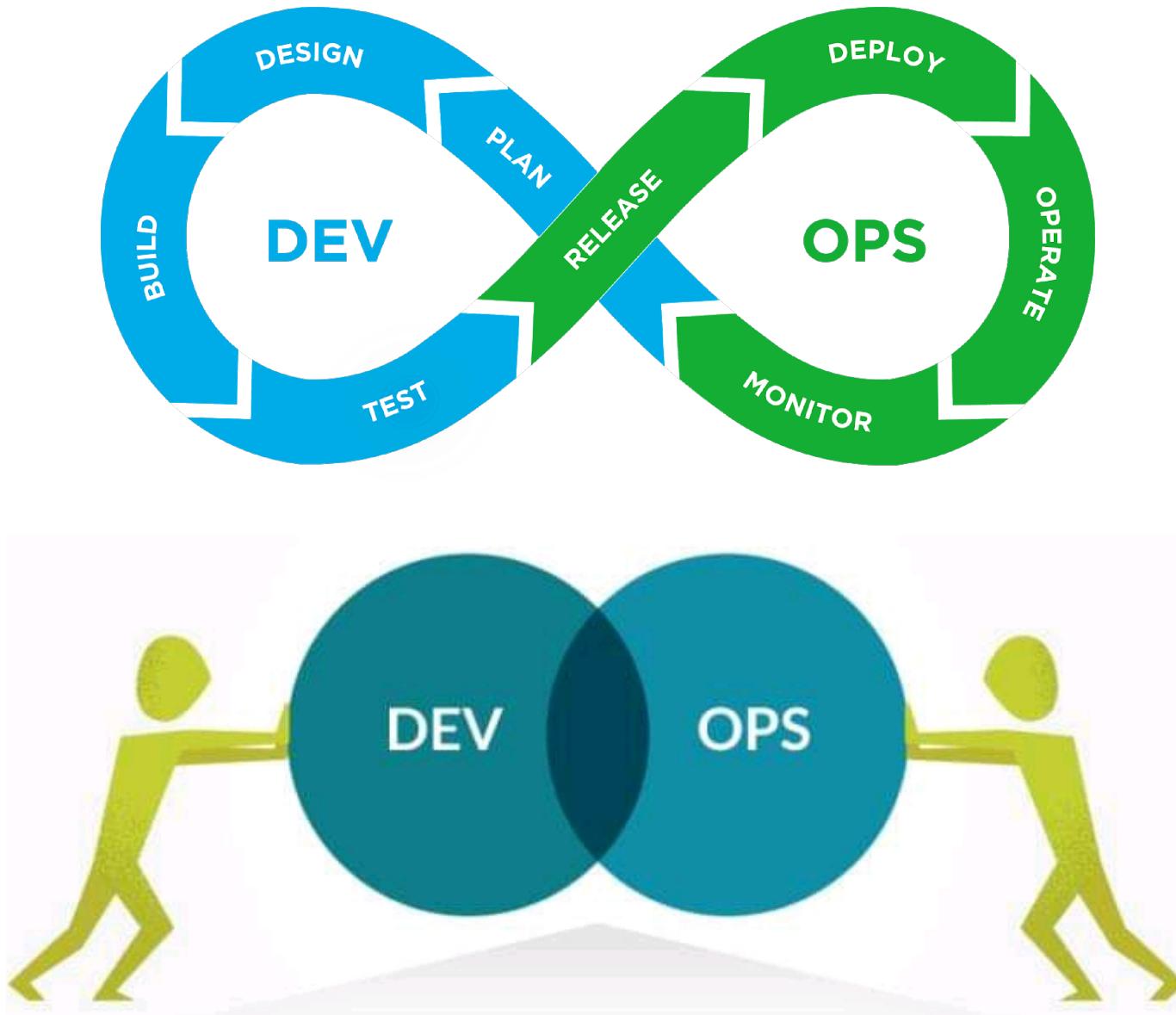
Processo de paragem/arranque

Metodologia para configuração de serviços

Bases de Dados

Gestão web centralizada

Gestão via linha de comandos



DevOps is a culture, not a role!

<https://medium.com/@neonrocket/devops-is-a-culture-not-a-role-be1bed149b0>

Stay focused

- Cloud architecture and services
- Big data analysis
- Software Defined Networks (SDN)
- “Smart things”
- AI and Machine Learning
- Site Reliability Engineering (SRE)
- DevOps
- Back (always) to basics!
- Cybersecurity
- Cloud Computing
- Virtualization
- Resilient networks
- Internet of Things (IoT)

Stay focused



- Home page updated
- Join to R&D pages, software and hardware manufacturers



- Join to R&D pages, software and hardware manufacturers

To follow important, up-to-date, useful, ... and standard information:

RFC*Editor*



NIST

Gartner®

The Internet Protocol Journal

To use digital libraries with up-to-date and relevant R&D information

Google
scholar

ic
online
instituto politécnico de leiria



IEEE

Bibliografia

- “*TCP/IP – Teoria e prática*”; *Fernando Boavida e Mário Bernardes; FCA;* ISBN: 978-972-722-745-7
- “*Gestão de Sistemas e Redes em Linux*”; *Jorge Granjal; FCA;* ISBN: 978-972-722-784-6
- “*Computer Networking, A top-down approach featuring the Internet*”; *Kurose, Ross, 6ed. (Cap.4); Addison Wesley*
- RFC: 791, 793 (www.rfc-editor.org)

Cloud computing - Introduction

1. Fundamentals on cloud computing
2. Cloud characteristics
3. Cloud service models
4. Cloud implementation models
5. Cloud technology
6. Standardization
7. Cloud bigdata
8. Final remarks

Fundamentals on cloud computing

According to NIST¹:

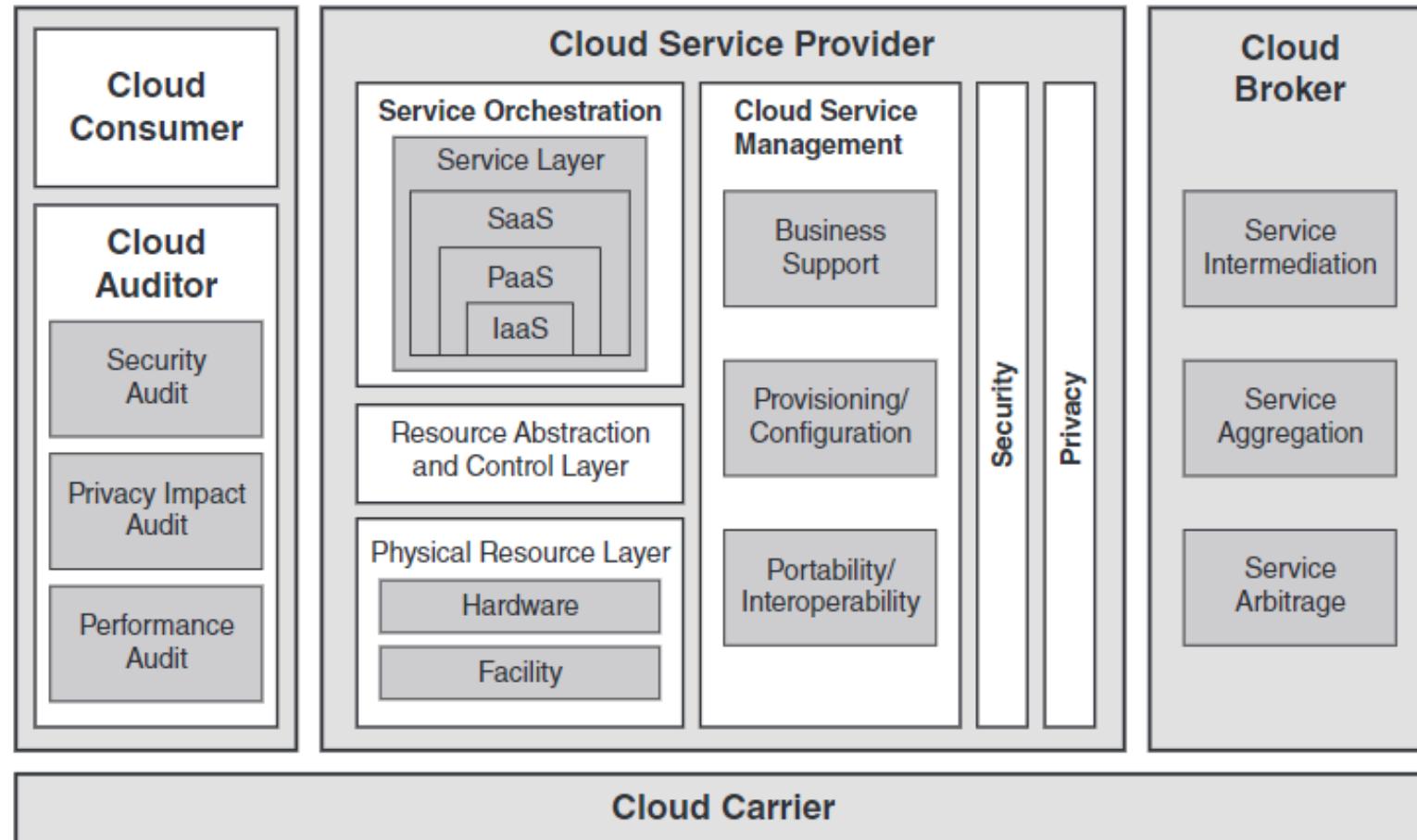


*“Cloud computing is a **model** for enabling **ubiquitous, convenient, on-demand** network access to a shared pool of **configurable computing resources** (e.g., networks, servers, storage, applications, and services) that can be rapidly **provisioned and released** with minimal management effort or service provider interaction.*

*This cloud model is composed of **five essential characteristics**, **three service models**, and **four deployment models**. ”*

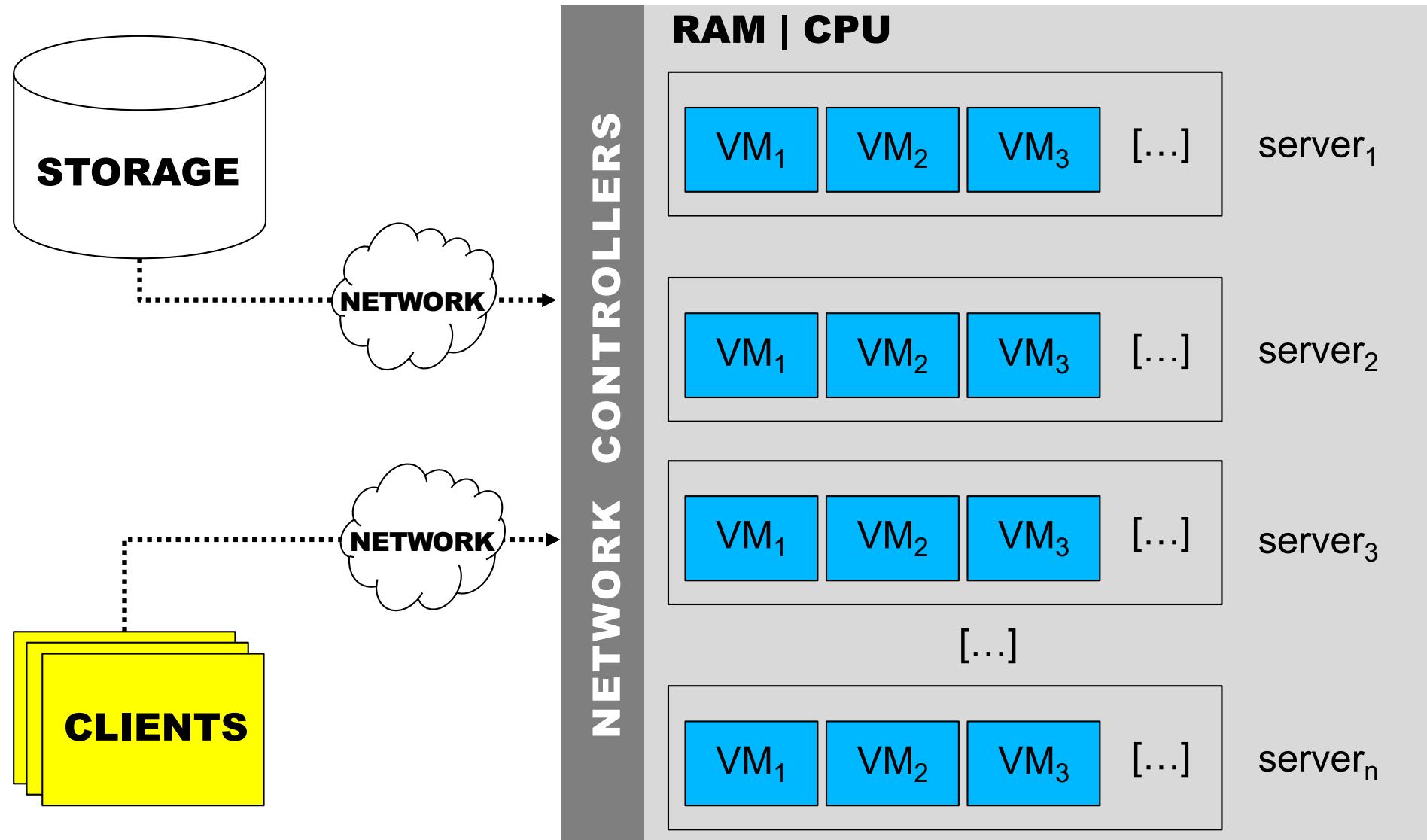
¹ The NIST Definition of Cloud Computing; <http://csrc.nist.gov/>.

Fundamentals on cloud computing



The Official (ISC)2® Guide to the CCSPSM CBK®, Second Edition
Adam Gordon; John Wiley & Sons, Inc, 2016

Fundamentals on cloud computing



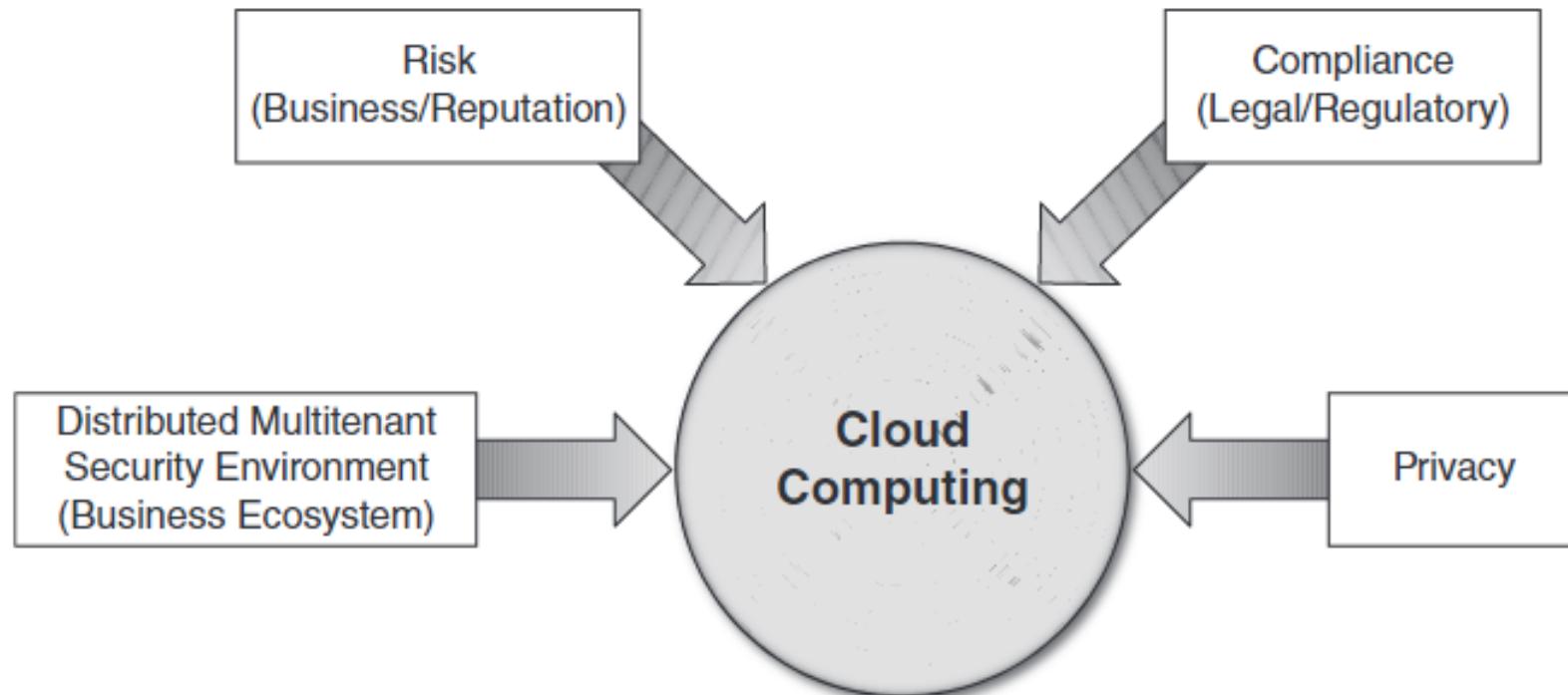
Fundamentals on cloud computing - challenges

- Investment on IT infrastructure CAPEX versus OPEX

- The desire to reduce IT complexity
 - Risk reduction
 - Scalability
 - Elasticity
- Consumption-based pricing
 - Risk reduction
 - Elasticity
- Business agility
 - Mobility
 - Collaboration and innovation

Fundamentals on cloud computing

Security, risks and compliance



The Official (ISC)2® Guide to the CCSP™ CBK®, Second Edition
Adam Gordon; John Wiley & Sons, Inc, 2016

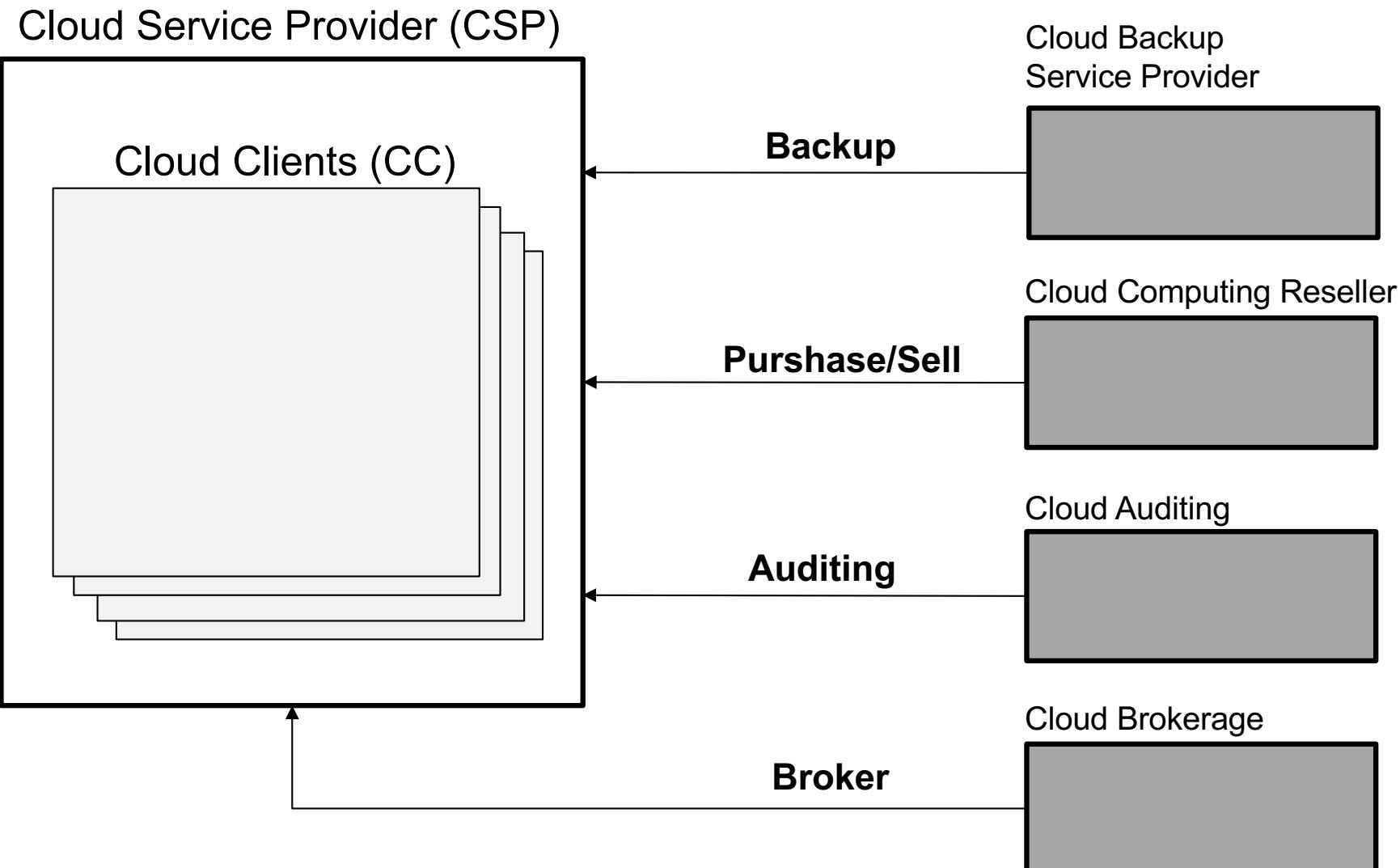
Fundamentals on cloud computing

Cloud \neq $\begin{cases} \text{technology itself} \\ \text{only virtualization} \end{cases}$

Cloud = $\begin{cases} \text{is “real” and exists} \\ \text{has a known geographic location} \end{cases}$

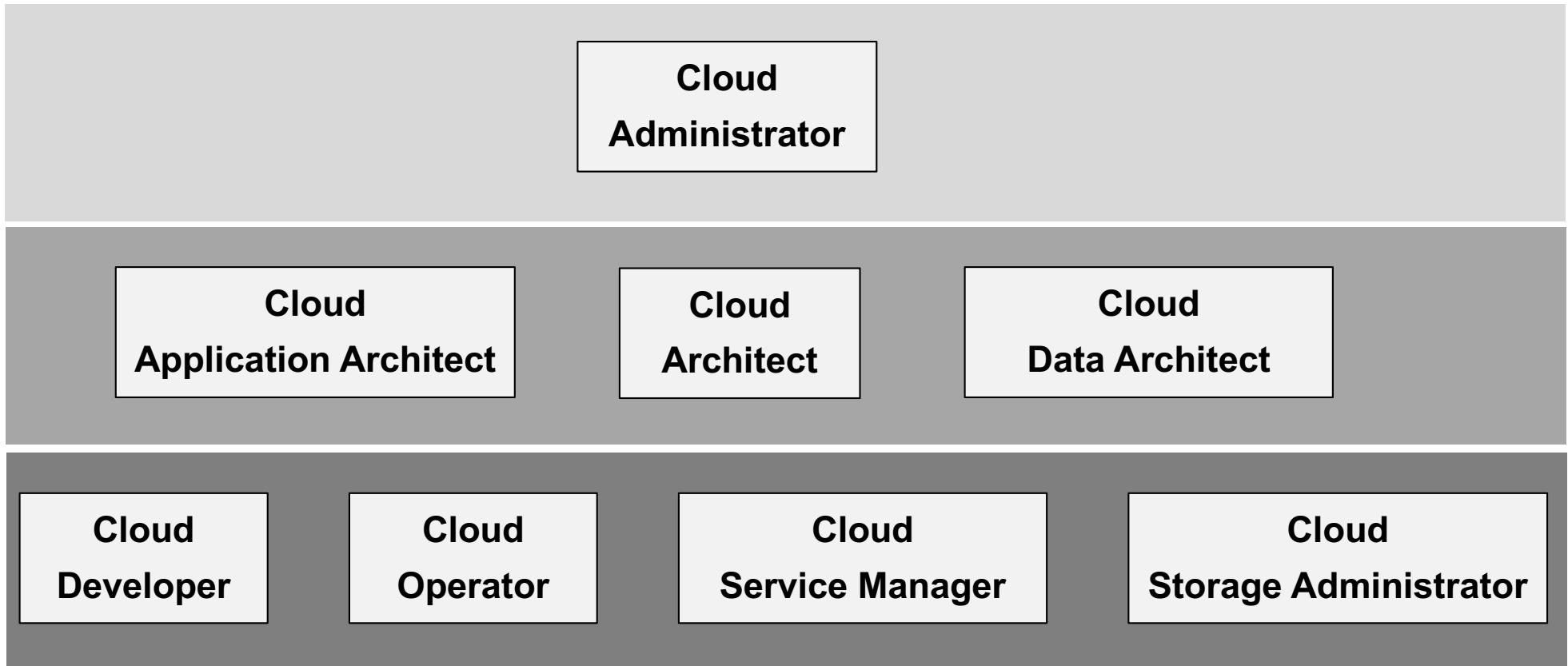
Cloud = $\begin{cases} \text{Abstract concept and IT model} \\ \text{IT technology independent ...} \\ \dots \text{but grounded on real IT resources} \end{cases}$

Cloud roles



The Official (ISC)²® Guide to the CCSPSM CBK[®], Second Edition
Adam Gordon; John Wiley & Sons, Inc, 2016 (pp.12)

Cloud functions



The Official (ISC)2® Guide to the CCSP™ CBK®, Second Edition
Adam Gordon; John Wiley & Sons, Inc, 2016 (pp.16-17)

Fundamentals on cloud computing

Five characteristics

- *On-demand self service*
- *Broad network access*
- *Resource pooling*
- *Rapid elasticity*
- *Measured service*

The NIST Definition of Cloud Computing;
<http://csrc.nist.gov/>



Three service models

- *Software as a Service (SaaS)*
- *Platform as a Service (PaaS)*
- *Infrastructure as a Service (IaaS)*
- **aaS*

Four implementation models

- *Private cloud*
- *Public cloud*
- *Hybrid cloud*
- *Community cloud*

Service models

IaaS - Infrastructure as a Service

PaaS – Platform as a Service

SaaS – Software as a Service

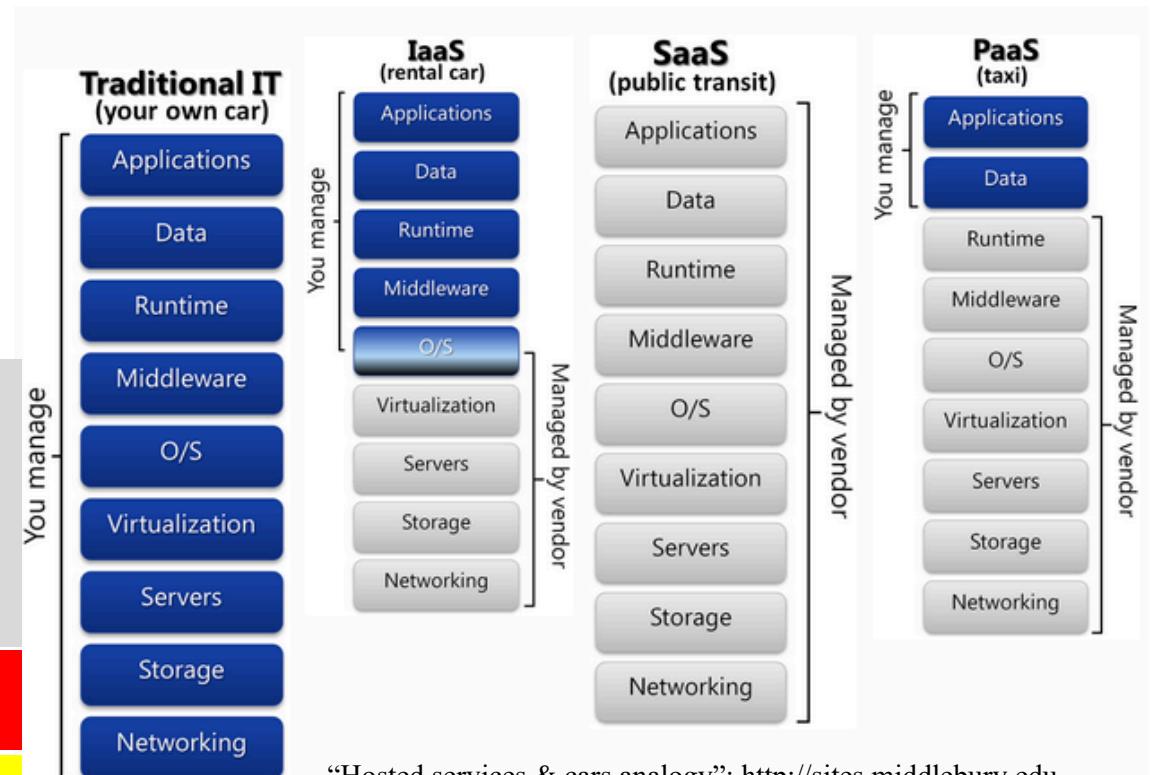
DBaaS – Database as a Service

BaaS – Billing as a Service

NaaS – Network as a Service

MaaS – Malware as a Service

***aaS** – “anything” as a Service



“Hosted services & cars analogy”; <http://sites.middlebury.edu>

How strong is your level of “independence“ from the cloud provider?

What is being managed by you, *versus* by the cloud provider?

Service models – IaaS

- **Resources made available by cloud provider:**
 - Almost everything!
 - Install and manage computational fundamental resources: storage, memory, CPU and network
 - Install and run programs: OS and applications
 - Control over OS and some IP networking configurations
- **User controls everything but the hardware used.**

Service models – IaaS - providers

Amazon Web Services aws.amazon.com	8 zonas (4 continentes)	EC2 (<i>compute</i>), S3 (<i>storage</i>)	0,0500 € ou \$ 0,0650 para 1.7 GB RAM, 1 CPU, 160 GB DISK
Rackspace Cloud www.rackspacecloud.com	3 zonas (3 continentes)	Cloud Servers, Cloud Files	0,0170 € ou \$ 0,0220 para 0.5 GB RAM, 1 CPU, 20 GB DISK
HP Cloud www.hpcloud.com	2 zonas (1 continente)	Cloud Compute, Cloud Object Storage	0,0307 € ou \$ 0,0400 para 1 GB RAM, 1 CPU, 30 GB DISK
GoGrid www.gogrid.com	3 zonas (2 continentes)	Cloud Servers, Cloud Storage	0,0307 € ou \$ 0,0400 para 0.5 GB RAM, 0.5 CPU, 25 GB DISK
Lunacloud www.lunacloud.com	2 zonas (1 continente)	Cloud Servers, Cloud Storage	0,0155 € ou \$ 0,0200 para 0.5 GB RAM, 1 CPU, 10 GB DISK
Joyent www.joyent.com	4 zonas (2 continentes)	SmartMachine	0,0230 € ou \$ 0,0300 para 0.5 GB RAM, 1 CPU, 15 GB DISK
ElasticHosts www.elastichosts.com	1 zona (1 continente)	Cloud Hosting	0,0920 € ou \$ 0,1200 para 1 GB RAM, 1 CPU, 10 GB DISK
Microsoft Azure www.azure.microsoft.com	17 zonas (4 continentes)	Virtual Machines Storage	0,0144 € ou \$ 0,0180 para 0.75 GB RAM, 1 CPU, 30 GB DISK

EC2 – Elastic Compute Cloud

Cloud regions and zones

António Miguel Ferreira;
“Introdução ao Cloud Computing”;
FCA; ISBN: 978-972-722-802-7; 2015
(Portuguese)

Service models – IaaS - providers

Gartner's *Magic Quadrant* for IaaS cloud providers **2019** **2020** 



Source: Gartner (July 2019)

Quadrant for service models also available at <http://www.gartner.com>.



Service models – IaaS - nomenclature

- Main characteristics of storage in the cloud:
 - Speed
 - Resiliency
 - Accessibility
 - Measured in GB

- About nomenclature:

S3 – Simple Storage Service



Cloud Storage

EBS – Elastic Block Store



Cloud Files

Glacier



Cloud Block Storage

Service models – IaaS - interoperability

- Each provider has its own API for management and development
- Convencional method: web interface

Problems – each provider has its own API

Effect – migration between cloud providers becomes hard. Need to deal with different APIs.

Solution – To adopt ongoing standard APIs and access methods, like Openstack used with REST API. 

To use *cloud brokers* and *cloud aggregators*

 Gravitant

Service models – PaaS

- **Resources made available by cloud provider:**
 - In house developed applications or purchased software packages
 - Programming languages compilers and libraries
 - Software versioning and revision control system
 - Aim: to use cloud as a software development platform
- **User has very little control over cloud infrastructure.**

Service models – PaaS - providers

Services and Platforms			
Heroku www.heroku.com	AWS USA (1 continente)	Ruby, Node.js, Clojure, Java, Python, Scala, Postgres, Mongo, Hadoop, etc.	\$ 0,05/hora para 1 processo + + \$ 9/mês para 1 base de dados
Nodejitsu www.nodejitsu.com	Joyent USA (1 continente)	Node.js	\$ 2,5/mês para 1 processo
Google App Engine www.appspot.goo- gle.com	13 zonas (4 continentes)	Java, Python, Go	\$ 0,05/hora para 1 app
CloudBees www.cloudbees.com	AWS USA, Europa, HP (3 continentes)	Java	\$ 60/mês para 5 GB de código e 2 processos
Appfog www.appfog.com	AWS USA, Europa, Ásia, Rackspace, HP, Azure (3 continentes)	Java, Scala, Python, Node.js, PHP, Ruby, Erlang, MongoDB, MySQL, Postgres	\$ 20/mês para 8 processos, até 2 GB RAM e 250 MB dados
dotCloud www.dotcloud.com	AWS USA (1 continente)	PHP, Node.js, Python, Ruby, Perl, Java, MySQL, MongoDB, Postgres	\$ 8,64/mês
OpenShift www.openshift.com	AWS USA (1 continente)	PHP, Node.js, Python, Ruby, Java	\$ 0,02/hora

António Miguel Ferreira; "Introdução ao Cloud Computing"; FCA; ISBN: 978-972-722-802-7; 2015 (Portuguese)

Service models – SaaS

- **Resources made available by cloud provider:**
 - Applications stored on the cloud.
 - Applications accessed through HTTP, usually via web browser
 - Billing (examples): storage, number of accounts, duration and/or functionalities provided
- **User has no control over the cloud applications. Little control on some configuration features.**

Service models – SaaS - providers

Google Apps



Microsoft Office365



iCloud



Mailchimp



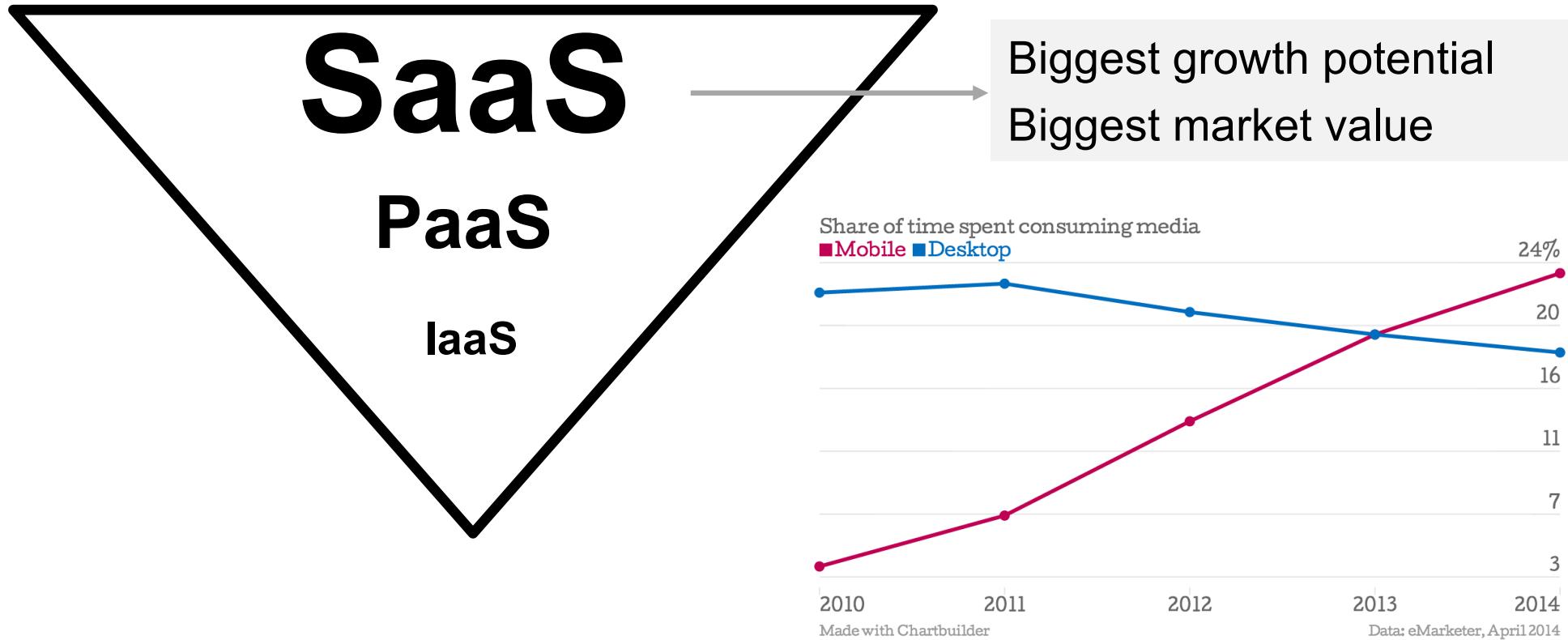
SAP BusinessOne



ServiceNow – Troubleticket service**now**

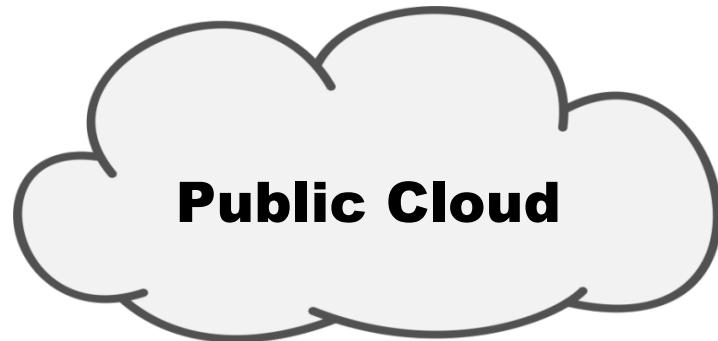
LogicMonitor – IT infrastructure monitoring Logic**Monitor**

Service models – a market perspective



Why? Mainly due to growing development for mobile devices iOS e Android:
Examples: Google Apps, Evernote, Dropbox, Facebook, Shazam

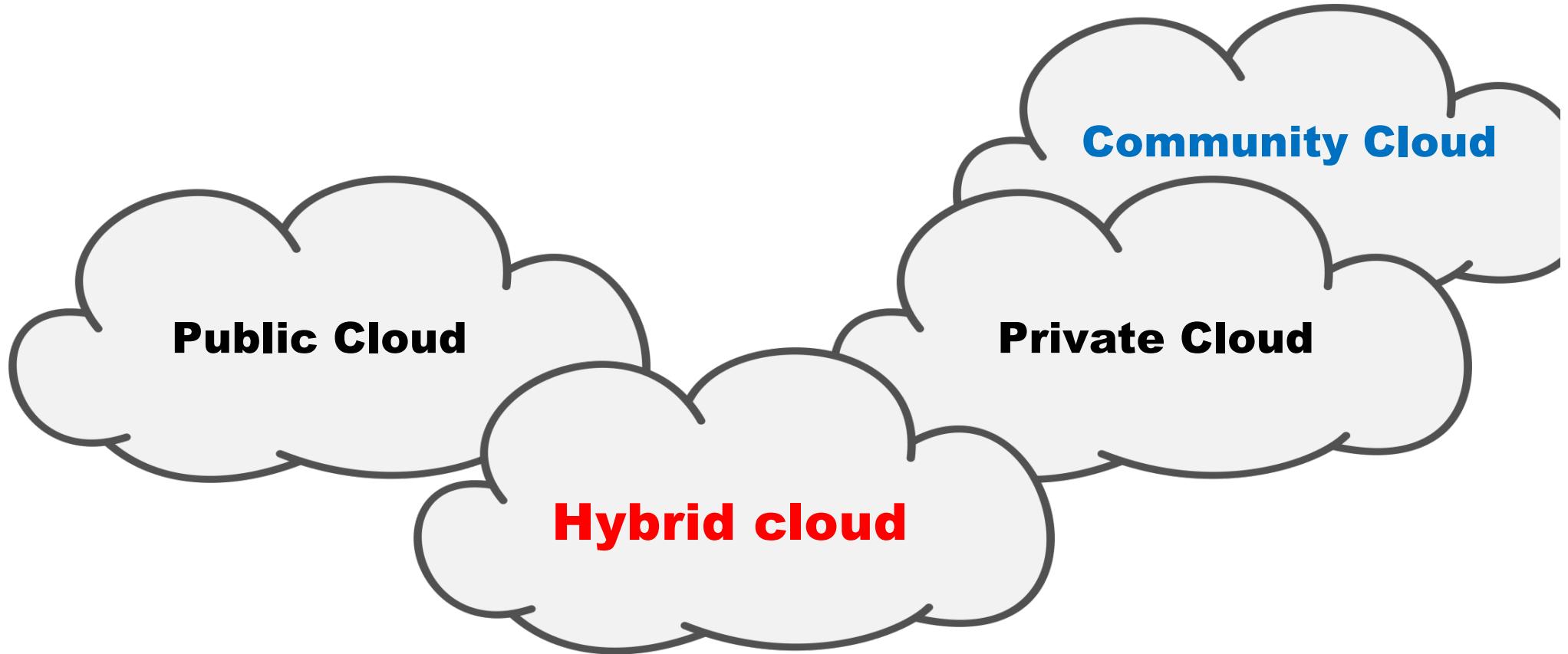
Implementation models



- Multiple clients
- Configured in a public Datacenter
- Shared infrastructure
- Access over web
- Low security
- Low cost in a “pay per use” basis
- “Do it yourself”

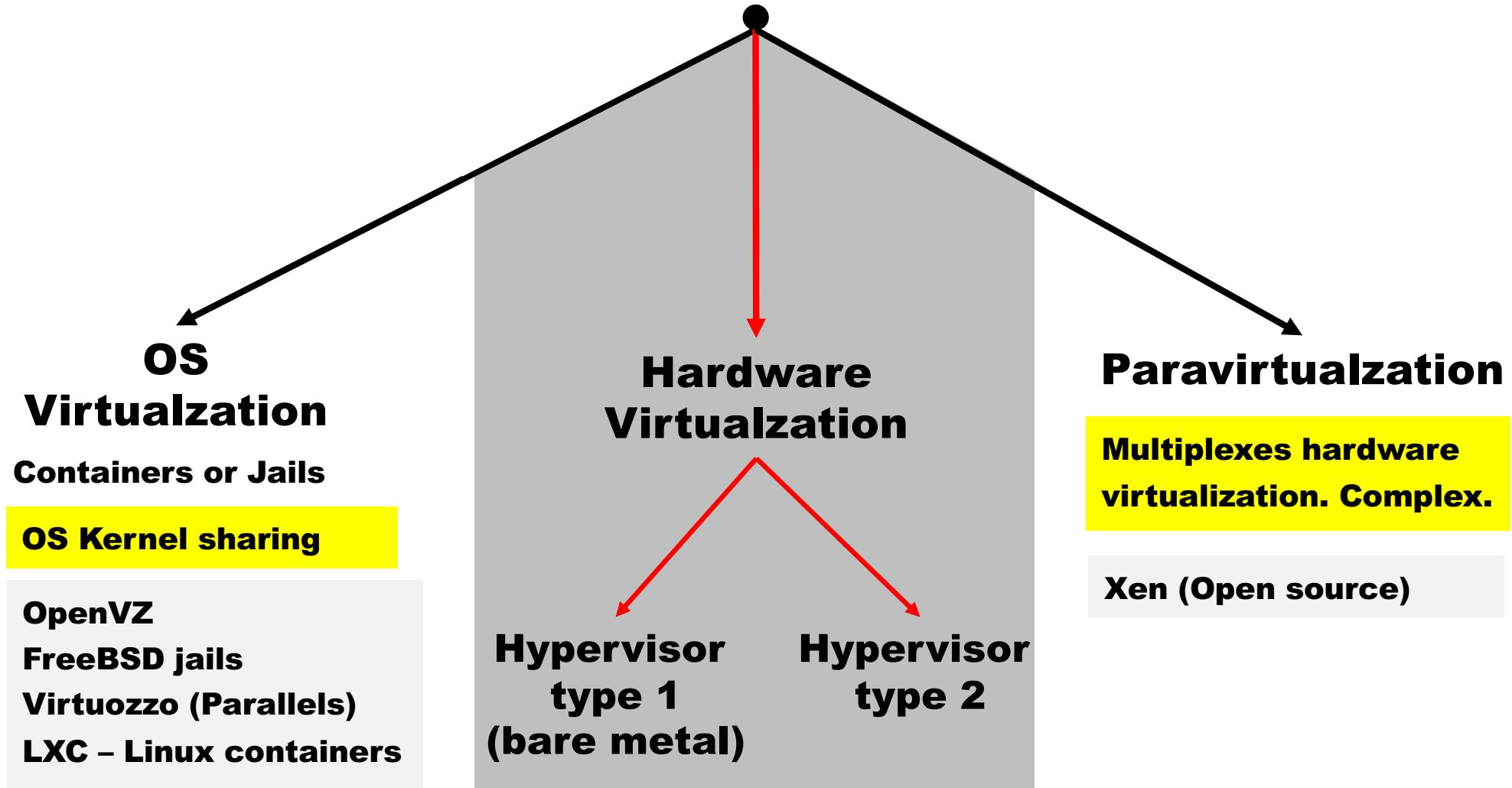
- Single-tenant solution
- Setup as a Virtual Private Datacenter
- Dedicated servers
- Access over secure private networks
- High security
- High TCO
- Custom solutions

Implementation models

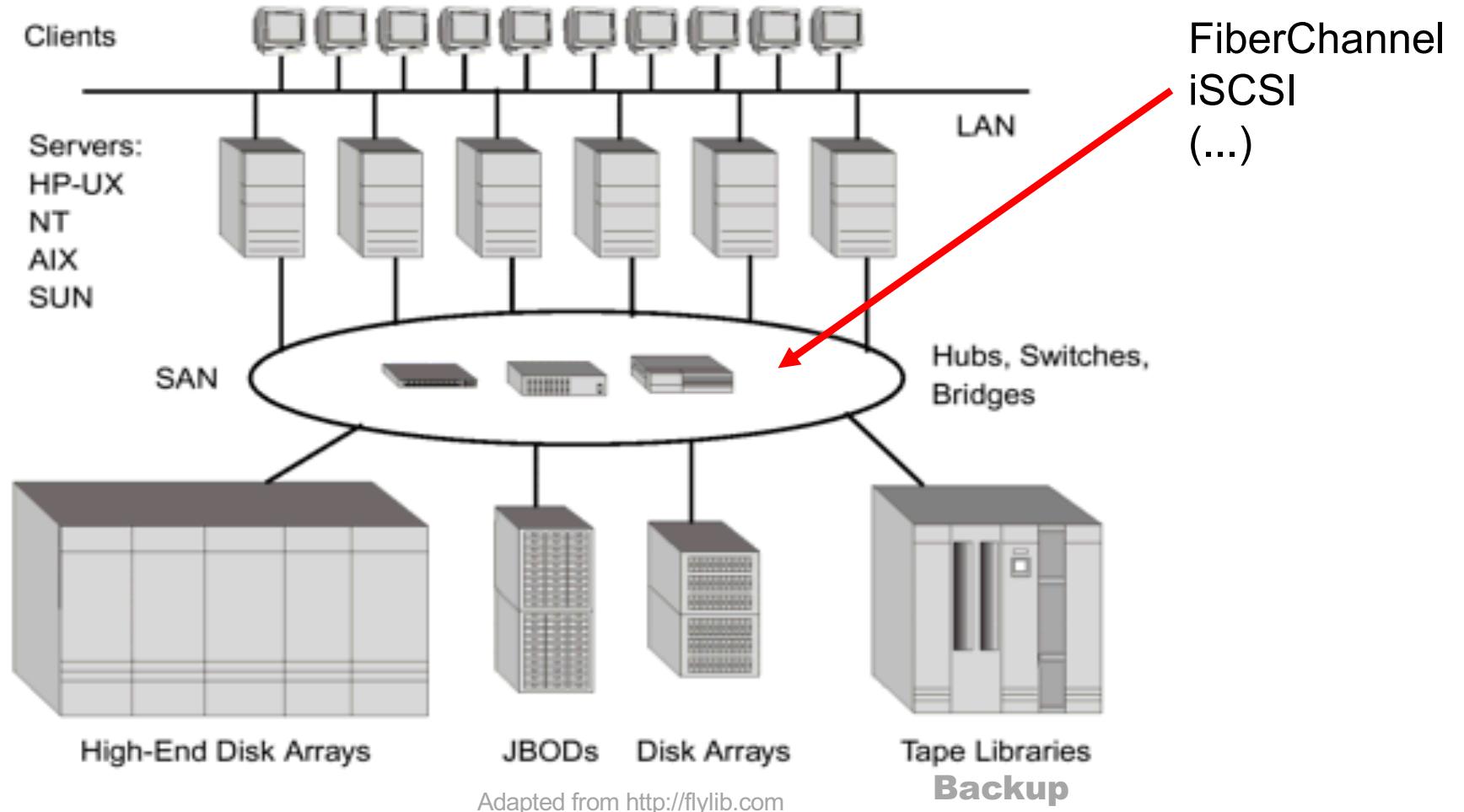


It combines features of public and private (and community) cloud models

Cloud technology - virtualization



Cloud technology – virtualization - storage



Cloud technology – virtualization - storage

- Grouping physical devices in one “logical unit”
- Grouping is irrespective to physical disks location
- Used with other local strategies: e.g. RAID
- Shared, block-based and transparent access to end-users
- Smooth storage manager and data replication
- Essential in a fault-tolerant and HA perspective
- Implementation over IP: iSCSI and iFC

Cloud technology – virtualization - Google

Americas

Berkeley County, South Carolina
Council Bluffs, Iowa
Douglas County, Georgia
Jackson County, Alabama
Lenoir, North Carolina
Mayes County, Oklahoma
Montgomery County, Tennessee
Quilicura, Chile
The Dalles, Oregon



Asia

Changhua County, Taiwan
Singapore

Europe

Dublin, Ireland
Eemshaven, Netherlands
Hamina, Finland
St Ghislain, Belgium

15 datacenters world wide

<http://www.google.com/about/datacenters/inside/locations/>
<http://www.datacentermap.com>

Cloud technology – virtualization - security

Critical component = Hypervisor

Security elements

Type 1 (hardware based)

Software that comprise the hypervisor package
(virtualization function and OS functions)

Type 2 (operating system based)

More attractive to attackers. More vulnerabilities.
OS and applications expose breaches.

Limited access and strong control over embedded OS increase robustness of Type 1 hypervisor.

Standardization is needed to effectively reduce the risk!

Service models – security considerations - IaaS

IaaS Main Threats

- 1. VM attacks
- 2. Virtual network
- 3. Hypervisor attacks
- 4. VM-based rootkits (VMBR)
- 5. Virtual switch attacks
- 6. DoS attacks
- 7. Colocation

Highly dependent on the widespread use of virtualization and the associated hypervisor components.

The Official (ISC)2® Guide to the CCSP™ CBK®, Second Edition
Adam Gordon; John Wiley & Sons, Inc, 2016 (pp.48-50)

Service models – security considerations - IaaS

New threats:

1. Provisioning tools and VM templates try to create new unauthorized VM or patch the VM templates
2. Infection propagates by new VM clones
3. These new threats are the result of a new, complex and dynamic nature of the cloud virtual infrastructure

Service models – security considerations - IaaS

Factors that determine the cloud dynamic notion:

1. Multitenancy
2. Loss of control
3. Dynamic network topology
4. Logical network segmentation
5. No physical endpoints
6. Single Point of Access/Failure (SPoA/SPoF)

Service models – security considerations - PaaS

PaaS
Main Threats

- 1. System and Resource Isolation**
- 2. User-level permissions**
- 3. User Access Management**
 - Intelligence
 - Administration
 - Authentication
 - Authorization
- 4. Protection against malware, backdoors and trojans**

The Official (ISC)2® Guide to the CCSP™ CBK®, Second Edition
Adam Gordon; John Wiley & Sons, Inc, 2016 (pp.50-52)

Service models – security considerations - SaaS

- SaaS**
- Main Threats**
- 1. Data segregation
 - 2. Data access and policies
 - 3. Web application security

Cloud Security Alliance Controls Matrix (CCM)

https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview

The Official (ISC)2® Guide to the CCSPSM CBK®, Second Edition
Adam Gordon; John Wiley & Sons, Inc, 2016 (pp.52-54)

Cloud technology – common threats



“The notorious nine” – cloud computing top threats in 2013

- 1. Data breaches**
- 2. Data loss**
- 3. Account or service traffic hijacking**
- 4. Insecure interfaces and API**
- 5. Denial of Service**
- 6. Malicious insiders**
- 7. Abuse of cloud services**
- 8. Insufficient due diligence**
- 9. Shared technologies vulnerabilities**

The Official (ISC)2[®] Guide to the CCSPSM CBK[®], Second Edition
Adam Gordon; John Wiley & Sons, Inc, 2016 (pp.43-47)

Cloud technology – security risks



OWASP Top 10 Application Security Risks – 2017
[<https://www.owasp.org>]

A1 - Injection

A2 – Broken Authentication and session management

A3 – Cross-Site Scripting (XSS)

A4 – Insecure Direct Object References

A5 – Security Misconfiguration

A6 - Sensitive Data Exposure

A7 – Missing Function Level Access Control

A8 – Cross-Site Request Forgery (CSRF)

A9 – Using Components with known vulnerabilities

A10 – Unvalidated Redirects and Forwards

The Official (ISC)2® Guide to the CCSP™ CBK®, Second Edition
Adam Gordon; John Wiley & Sons, Inc, 2016 (pp.54-55)

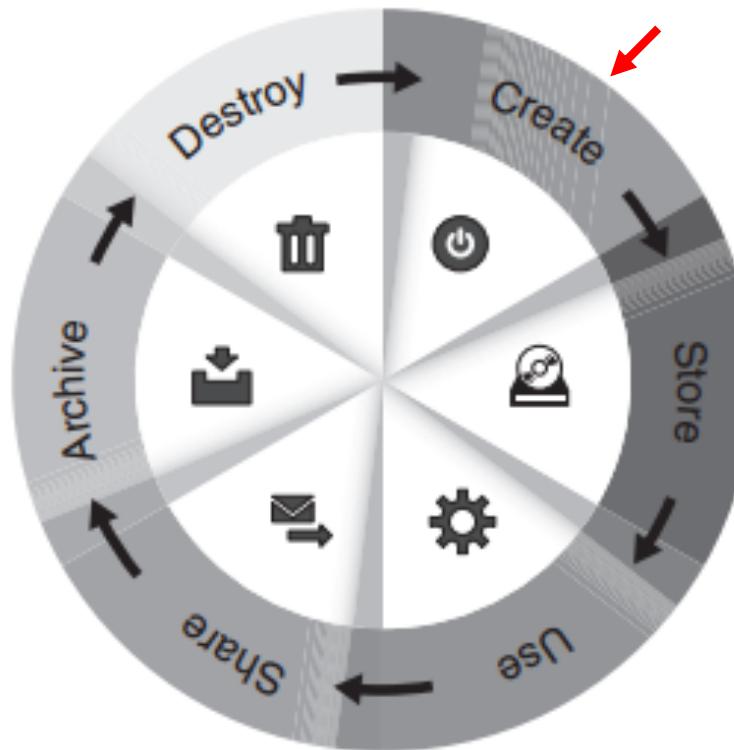
Cloud security – data and media sanitization

- Ability to safely remove all data from a system or media.
- Needed if you want to leave or migrate one CSP to another.

- Challenges:
 - Vendor lock-in
 - Cryptographic erasure
 - Data overwriting

Cloud secure data lifecycle

- Data is the single most valuable asset for most organizations.
- Auditing, compliance and other control requirements implies a good understanding of data lifecycle.



Be aware of logical and
Physical location of data.

The Official (ISC)2® Guide to the CCSP™ CBK®, Second Edition
Adam Gordon; John Wiley & Sons, Inc, 2016 (pp.55-56)

Cloud cross-cutting aspects

Cloud architecture - key principles

- Define protections that enable trust in the cloud.
- Develop cross-platform capabilities and patterns for proprietary and open source providers.
- Facilitate trusted and efficient access, administration, and resiliency to the customer or consumer.
- Provide direction to secure information that is protected by regulations.
- Facilitate proper and efficient identification, authentication, authorization, administration, and auditability.
- Centralize security policy, maintenance operation, and oversight functions.
- Make access to information both secure and easy to obtain.
- Delegate or federate access control where appropriate.
- Ensure ease of adoption and consumption, supporting the design of security patterns.
- ■ Make the architecture elastic, flexible, and resilient, supporting multitenant, multilandlord platforms.
- Ensure the architecture addresses and supports multiple levels of protection, including network, OS, and application security needs.

The Official (ISC)2® Guide to the CCSP™ CBK®, Second Edition
Adam Gordon; John Wiley & Sons, Inc, 2016 (pp.27)

Cloud cross-cutting aspects

NIST Cloud Technology roadmap

- 1. Interoperability**
- 2. Portability**
- 3. Availability**
- 4. Security**
- 5. Privacy**
- 6. Resiliency**
- 7. Performance**
- 8. Governance**
- 9. SLAs**
- 10. Auditability**
- 11. Regulatory compliance**

- Industry-recommended
- Guidance and recommendations
- Target: security architects, enterprise architects, and risk-management professionals
- Useful to review and understand which controls and techniques may be required

The Official (ISC)2® Guide to the CCSP™ CBK®, Second Edition
Adam Gordon; John Wiley & Sons, Inc, 2016 (pp.28-32)

It is worth being on the cloud?

- OPerational EXpenses *versus* CAPital EXpenses
- How big (€£\$) is the TCO (OPEX + CAPEX)?
- How much (€£\$) for the specialized human resources?
- How much (€£\$) for the defined SLA?
- And what about to buy and to subscribe software?
- “*Pay only if you use and use only if you need*”
- Do you need support for entrepreneurship and innovation?

Cost-benefits analysis

1. Resource pooling
2. Shift from CAPEX to OPEX
3. Factor in time and efficiencies
4. Have in mind depreciation of IT technologies
5. Reduction in maintenance and configuration time
6. Shift in focus regarding professionals' functions
7. Utilities cost (power, cooling, datacenter space, ...)
8. Software and licensing costs
9. Pay per usage
10. Others – new tech, revised roles, legal costs, SLA revision, ...

It is worth being on the cloud?

Initial costs (CAPEX)

- hardware acquisition and instalation
- OS and software acquisition
- Building infrastrucutres
- (...)

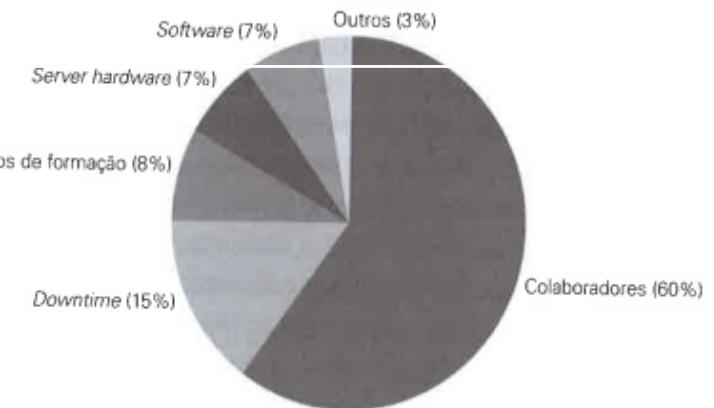
Operational costs (OPEX)

- Power consumption
- HAVC (rent)
- UPS (rent)
- Human resources
- (...)

TCO = Total Cost of Ownership

The value of the project through its lifetime.

$$\text{TCO} = \text{CAPEX} + \text{OPEX}$$



António Miguel Ferreira; "Introdução ao Cloud Computing"; FCA;
ISBN: 978-972-722-802-7; 2015
IDC Withepaper sobre TCO.

Cloud technology – the future

- Ubiquity *de facto*
- Faster, wider , safer, bigger
- Interoperability – standards please!
- Fog Computing (*fogging*)
- Internet of Things (IoT)
- Bring Your Own Device (BYOD)
- Big Data

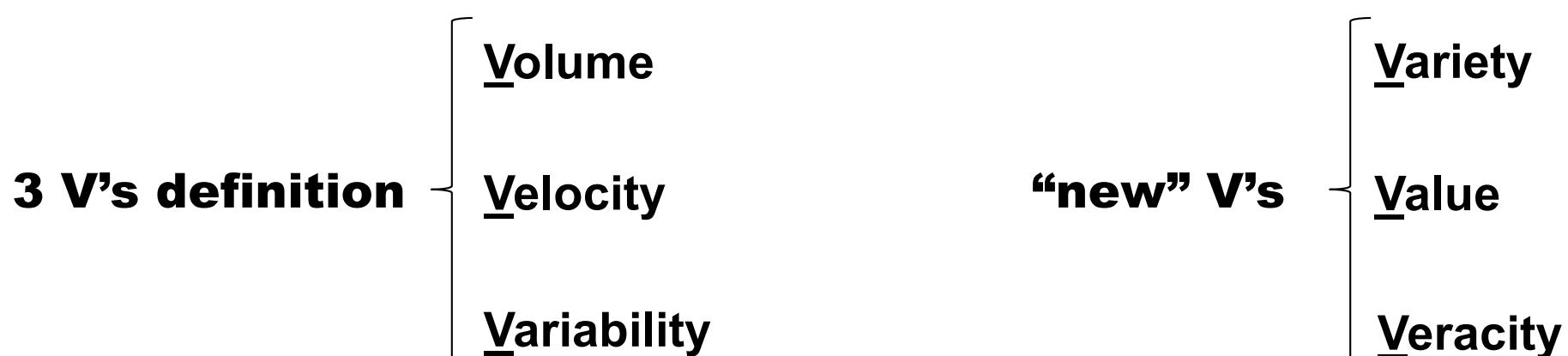
Big data - overview

According to NIST¹:

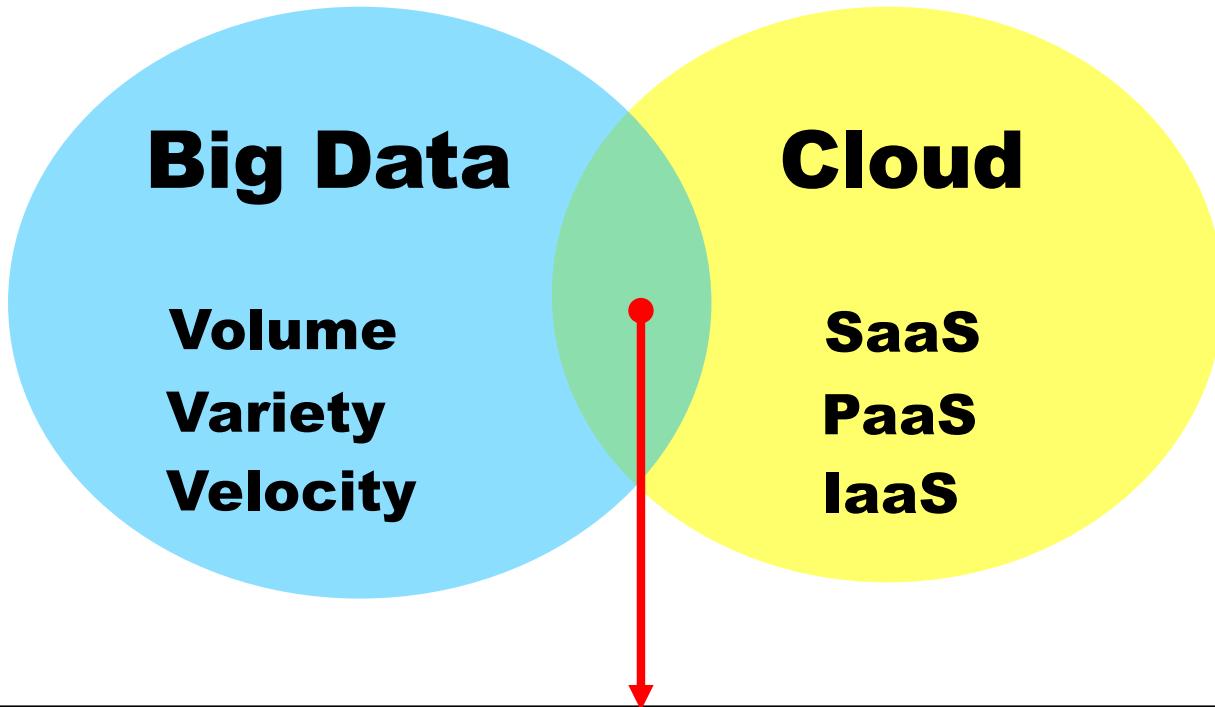


Big Data consists of extensive datasets – primarily in the characteristics of volume, variety, velocity, and/or variability (and/or value) – that require a scalable architecture for efficient storage, manipulation, and analysis.

¹ The NIST Definition of Cloud Computing; <http://csrc.nist.gov/>.



Big data - overview



	Volume	Variety	Velocity
SaaS	Client-side Personalization	Types of visualization	Real-time
PaaS	Distributed processing	Schemaless databases	Integration on the fly
IaaS	Scalable storage	Federated databases	On-demand resources

Certification

Security standards applied to cloud environment:

- ISO/IEC 27001:2013
- ISO/IEC 27002:2013
- ISO/IEC 27017:2015
- SOC 1/SOC 2/SOC 3 → Audit Reports
- NIST SP 800-53
- PCI DSS

Cardholder data management for merchants.

Standards for Risk Management

1. Information Security Policies
2. Organization of Information Security
3. Human Resources Security
4. Asset Management
5. Access Control
6. Cryptographic
7. Physical and Environmental Security
8. Operations Security
9. Communications Security
10. System Acquisition, Development, and Maintenance
11. Supplier Relationship
12. Information Security Incident Management
13. Information Security Business Continuity Management
14. Compliance

The Official (ISC)2® Guide to the CCSPSM CBK®, Second Edition
Adam Gordon; John Wiley & Sons, Inc, 2016 (pp.62-72)

Bibliography

- Cloud Industry Forum



- IEEE Cloud Computing



- ISO/IEC 27017 cloud security



17788, 17789 e 27017

- Asia Cloud Computing Association



- EuroCloud Europe



EuroCloud Portugal
[www.eurocloud.pt]

Bibliography

- “The NIST Definition of Cloud Computing”; Peter Mell, Timothy Grance; <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>.
- “NIST Cloud Computing Standards Roadmap”; http://www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf; 2013.
- “*Introdução ao cloud computing*”; A.M. Ferreira; FCA; (pp. 11-78; pp. 89-106)
- “The Official ISC²® Guide to the CCSPSM CBK[®], Second Edition”; Adam Gordon; John Wiley & Sons, Inc; 2016 (Chapter 1; pp.3-77)
- “Certified Cloud Security Professional (CCSP), Official Study Guide”; B. O’Hara, B. Malisow; John Wiley & Sons, Inc; 2017 (Chapter 1)
- “CCSP Official ISC²® Practice tests”; B. Malisow; Sybex; 2018; (Chapter 1; pp.1-30)

Backups

- Backups – noções gerais
- Soluções integradas

Motivação

“Existem dois tipos de administradores de sistemas: os que já perderam pelo menos um disco, e os que hão de vir a perder...”

-- W. Curtis Preston, *UNIX Backup & Recovery*



Motivação

- A solução de cópias de segurança deve inserir-se no **plano de sobrevivência a catástrofes** da organização.
- A incapacidade de recuperar um sistema quando necessário é **causa frequente de despedimento** de administradores de sistemas!



"You should check your e-mails more often. I fired you over three weeks ago."

Motivação

1. **WHY ?** → Impacto para o negócio. Estimativa de perdas.
2. **WHAT ?** → Volume de dados que devem ser guardados.
3. **WHEN ?** → De dia? À noite? Qual a periodicidade.
4. **WHERE ?** → Para disco? Para Tape?
5. **WHO ?** → Responsabilidades de execução e análise.
6. **HOW ?** → Comandos e procedimentos

Motivação

- Quando é que é necessário recuperar os dados?
 - Perda accidental de dados (p.e. `rm -Rf *`)
 - Falhas de discos
 - Medida MTBF dos discos
 - Erros humanos, por engano ou propositadamente
 - Questões legais (p.e. prova em tribunal)
 - Dados corrompidos por engano, propositadamente ou outros

Os backups têm de ser **fiáveis**

Plano de contingência (1)

- 1) Quanto tempo pode demorar a recuperar de...
 - uma falha total do sistema?
 - uma falha parcial do sistema?
- 2) Enquanto o sistema está activo será possível...
 - fazer recuperações?
 - fazer cópias de segurança?
- 3) Quais as falhas que provocarão mais perdas?

Plano de contingência (2)

- 4) Quem perde mais por erro humano ou falha hw?
- 5) Quais as prioridades na recuperação?
- 6) Quantas cópias de segurança são necessárias?
- 7) Quanto tempo será necessário manter as cópias?
- 8) Qual o orçamento disponível?

Plano de contingência (3)

Cinco passos que devem constar do plano de contingência:

1) Definir “*Perdas Aceitáveis e Inaceitáveis*”

- Informação que pode ou não ser perdida
- Tempo de recuperação

2) Salvaguardar todos os dados

- Além dos dados, armazenar meta-dados e instruções de recuperação dos dados

3) Organizar e documentar todas as ações

Plano de contingência (4)

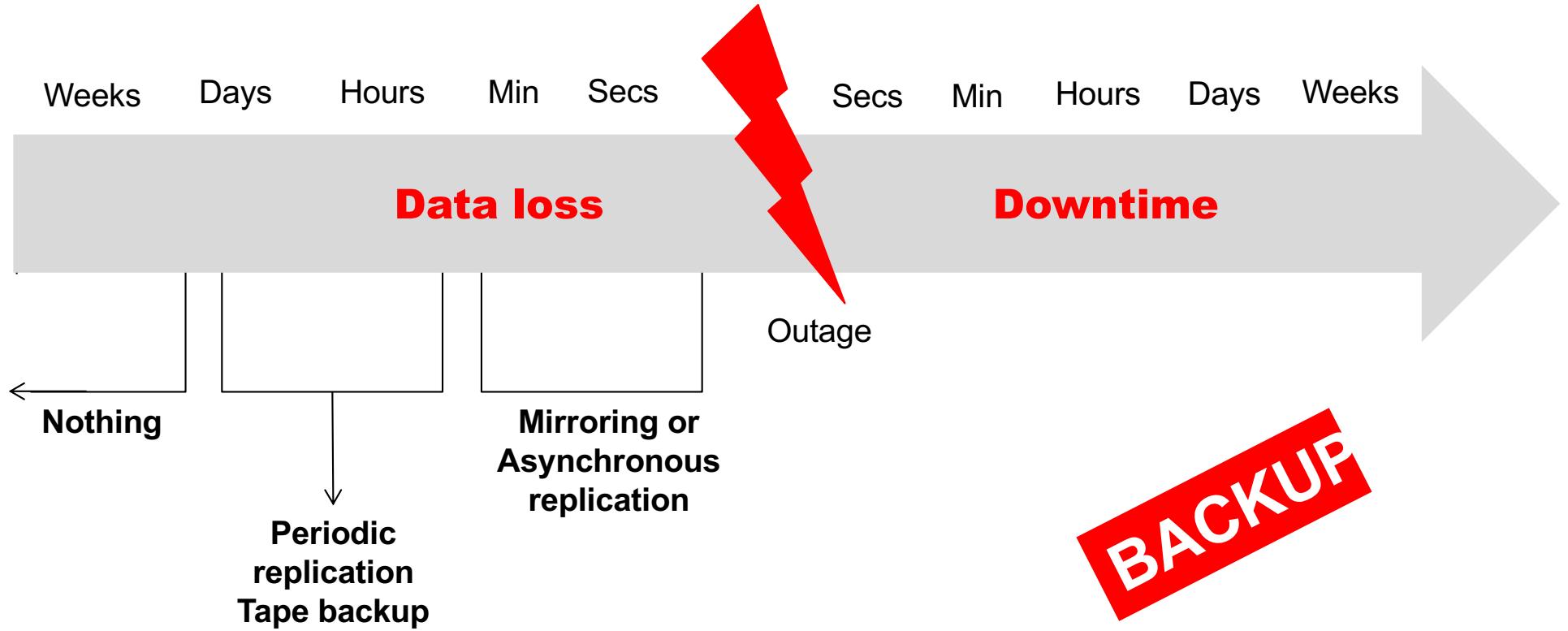
4) Protecção contra todo tipo de desastres

- Os desastres naturais não são os únicos
 - Ex.: ataque ao WTC
 - Protecção anti-fogo e ... anti-água!
 - Roubos...
- O suporte das cópias de segurança também pode falhar!
- Pode haver uma combinação de várias causas!

5) Testar, testar e ... testar!

- Plano de contingência não testado? É apenas uma “proposta”.
- Para prevenir surpresas, testar, testar e testar ainda mais!

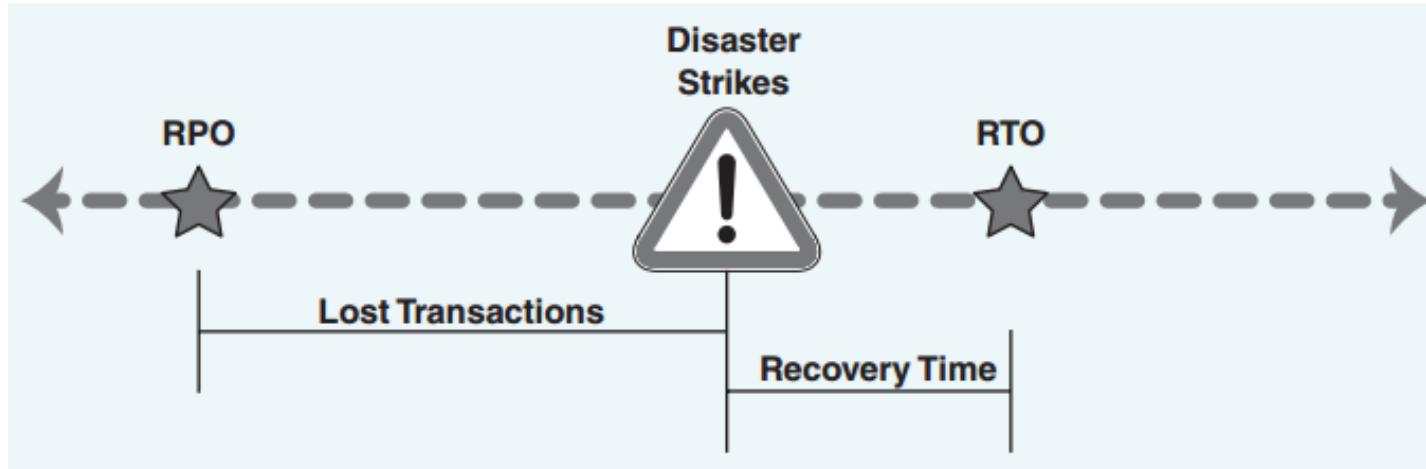
Estratégias de mitigação - dados



Objetivo: minimizar perda de dados e garantir a consistência

Estratégias de mitigação - dados

- Quantos dados está a empresa disposta a perder?
- Ao fim de quanto tempo terá o sistema de estar disponível após o desastre?



RPO = Recovery Point Objective

RTO = Recovery Time Objective

Políticas de backup e SLA

Definir convenientemente:

- Qual a necessidade de fazer backups
- Em que consistem as operações de backup
- Que dados devem ser salvaguardados
- Quais os requisitos legais
- A que horas deverão ser realizados
- Período de tempo usado para a recuperação de dados
- Período de tempo de retenção dos dados
- Método de escalonamento das operações de backup
- Planeamento de capacidade e utilização das tapes

Exemplo de um SLA

“Customers should be able to get back any file with a granularity of one business day for the last six months and with a granularity of one month for the last three years.

Disk failures should be restored in four hours, with no more than two business days of lost data.

Archives should be full backups on separate tapes generated quarterly and kept forever.

Critical data will be stored on a system that retains user accessible snapshots made every hour.”

Tipos de backup

1) Completo

- Cópia completa e integral de todos os ficheiros existentes no disco
- Para restaurar a informação apenas é necessário restaurar a cópia completa
- O tempo de salvaguarda é longo
- Reposição do backup é simples. Implica apenas uma cópia.

Tipos de backup

2) Incremental

- Copia apenas ficheiros modificados/criados desde a última salvaguarda (incremental ou completa)
- Para restaurar → necessário restaurar primeiro a ÚLTIMA cópia completa e TODAS as salvaguardas incrementais
- Salvaguarda é rápida: apenas as modificações são gravadas
- Recuperação dos dados pode ser longa
 - Último backup completo + backups incrementais

Tipos de backup

3) Diferencial (ou integral cumulativo)

- Copia todos os ficheiros modificados/criados desde a última **salvaguarda completa**
- Para restaurar → repôr a última cópia completa e depois a salvaguarda diferencial
- Salvaguarda pode não ser rápida
- A restauração dos dados pode ser medianamente longa
 - Último backup completo + último backup diferencial

Níveis de salvaguarda

Níveis - Definição de níveis 0 até 9

Nível 0

- Backup integral

Nível 1

- Backup diferencial

Nível i ($i=2$ até 9)

- Backup incremental em relação ao último backup nível $i-1$
- *Backup nível 3* → backup incremental em relação ao último nível 2

Table 5-1: Backup Level

Backup Level	Description	Linux Troubleshooting Bible Christopher Negus and Thomas Weeks
Level 0	A full backup; backs up all files.	
Level 1	The first incremental level; gets all files that have changed since the last level 0 backup. It acts like a differential by getting everything that has changed since the level 0/full backup.	
Levels 2-9	Backs up whatever files have changed since the next <i>lower</i> level backup. Can work as an incremental if used sequentially, or as a differential if all the same number is used. Can also be "mixed" to create hybrid backup strategies.	

Níveis de salvaguarda

Exemplos:

Dom.	2 ^a	3 ^a	4 ^a	5 ^a	6 ^a	Sab.
Full/0	Full/0	Full/0	Full/0	Full/0	Full/0	Full/0
Full/0	Diff/1	Diff/1	Diff/1	Diff/1	Diff/1	Diff/1
Full/0	Incr/1	Incr/2	Incr/3	Incr/4	Incr/5	Incr/6

Quando? Geralmente, durante a noite

Porquê?

- **Integridade:** Pouca atividade e maior estabilidade do sistema (ficheiros)
- **Velocidade:** Sistema e rede mais libertos para operações de backup.

Proteção contra falha de suporte

1) Possuir dois conjuntos de suporte



2) Ciclo rotativo A + B

- Dois conjuntos completos: A e B
- A é empregue nos dias pares, B nos ímpares
- Cada arquivo incremental tem os ficheiros dos dois últimos dias
- Há redundância no arquivo (ficheiros duplicados nos dois conjuntos) excepto para o último dia

Características do suporte de backup

- 1) Custo:** precisamos de muito mais espaço de cópias de segurança do que espaço ocupado pelos dados
- 2) Fiabilidade:** de nada serve uma cópia de segurança se o meio de suporte falhar
- 3) Velocidade:** suficientemente rápido para permitir concluir a cópia durante o tempo disponível para o efeito
- 4) Disponibilidade:** não é possível fazer cópias de segurança para CD-R sem um gravador de CDs!
- 5) Usabilidade:** quanto mais fácil de fazer melhor

Que servidores proteger?

- 1) Cópias de segurança devem ficar num servidor diferente daquele que se pretende proteger
- 2) Fazer cópias de segurança de todas as máquinas numa mesma LAN ou hub para um servidor local
- 3) Fazer cópias de segurança de todos os servidores locais de um edifício para um servidor noutro edifício.

ONSITE versus OFFSITE !!!!

Que suporte utilizar?

- **Disquete:** uma cópia integral de /etc ** OBSOLETO**
 - **Drive ZIP:** ~200 MB ** OBSOLETO**
 - **CD-R:** 600 MB ** OBSOLETO**
 - **DVD:** 4.7 GB (ou 9 GB se for double-sided)
 - HD-DVD 17 GB p/camada), Blu-Ray (25 GB p/camada)
 - **Banda magnética:** 40GB até vários TB (LTO-4/120MB/s)
 - **Discos rígidos:** 500 GB a muitos TB...
 - **Bibliotecas robotizadas:** muitos TB
- } amovíveis

Tapes

Drive de tape - *Sun StorageTek T10000C*

- Capacidade até 5 TB
- 252 MB/segundos



Unidades robotizadas (*libraries*)

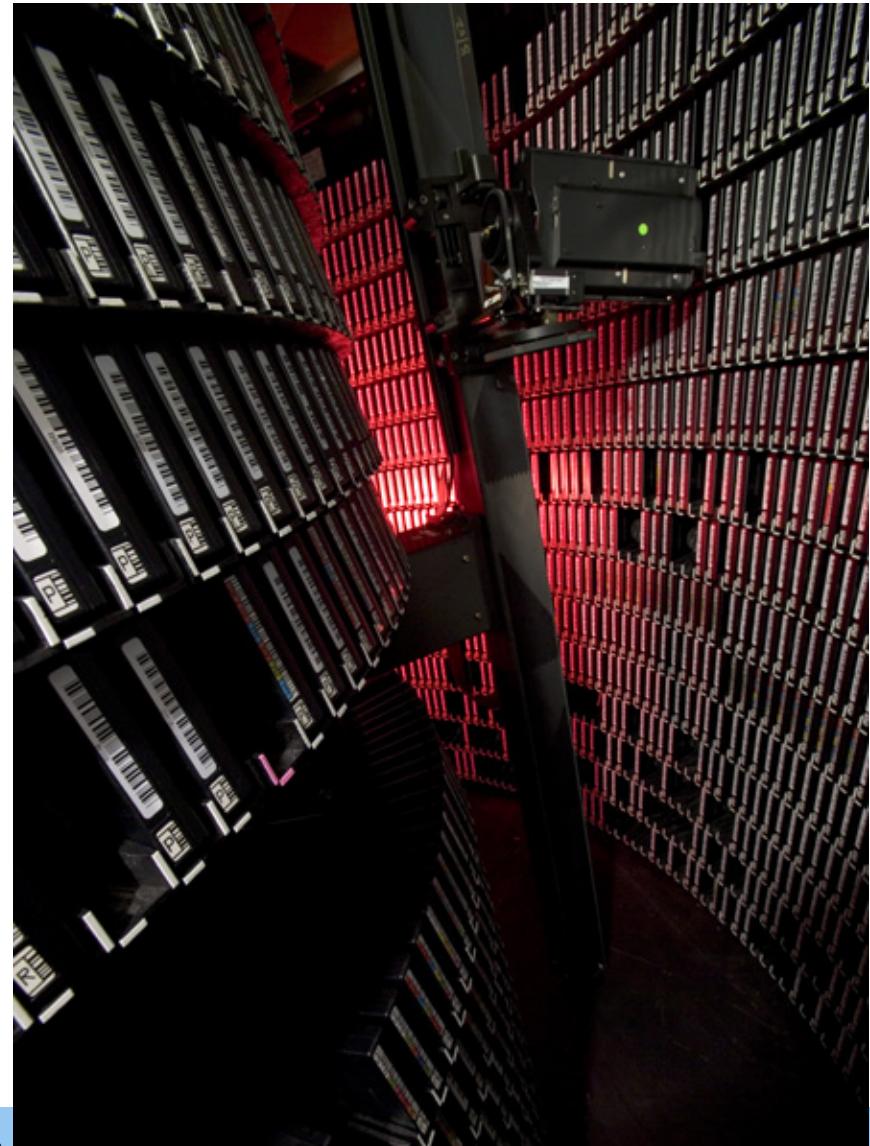
(+) Grande capacidade de armazenamento

Facilmente atingem vários terabytes

(-) Acesso muito lento

Robô tem que ir buscar a tape
A tape tem que ser lida

(-) Caros!



Unidades robotizadas (*libraries*)

Sun StorageTek SL8500 Modular Library system

- até 100.000 slots
- até 1.000 PB (2:1)
- modular
- 64 drives $T10000C = 55.3 \text{ TB/hora}$



Soluções integradas opensource



Soluções integradas

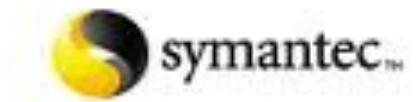
Open source

Linux e/ou Windows

Escaláveis

**Integração com unidades
robotizadas de backup**

Soluções integradas comerciais



<http://www.backupcentral.com/>

Leituras...

- “*Backup and Recovery*”; *Curtis, 2006*

Datacenters – conceitos fundamentais

1. História
2. Requisitos gerais
3. Desafios emergentes
4. Normalização
5. Norma TIA-942
6. Layout geral de um datacenter
7. Organização em racks
8. Eficiência energética
9. Segurança

História



www.ibm.com

História



www.ibm.com



História



www.ibm.com

História



www.ibm.com

História – 60’ e 70’

- Grandes salas de computadores.
- Operacionalidade do equipamento difícil.
- Infraestruturas físicas (arrefecimento, racks, chão falso,...)
- Existência de um “mainframe” para o cálculo mais exigente.
- Consumo elevado de energia, mas sem preocupações ambientais.
- Segurança: elevada, devido ao custo avultado dos computadores.
- Principal uso: fins militares.

História – 80’ e 90’

- Popularização dos computadores e das “salas” adequadas
- Datacenters privados.
- Noção de “batch”, “server” e “time sharing”
- Desenho hierárquico assente em normas
- O “alarme” do bug do ano 2000!
- Principal uso: instituições bancárias e seguros. Empresas (multi)nacionais de média/grande dimensão.

História – 2000'

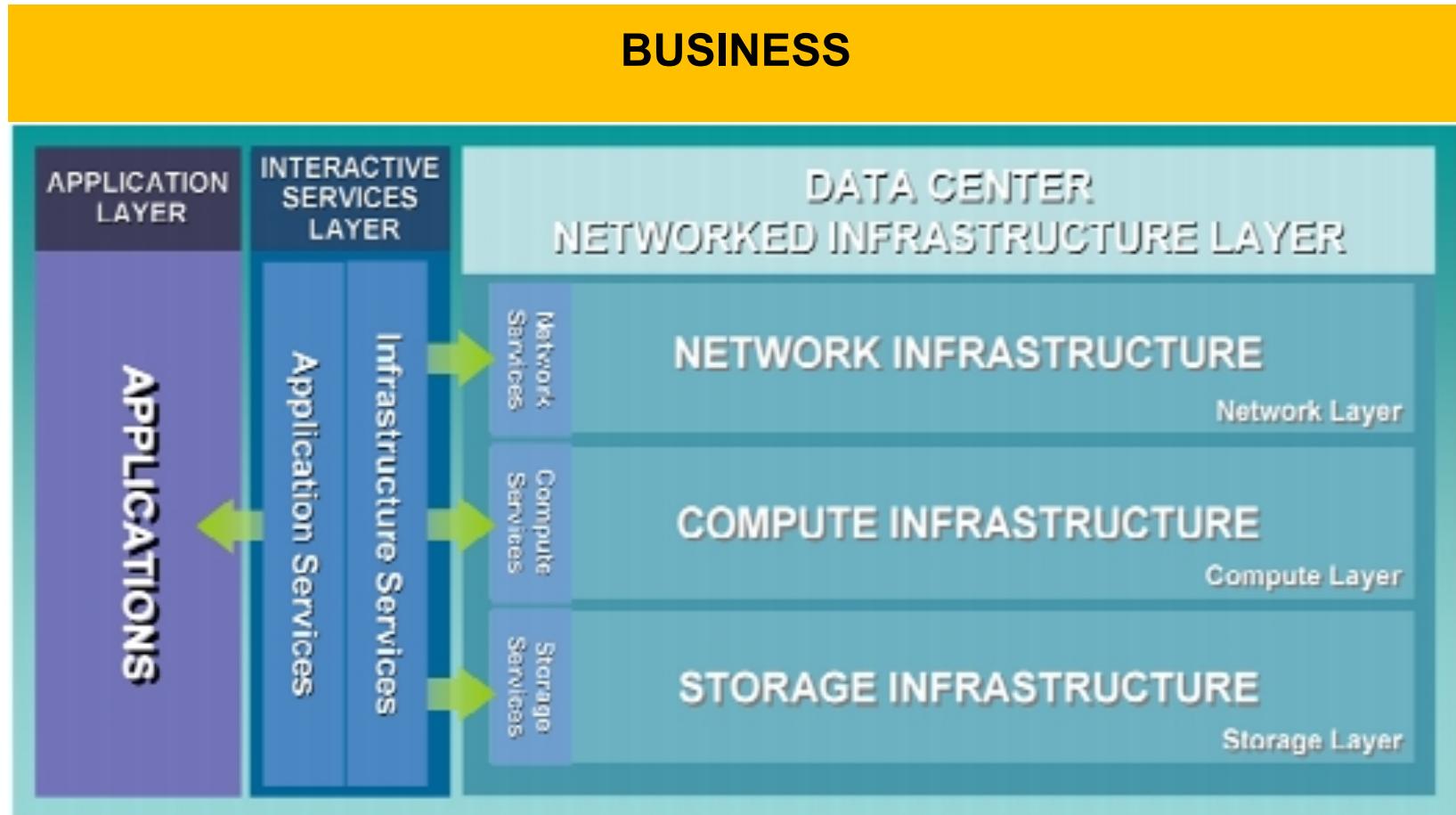
- O *boom* do “dot com” popularizou (ainda mais) os datacenters
- Alta disponibilidade, tolerância a falhas e afins.
- Negócios assentes em serviços informáticos e em datacenters
- Mais recentemente: “cloud” e a distribuição efetiva de datacenters
- Preocupações ambientais crescentes

Enquadramento

“Datacenter as a computer”

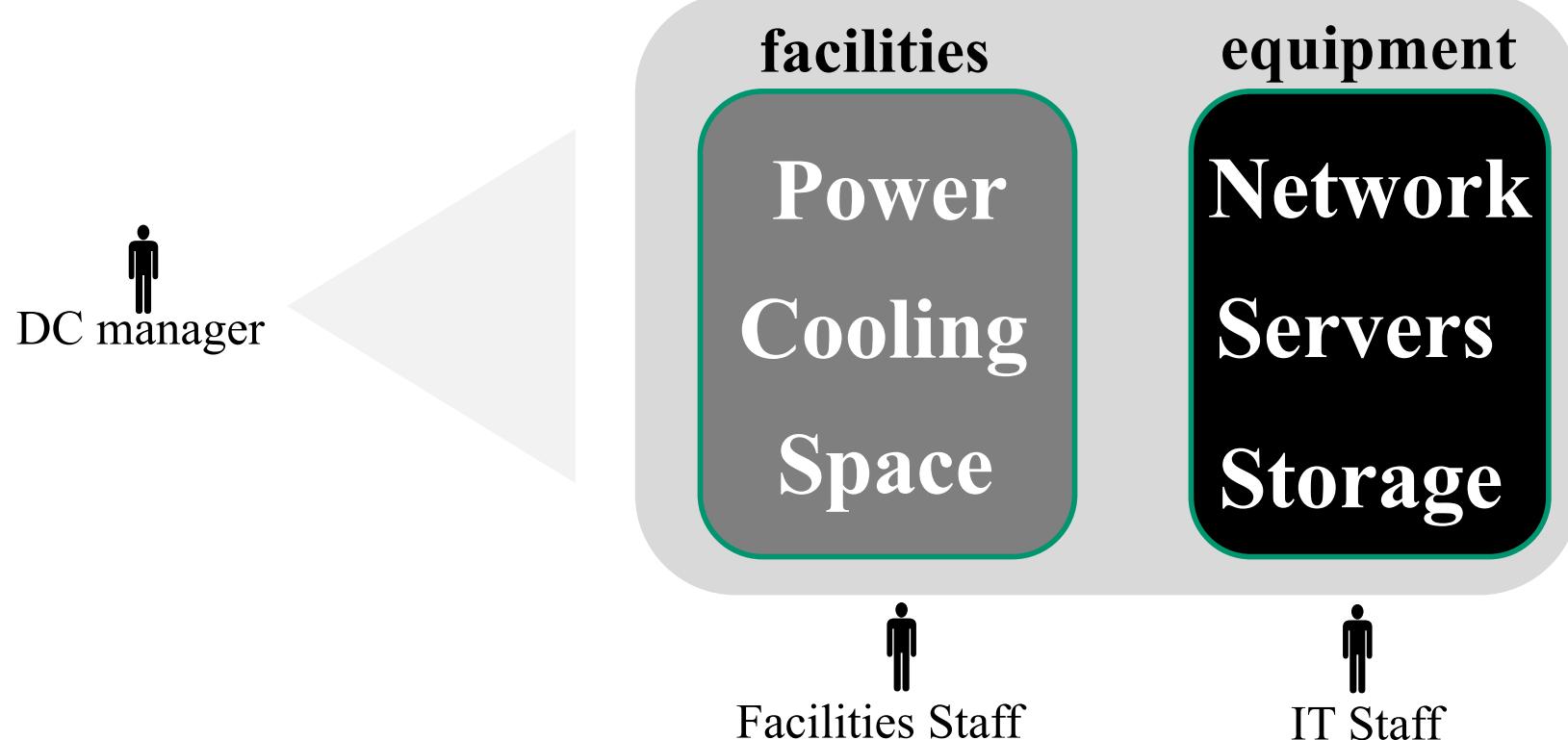


Enquadramento

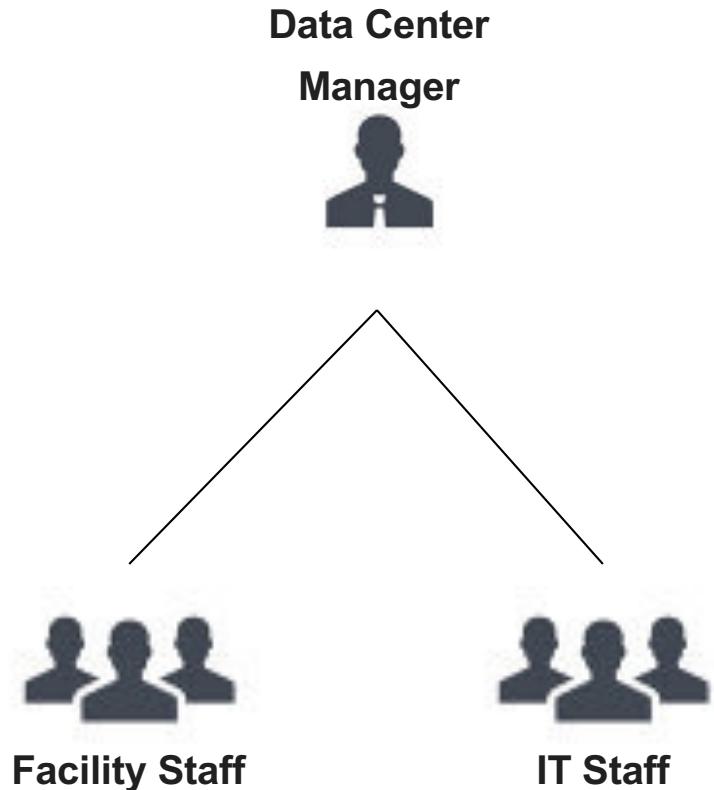


Enquadramento

Componentes essenciais de um datacenter moderno



Enquadramento



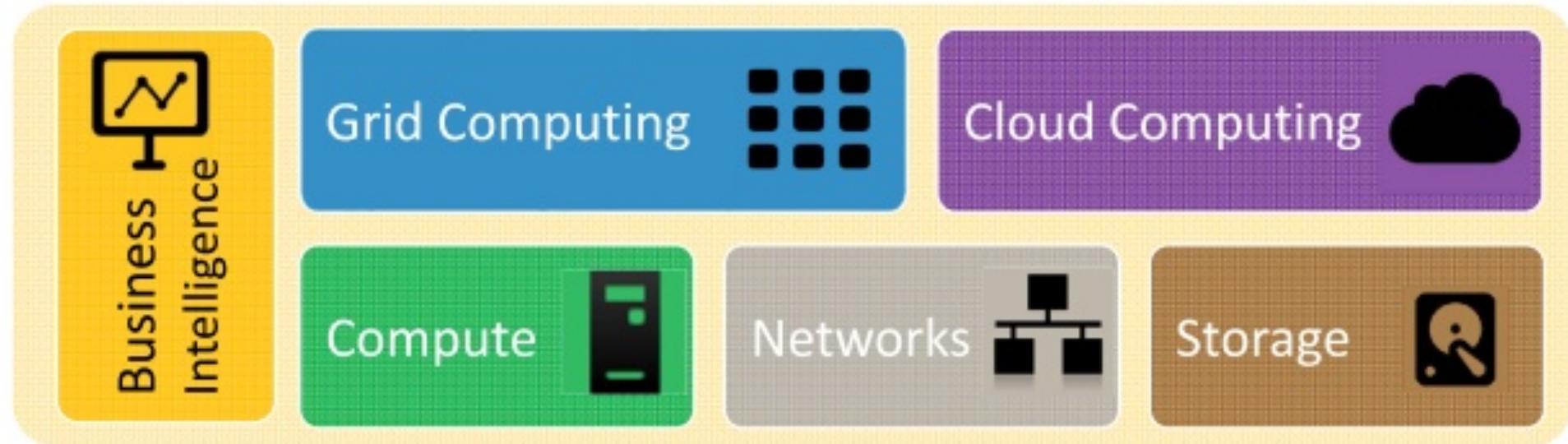
DC Manager: Responsável por todas as operações inerentes ao funcionamento do DC.

DC Facility Staff: Responsável pelas operações referentes às “facilities”, como sejam AVAC, energia e edifício.

DC IT Staff: Responsável pelas operações de TI no DC, como a gestão de sistemas operativos, storage e backups, entre outras,

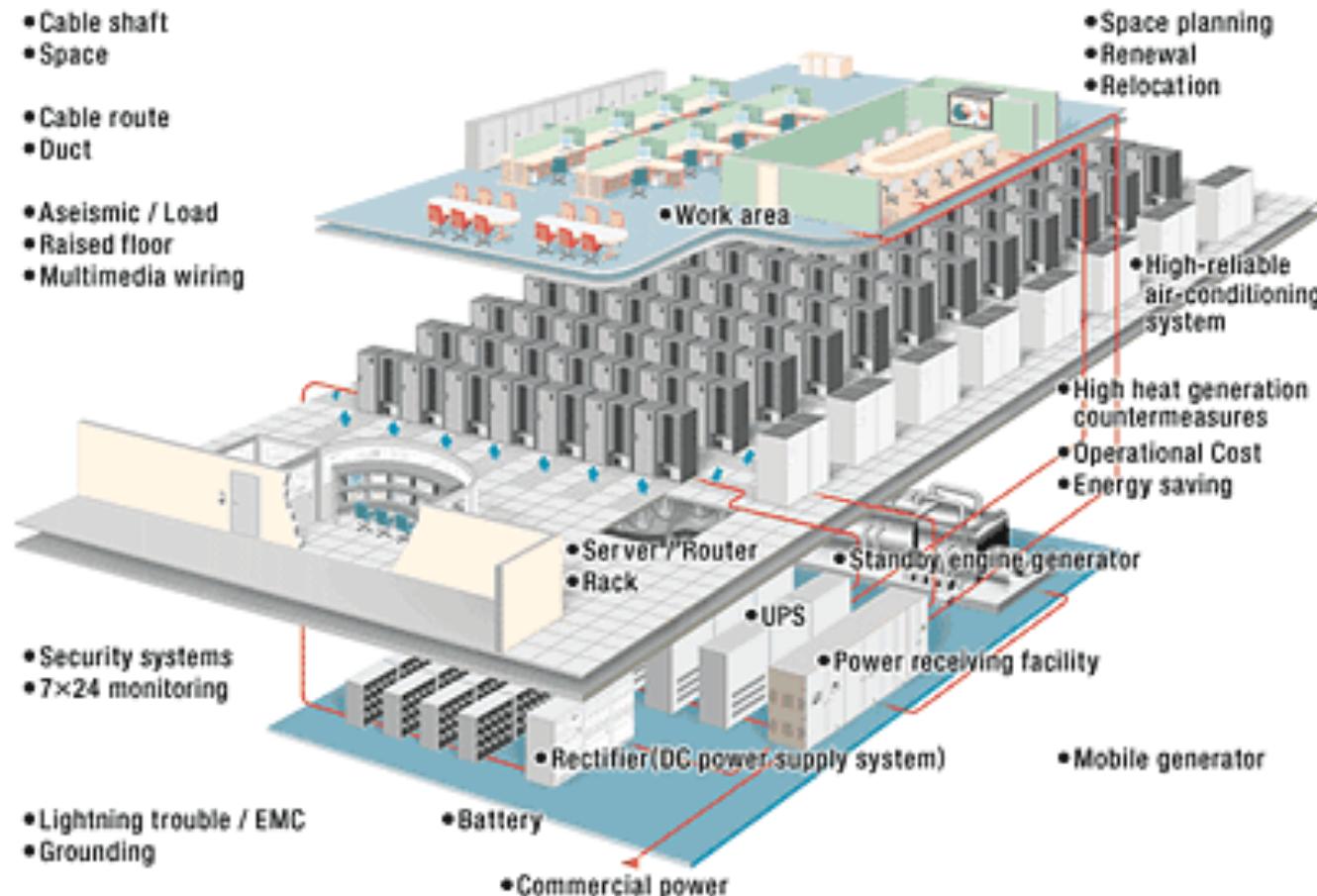
Enquadramento

Áreas principais na gestão de datacenters – desafios



Challenges in Modern Data Centers Management; <http://webcourse.cs.technion.ac.il/>

Visão global



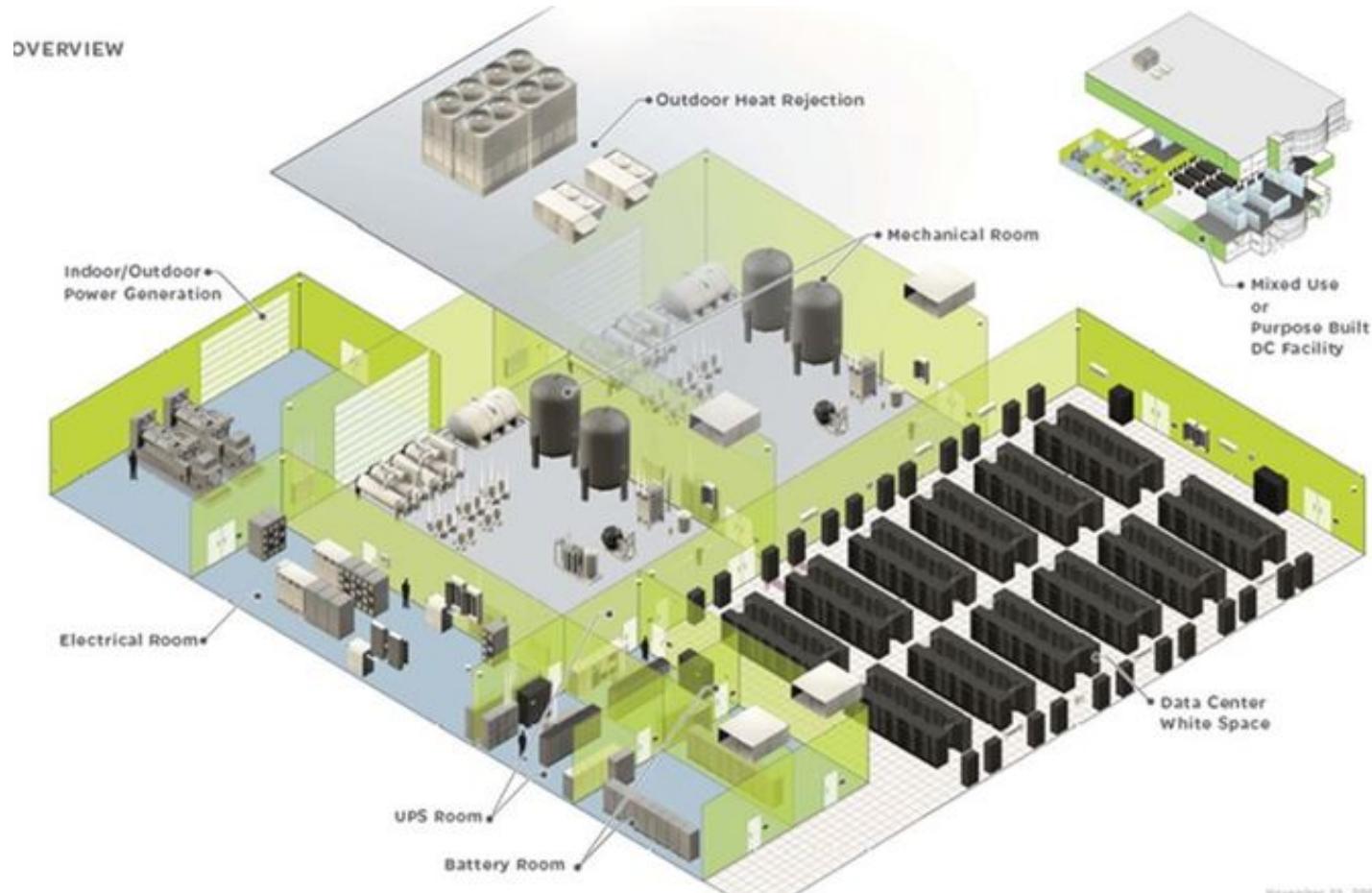
Operations room

Equipment room

Facilities

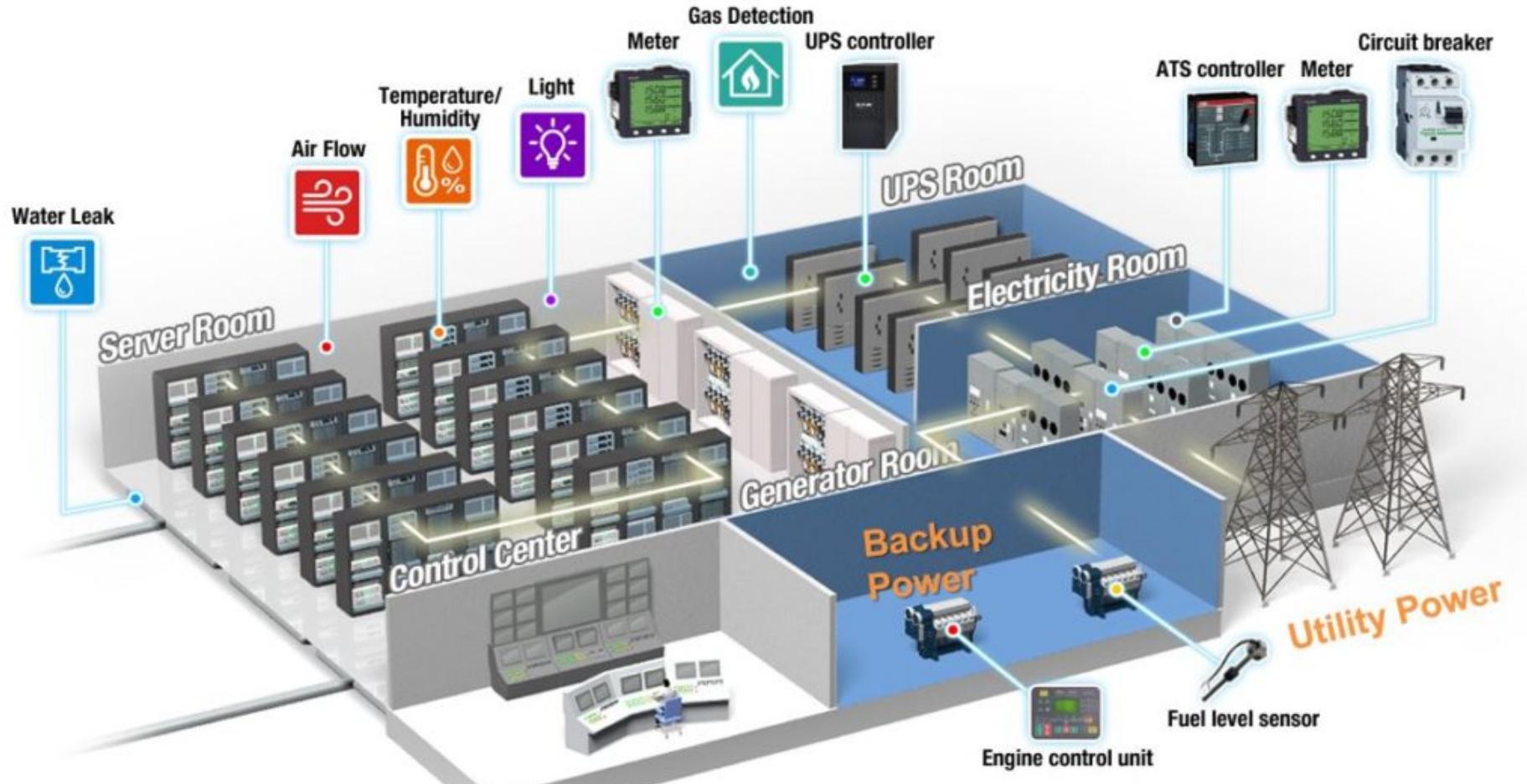
<http://www.ntt-f.co.jp>

Visão global



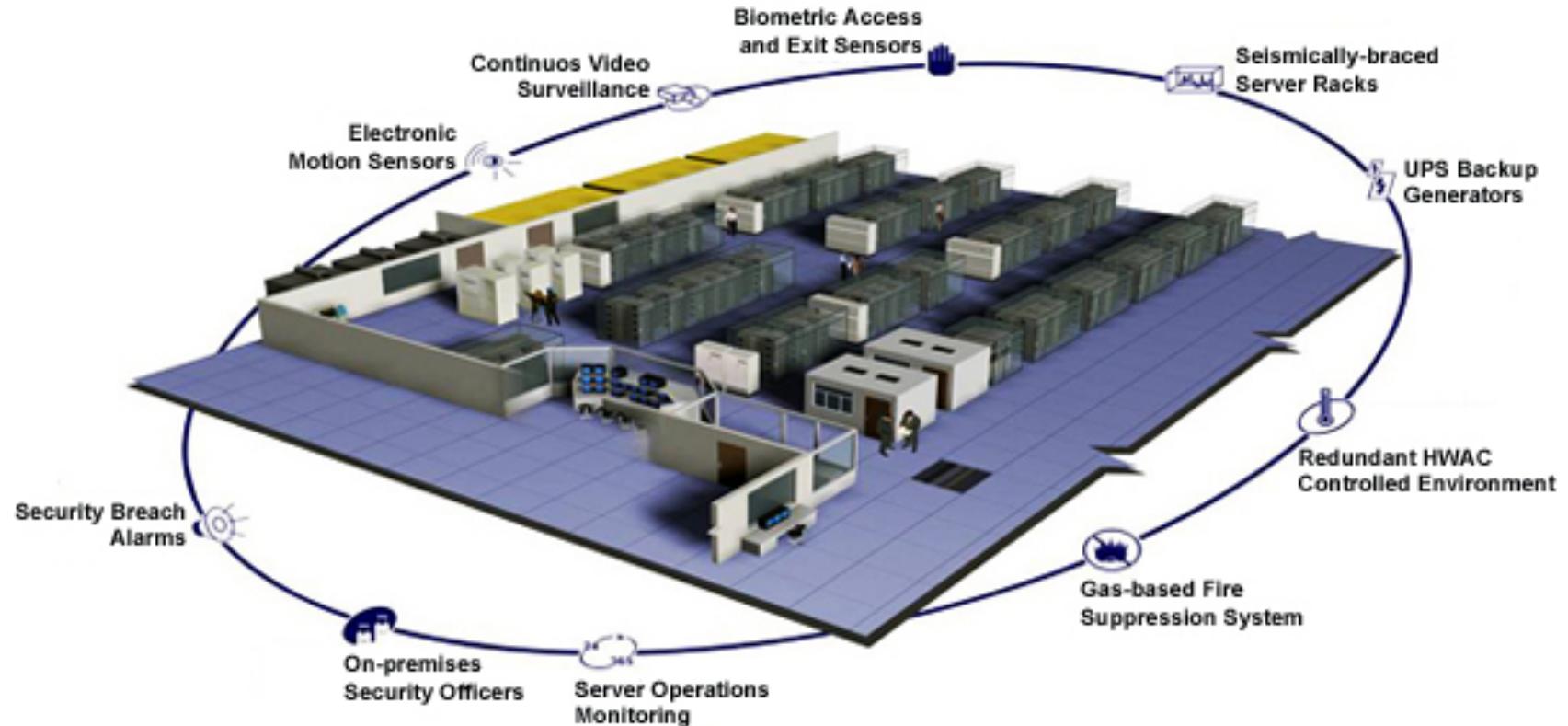
<https://www.neteon.net>

Visão global



<https://www.neteon.net>

Visão global



<http://www.ntt-f.co.jp>

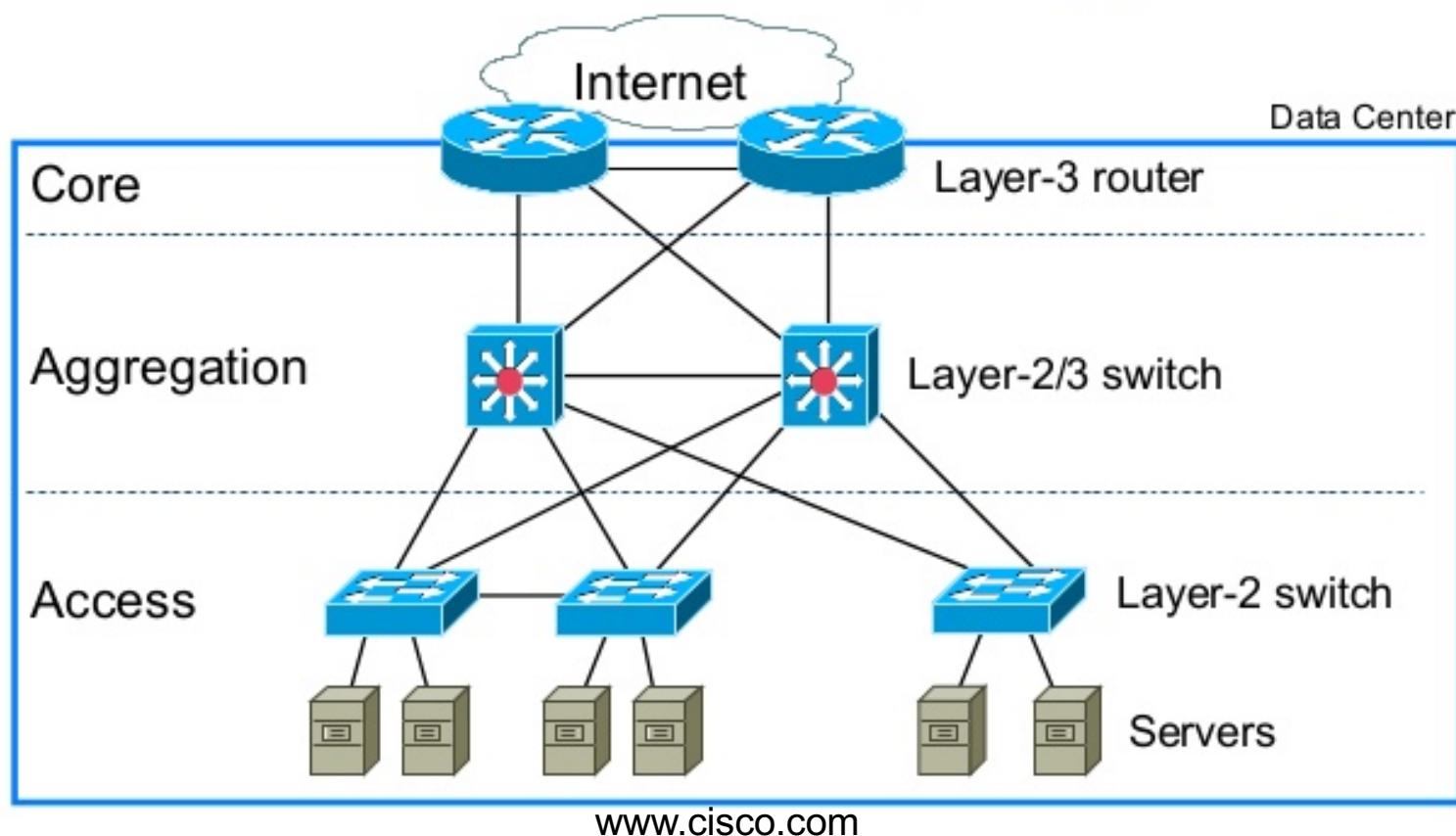
Deteção de incêndio
Deteção de intrusões

Vigilância
Operação
Monitorização

24x7

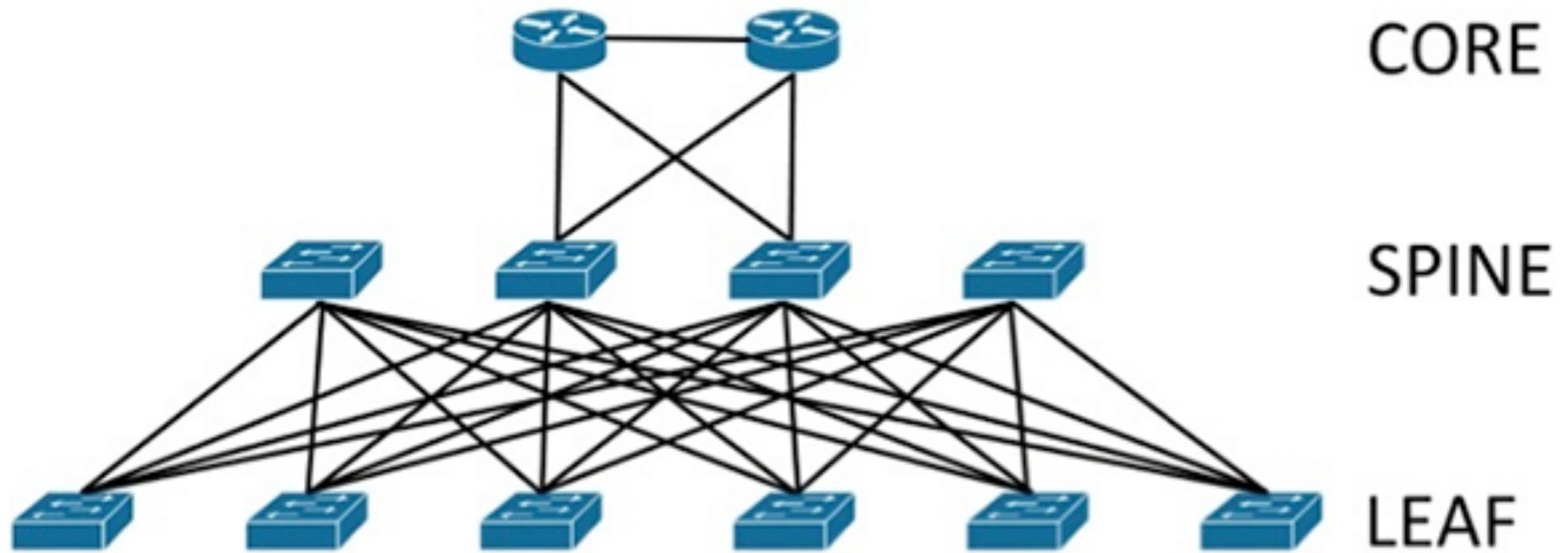
Topologia de rede

Topologia clássica: Three-Tier



Topologia de rede

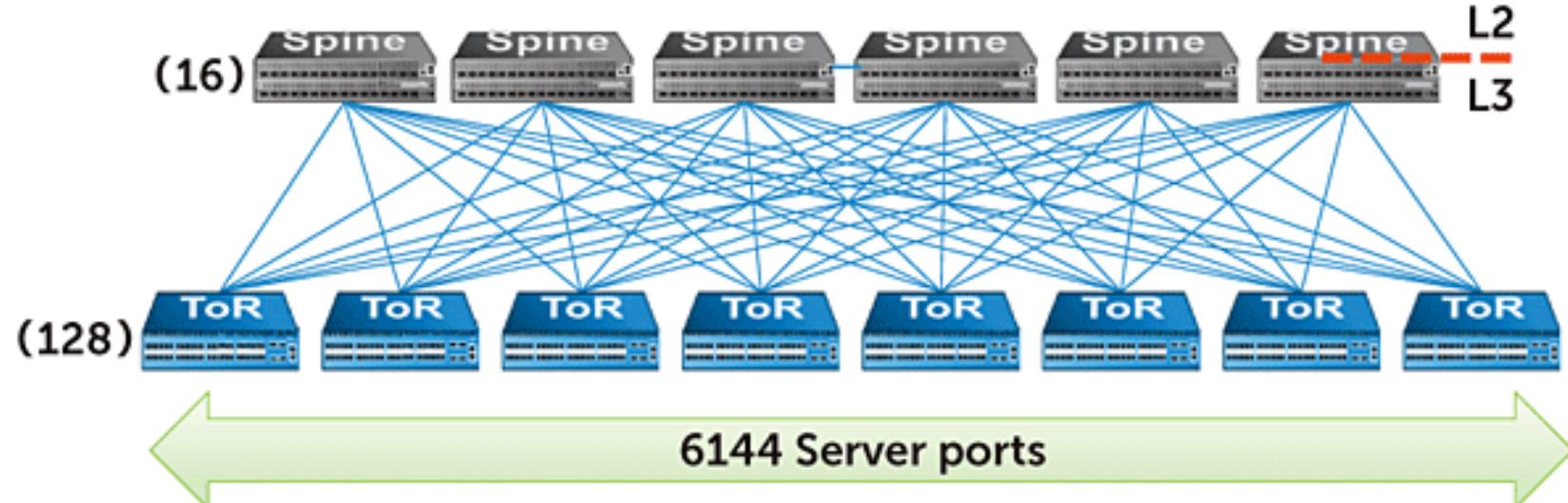
Topologia “spine-leaf” (fat-tree / Clos topology)



Topologia de rede

- Access Layer = Leaf switches
- Full-mesh → access (leaf) + aggregation (spine)
- Implementação pode ser L2 ou L3:
- Encaminhamento por todas as portas (STP desativado)
- Escalabilidade considerável pelo efeito “fabric” (L2/L3)

Topologia de rede

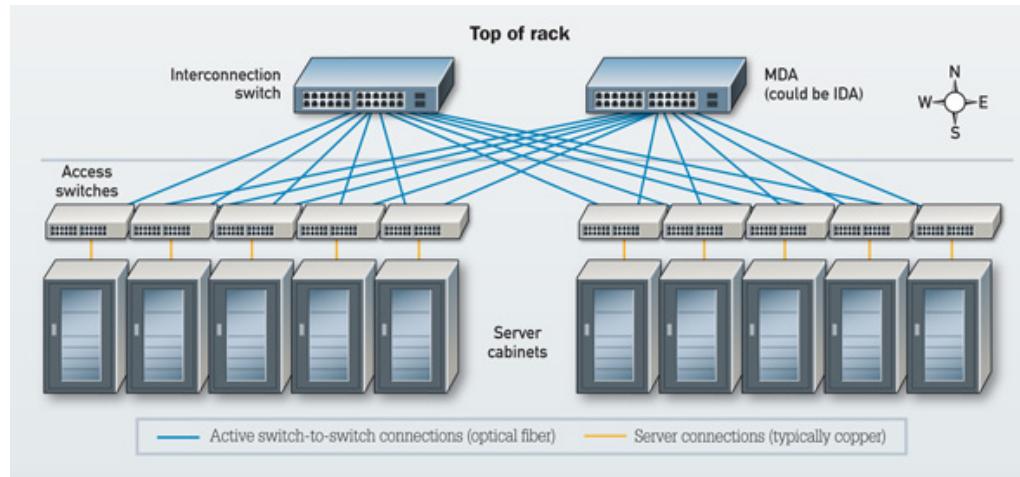


Top-of-Rack (ToR) agrega acesso dos servidores (leaf)

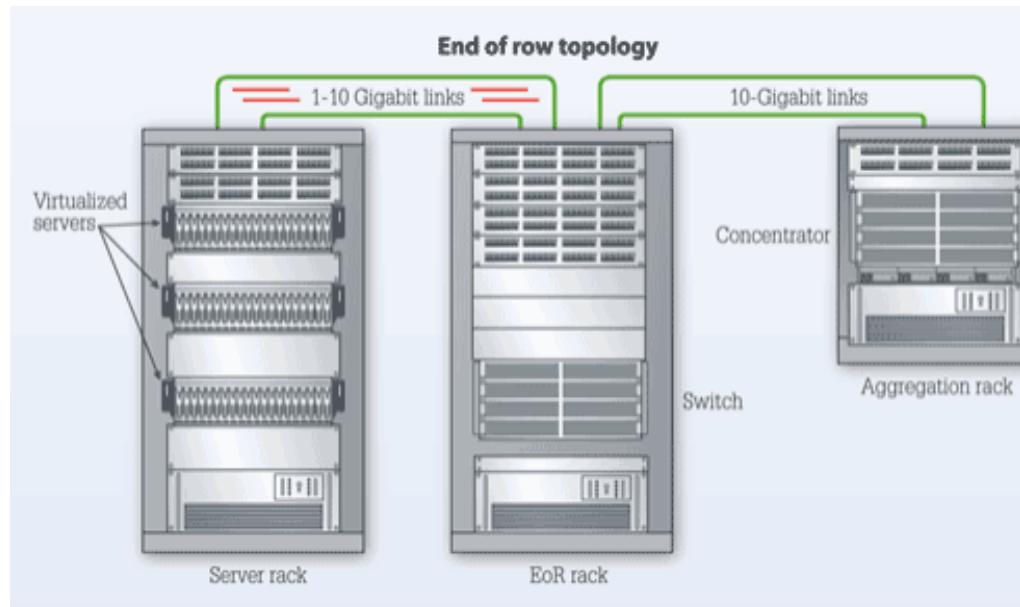
Estratégia alternativa a “End of Row”

Gestão centralizada e encaminhamento virtualizado (SDN)

Topologia de rede



Top of Rack (ToR)



End of Row

Topologia de rede

Multi-tier leaf-spine

Dcell

Hypercube

FiConn

Toroidal (ring-based)

Bcube

Jellyfish

CamCube

Scafida

Butterfly

Topologias implementadas em cenários específicos

Topologia de rede

Um site



www.google.com

World wide



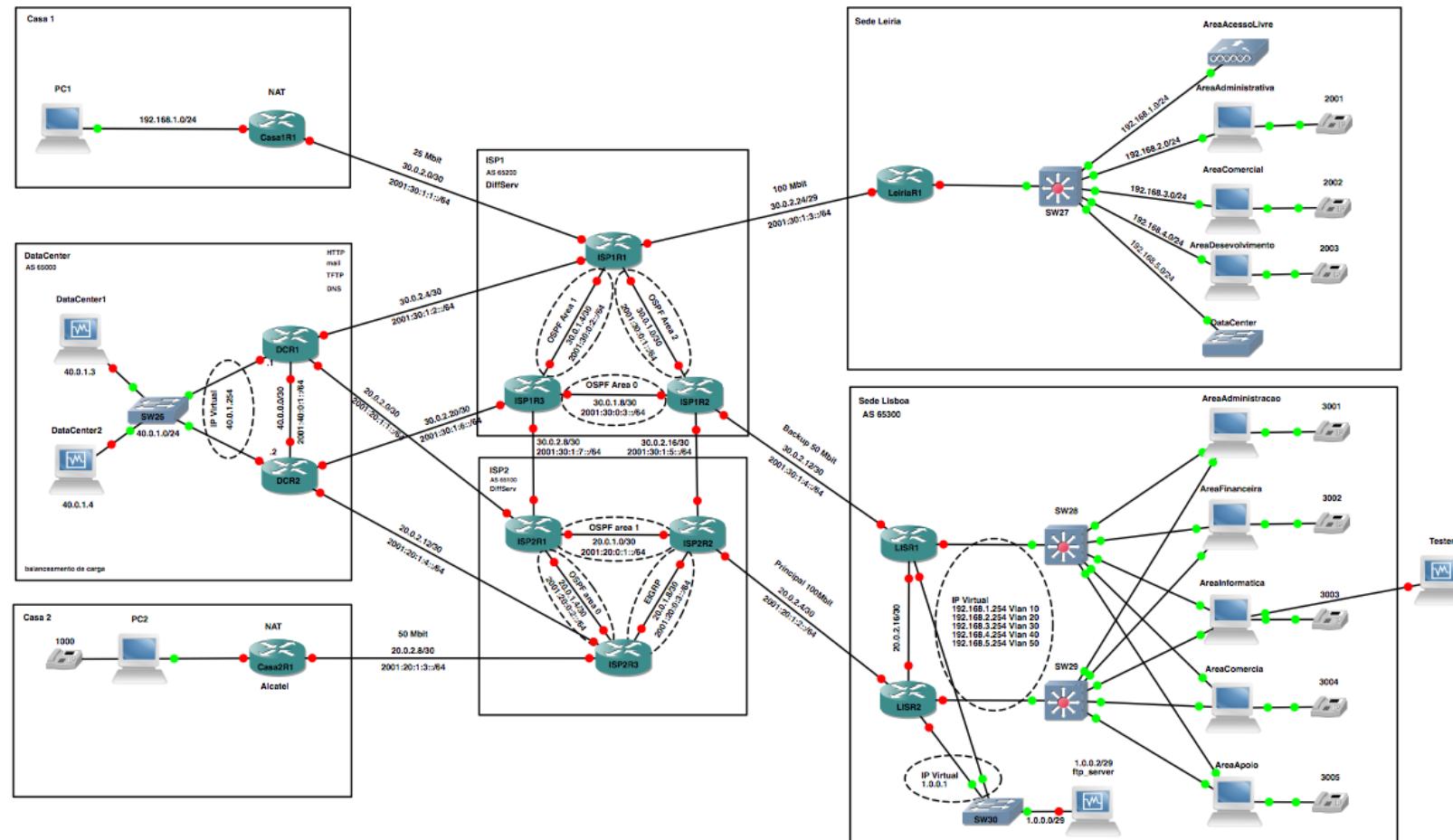
www.google.com



www.claranet.pt

Topologia de rede

Exemplo: Cenário prático no GNS3 com múltiplos sites



Rui Rodrigues, Hernani Gama; Trabalho prático das UCs de TAR e SvM; Ed.14/15

Topologia de rede

Alojamento físico num “condomínio”

- Cada inquilino (*tenant*) gere o seu espaço físico e facilities
- Algumas facilities são partilhadas
- CAPEX reduzido
- Preço do aluguer:
 - por m² utilizado
 - serviços disponíveis (portaria, energia, ...)
- Exemplo: itconic (<http://www.itconic.com>)

Topologia de rede

Alojamento em infraestrutura própria:

- Companhia é dona do espaço e faz a sua gestão
- Maior segurança e controlo de toda a infraestrutura
- CAPEX muito elevado
- Exemplo: grandes companhias (banca, seguros, ...)

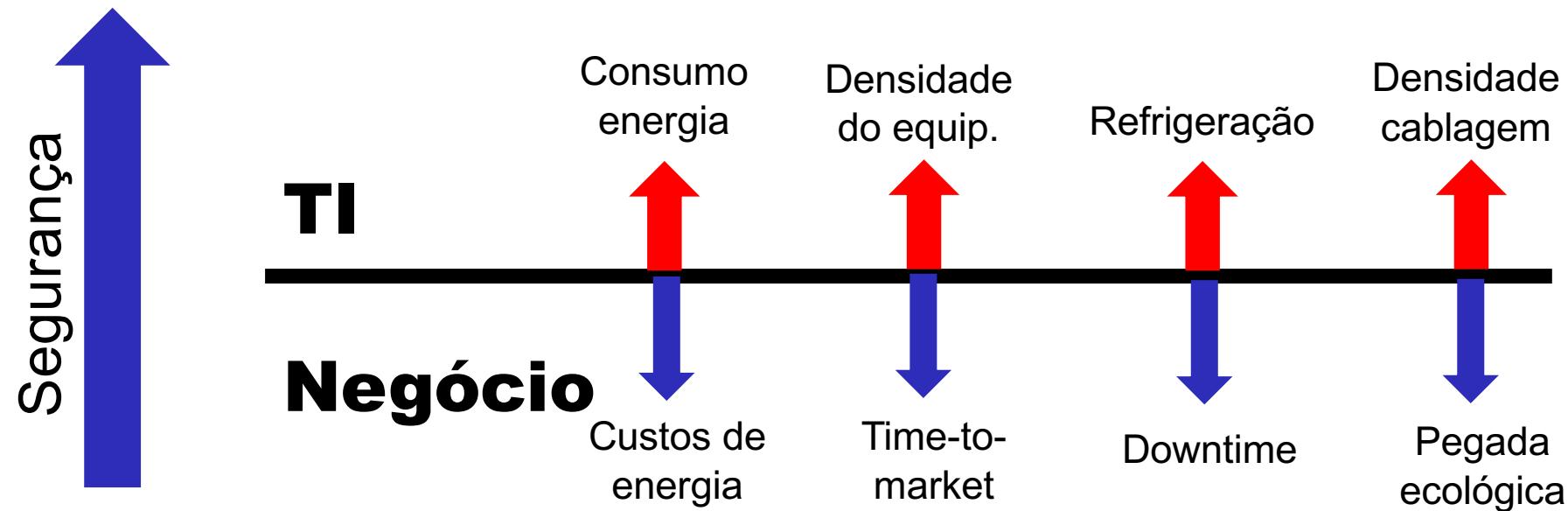
Requisitos gerais

- *Business continuity*
- Segurança (infraestrutura e dados)
- Edifício, infraestrutura física e *facilities*: TIA-942
- Equipamentos de telecomunicações: Telcordia GR-3160
- Uso de normas no desenho, conceção e implementação
- Modularização e escalabilidade para prever crescimento
- “*lights-out datacenter*” ou “*dark datacenter*”
- Acesso remoto e monitorização

Desafios no planeamento

- Localização física
- Aplicação eficiente das normas
- Dimensionamento do número de datacenters
- Definição de políticas de substituição de equipamento
- Virtualização
- Automatização (configuração, reserva de recursos, gestão de versões, processos, ...)
- Cuidados redobrados com a segurança

Desafios no planeamento



Desafios no planeamento

Desenho modular

- Crescimento à medida das necessidades
- Escalabilidade da operação

Freecooling

- Obter ar do exterior para arrefecimento
- Eficiência do processo de refrigeração
- Cumprir requisitos ASHRAE

Certificações

- Uptime Tier:
 - Ao nível do design
 - Ao nível das facilities
- Certificação LEED
- Cerificação ambiental

Visão integrada do edifício no ecossistema

Normalização

- “*Telecommunications Infrastructure - Standard for Data Centers: TIA-942*” <http://www.tia-942.org/>
- “*ANSI/NECA/BICSI -002 Data Center Design and Implementation Best Practices*”
- “*Label Standards – TIA-606*”
- “*Information technology –Generic cabling for customer premises - ISO/IEC 11801*”

Normalização

- “*Information Security Management System Standard: ISO 27001*” - <http://www.iso.org>
- “*ISO 50001:2011 Energy Management System Standard*” - <http://www.iso.org>
- “*ITIL -Information Technology Infrastructure Library*” (*best practices*)
- “*Information technology - Service management: ISO 20000*” - <http://www.iso.org>

Normalização: TIA-942 - componentes

Layout, espaços e facilities

Infraestrutura de cablagem

Níveis de fiabilidade

Considerações ambientais

Normalização: TIA-942 – componentes

Cablagem

- cobre e fibra óptica
- conectores e cabos
- equipamentos de interligação
- distâncias dos cabos
- gestão do espaço

Facilities

- dimensionamento do datacenter
- metodologia de gestão de energia
- caminhos de cabos e espaços
- AVAC, segurança e operações
- gestão do espaço e escalabilidade

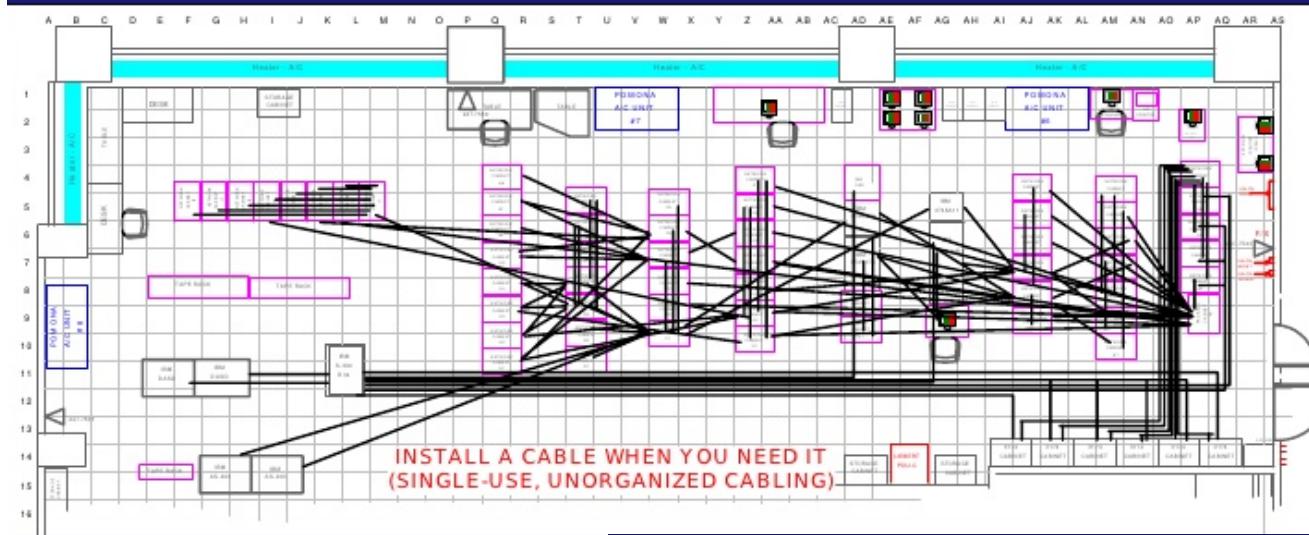
Rede

- suporte de sistemas legados
- uso de tecnologias emergentes

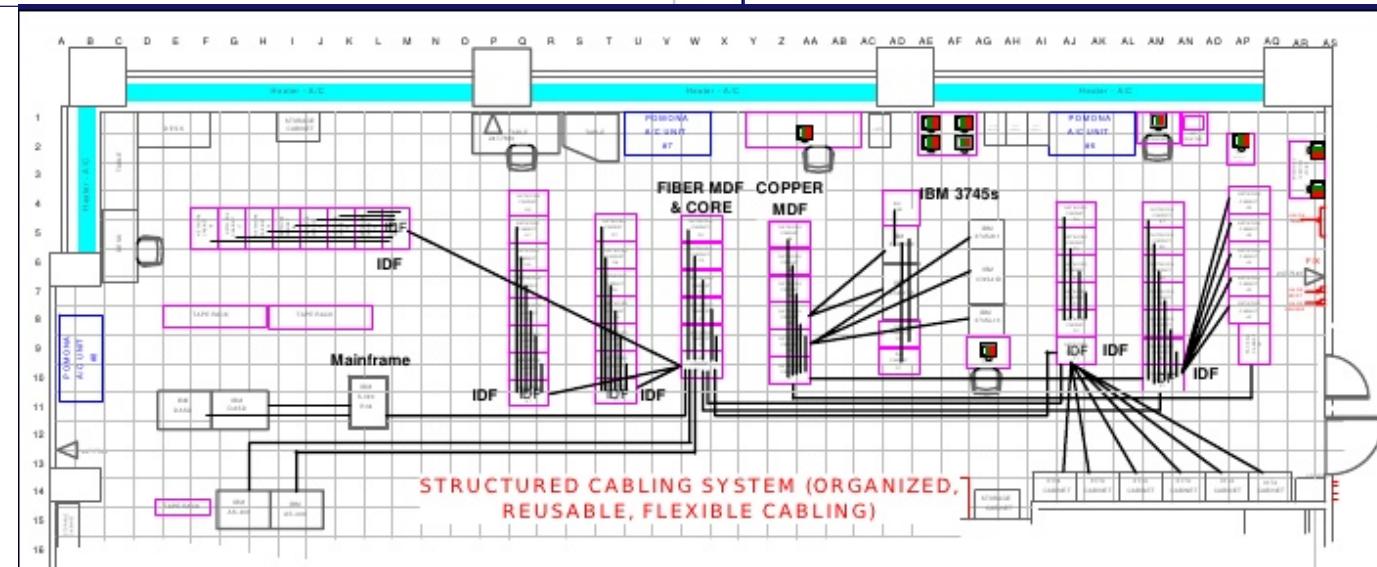
Anexos (com boas práticas)

- Annex A Cabling Design Considerations
- Annex B Telecom infrastructure Admin
- Annex C-Access provider information
- Annex D - Coordination of equipment plans with other engineers
- Annex E - Data center space considerations
- Annex F - Site selection

Normalização: TIA-942 - cablagem



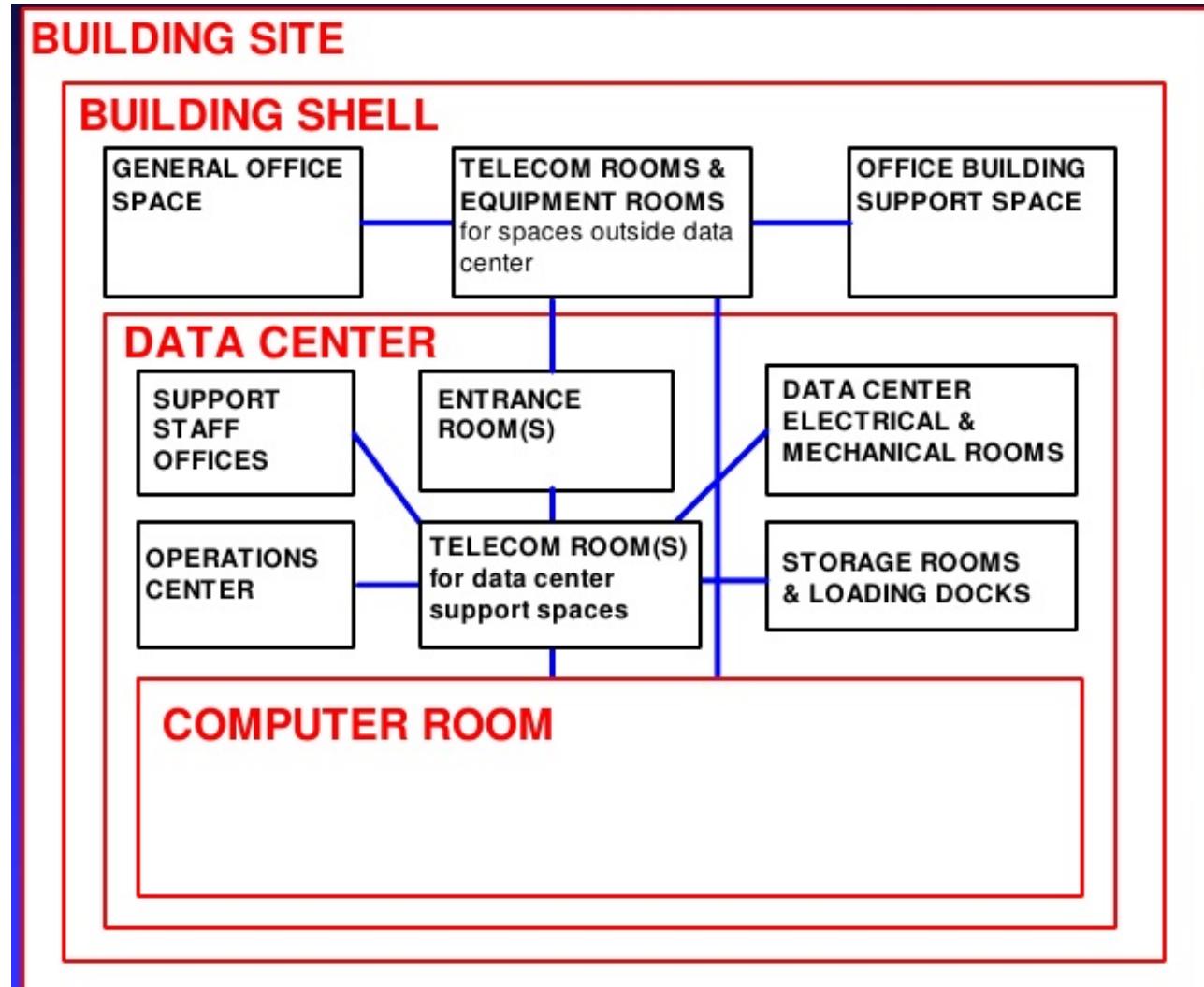
Cablagem não estruturada



Cablagem estruturada

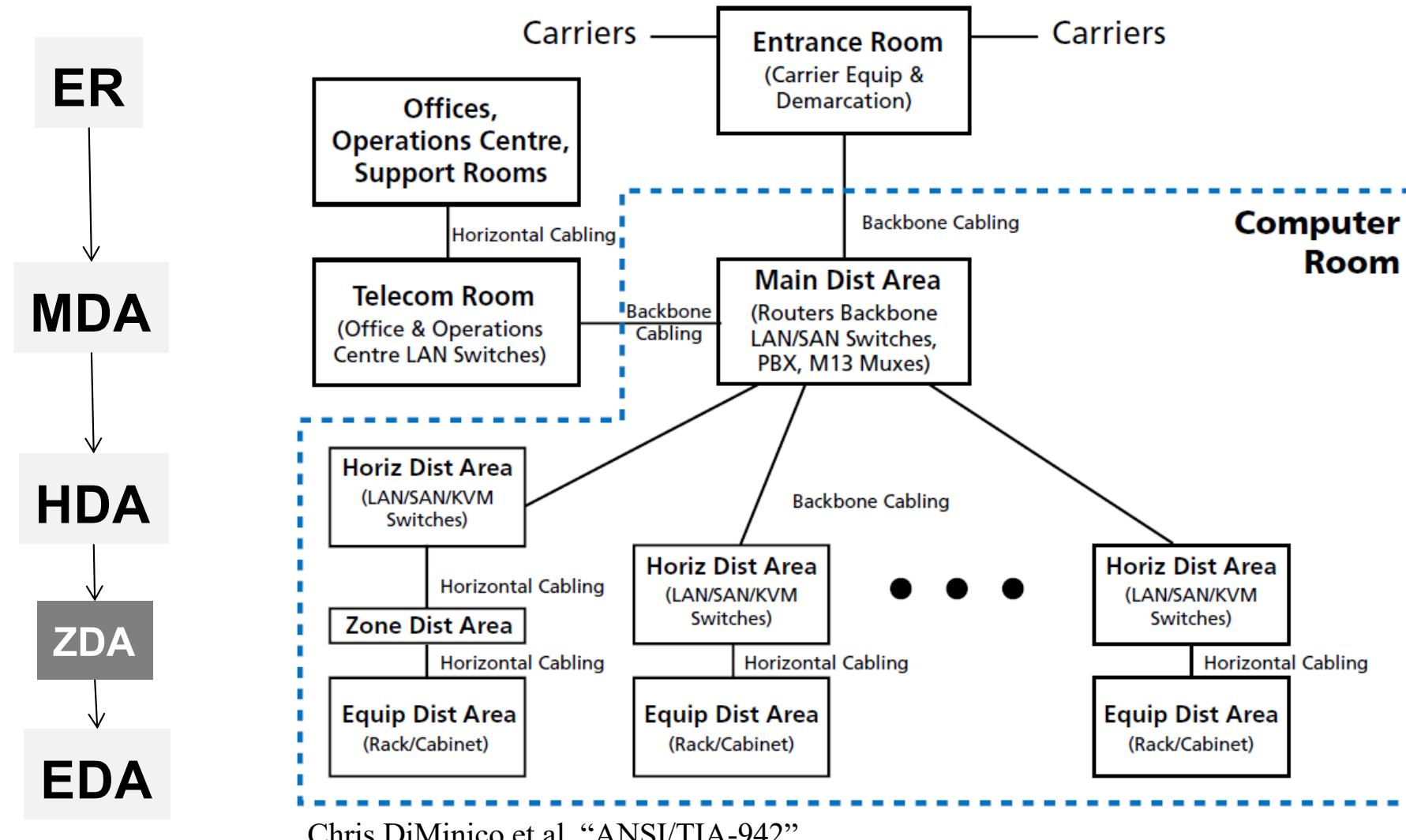
Chris DiMinico et al. “ANSI/TIA
ANSI/TIA-942”

Normalização: TIA-942 - espaços



Chris DiMinico et al. "ANSI/TIA-942"

Normalização: TIA-942 - topologia



Normalização: TIA-942 – cablagem horizontal

1. 100Ω Twisted Pair (ANSI/TIA/EIA-568-B.2), CAT 6 recomendado (ANSI/TIA/EIA-568-B.2-1)
2. Fibra multimodo, $62.5/125\mu$ ou $50/125\mu$ (ANSI/TIA/EIA-568-B.3)
3. Fibra monomodo (ANSI/TIA/EIA-568-B.3)
4. 75Ω coaxial (Telcordia Technologies GR-139-CORE)

Normalização: TIA-942 – cablagem horizontal

1. Distância máxima em cablagem horizontal = 90 metros para qualquer tipo de cabo
2. Distância máxima, incluindo equipamentos e chicotes = 100 metros
3. Para zonas de interligação de cablagem:
 - 300 metros para fibra (inclui equipamentos)
 - 100 metros para cobre (inclui equipamentos)

Normalização: TIA-942 – cablagem de backbone

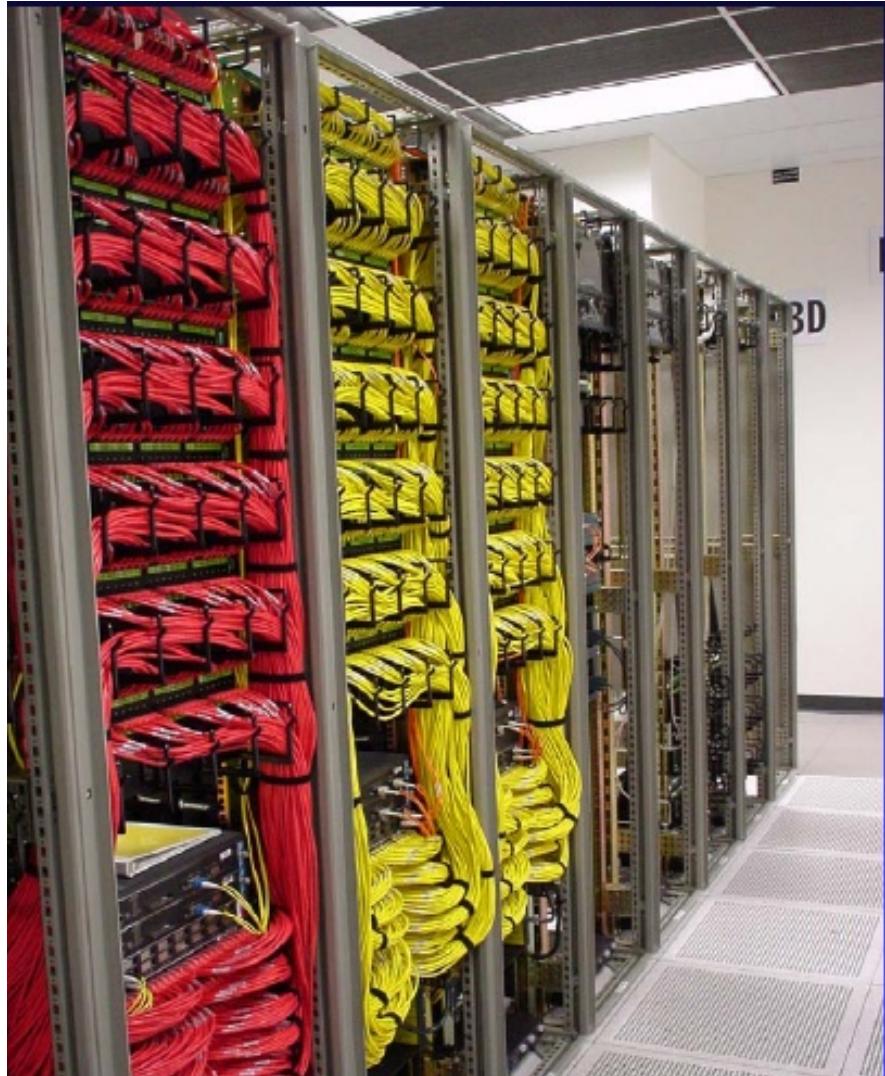
1. Inclui cablagem dos MDA para o ER e HDA e opcionalmente entre os HDA
2. Tamanhos máximos dependem das tecnologias usadas
3. Cablagem óptica centralizada, com topologia em estrela e sem ligações intermédias.
4. Topologias redundantes

Cabos devidamente arrumados: poupança de cerca de 10% de energia

Normalização: TIA-942 – sala de computadores

- Altura mínima de 2.6m
- Tamanho mínimo da porta: 1m de largura e 2.13m altura
- Carga suportada pelo chão: **7.2 kPA/150lbf/ft².**
Recomendado: **12 kPA/ 250 lbf/ft²** → 724 Kg/m²
- Temperatura ambiente: 20°C a 25°C → 1224 Kg/m²
- Humidade relativa: 40% a 55%
- Equipamento metálico, calhas e outras estruturas (Common bonding network - CBN), com ligação à terra.

Normalização: TIA-942 – bastidores

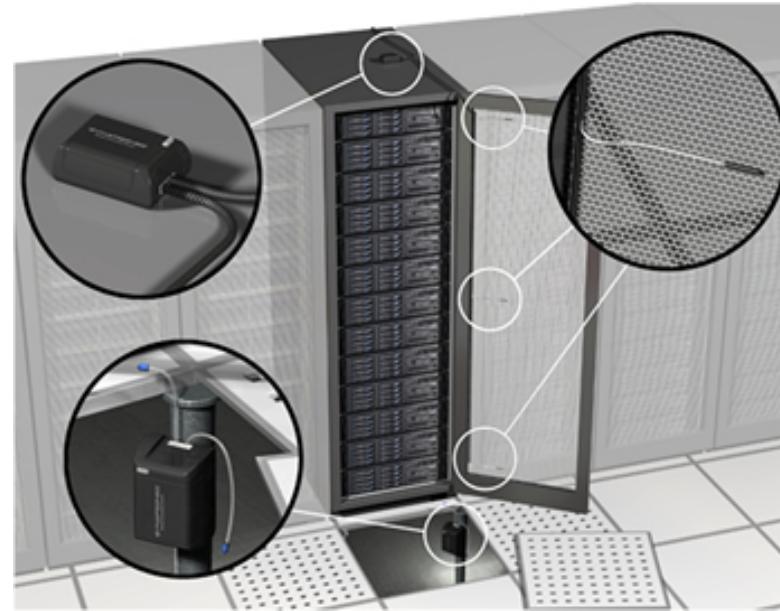


- Caminho de cabos frontais deverá facilitar manuseamento dos “*patch cords*”
- Minimizar número de switches para interligar cablagem
- Réguas perfuradas para encaixar equipamentos
- Bastidores com porta para evitar acesso físico
- Ventilação autónoma
- UPS integrada

Normalização: TIA-942 - bastidores

Racks

- Tripartidos
- Dual
- Full



Sensores para medição de temperatura, humidade e consumo de energia.

Racks com medidor independente de energia (32Amp/rack)

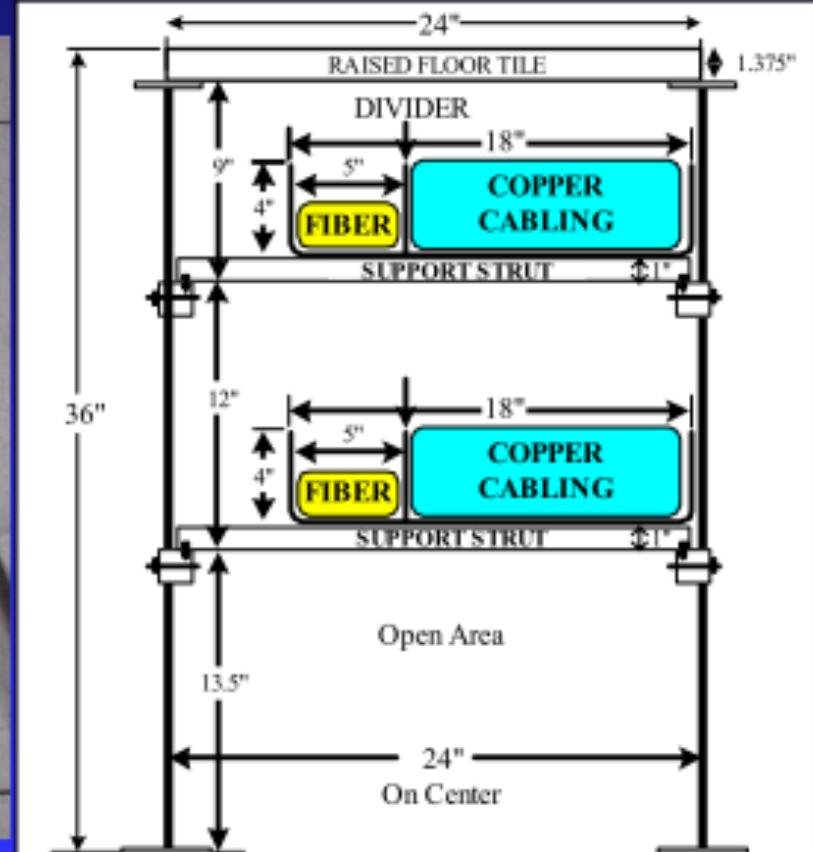
Distribuição de carga energética por várias fases.

Normalização: TIA-942 – chão levantado



- Acondicionamento da cablagem
- Permite maiores densidades de energia, melhor control e gestão da localização dos sistemas de arrefecimento
- Cada vez mais computadores estão preparados para serem ligados a partir do chão
- Recomendam-se calhas metálicas apropriadas, separando a cablagem de cobre, telecom e energia

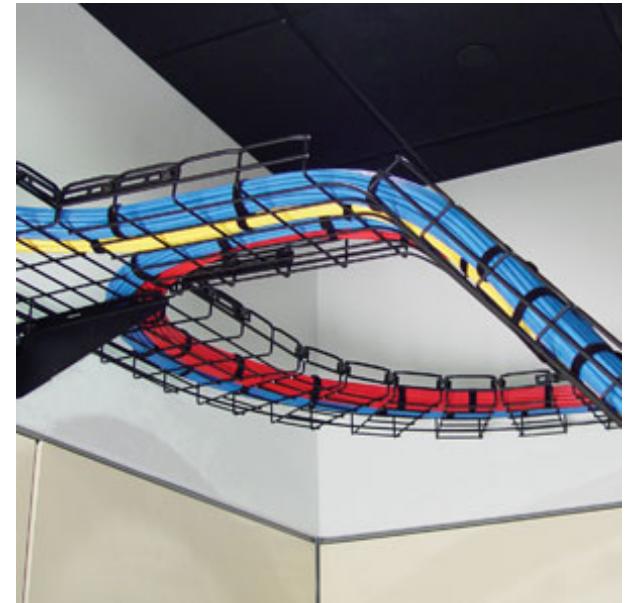
Normalização: TIA-942 – chão levantado



Chris DiMinico et al. “ANSI/TIA ANSI/TIA-942”

Normalização: TIA-942 – tecto “falso”

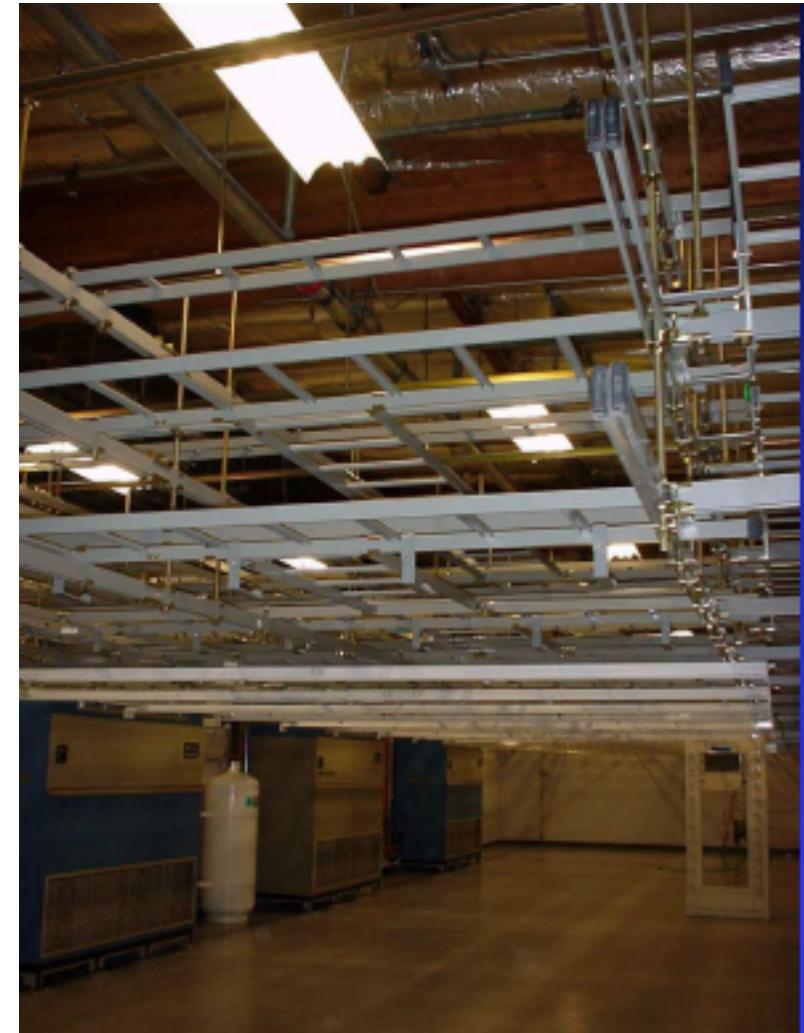
- Incluir calhas separadas para os vários tipos de cablagem



Chris DiMinico et al. “ANSI/TIA ANSI/TIA-942”

Normalização: TIA-942 – tecto “falso”

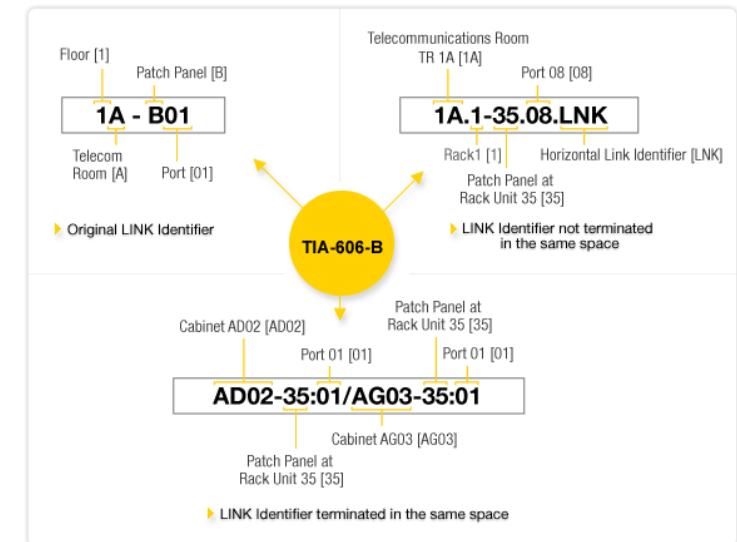
- Menos dispendioso que o chão falso
- Fixação fácil no tecto
- Maior flexibilidade para integrar com bastidores de altura diferente
- Podem existir várias camadas de calhas (cobre, energia, fibra)



Chris DiMinico et al. “ANSI/TIA ANSI/TIA-942”

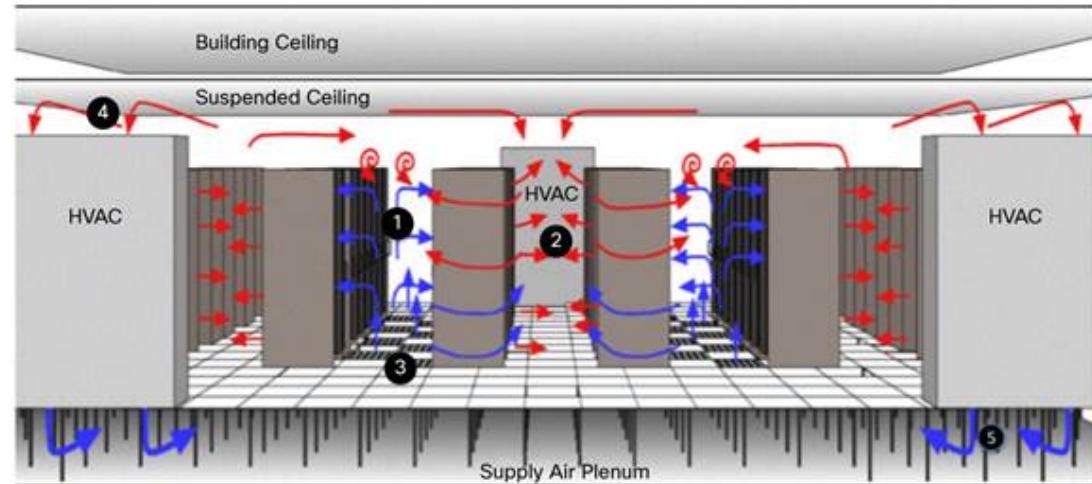
Normalização: TIA-942 – identificação

- Norma TIA-606 para etiquetagem de cablagem estruturada.
- Identificar todos os componentes do data center: bastidores, terminações em painéis de patch, equipamentos ativos,...
- Define esquema de cores e metodologia de identificação dos vários equipamentos por local e tipo.



Normalização: TIA-942 – elétrica e mecânica

- Definir equipamentos apropriados para AVAC, (des)humidificação, pressurização e deteção de incêndio
- Sistemas de refrigeração por circulação de água.
- Planeamento da distribuição de energia, cargas dos equipamentos e sistemas de UPS.



Normalização: TIA-942 – eletrica e mecânica



Refrigeração por circulação de água

UPS central



Normalização: TIA-942 – seleção do local

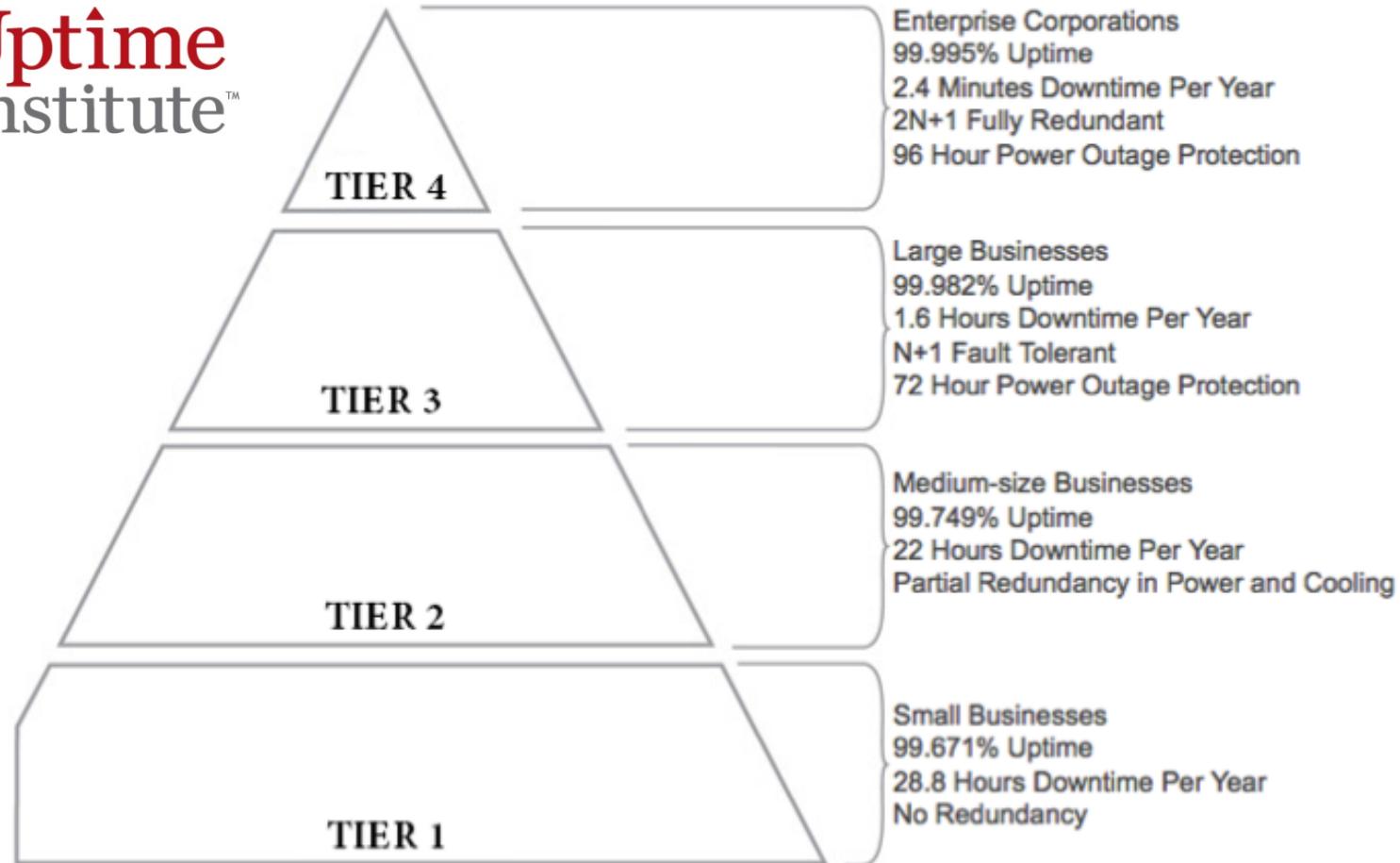
- Anexo (F) com guia sobre a escolha do local para construção de um datacenter, segundo os seguintes items:
 - Arquitetura
 - Eletrotécnico
 - Mecânico
 - Telecomunicações
 - Segurança
 - Outros

A ter em conta:

- Terramotos
- Inundações
- Iluminação
- Incêndios
- Furacões
- Tornados
- Fornecimento de energia

Normalização: TIA-942 - classificação

Uptime
Institute™



Fonte: www.datacenters.com

**Tolerância a
falhas**

**Manutenção
contínua**

**Componentes
redundantes**

**Instalação
básica**

Organização em bastidores (rack) - vantagens

- **Organização** – sistemas dispostos por afinidade e funcionalidade
- **Segurança** – acesso físico aos equipamentos é vedado, por exemplo, através de portas nos bastidores
- **Energia** – mecanismos centralizados de corrente elétrica, com sistemas de UPS autónomos
- **Arrefecimento** - mecanismos centralizados de arrefecimento, com sistemas de ventilação autónomos
- **Eficiência** – uso eficiente do espaço físico e das *facilities* disponíveis.

Organização em rack - desvantagens

- ✗ **Relocação difícil** – pouco viável a mudança sistemática de equipamentos
- ✗ **Cablagem** – difícil acomodação do elevado volume de cablagem. Implica dimensionamento apropriado.
- ✗ **Riscos físicos** – devido ao peso e à grande dimensão. Implica planeamento adequado.
- ✗ **Folga** – entre as filas de racks e no acesso a portas e corredores. Pode não ser aconselhável para todos os tipos de equipamentos.

Organização em rack - exemplos



www.collocationamerica.com



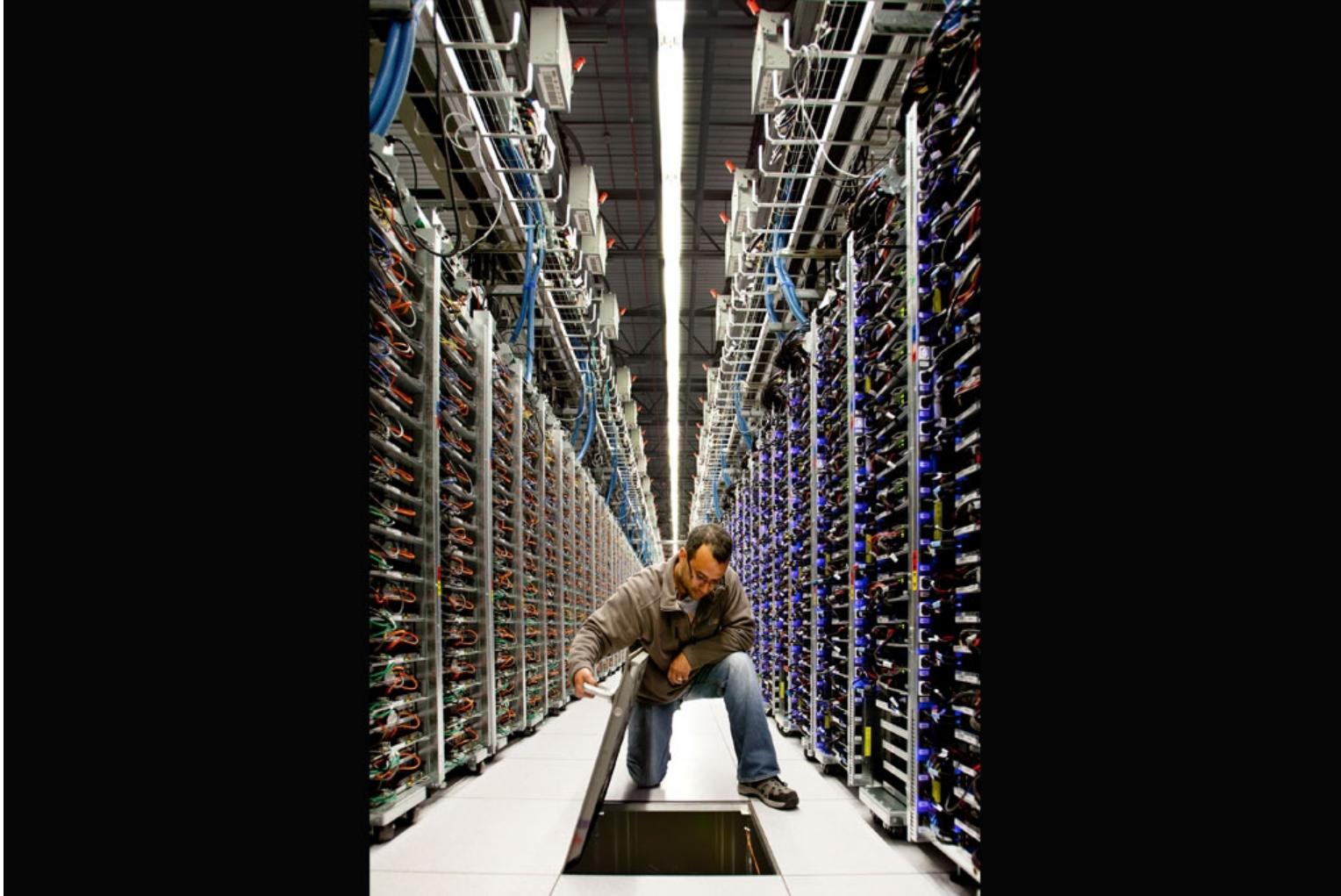
<http://www.ntsource.com>



<http://iltsarnews.blogspot.pt/>



Exemplo - Google



<http://p3.publico.pt/vicios/hightech/5093/google-vista-por-dentro>

Datacenters modulares



- Google's Hamina Data Center --> <http://www.youtube.com/watch?v=VChOEvKicQQ>
- Google container data center tour --> <http://www.youtube.com/watch?v=zRwPSFpLX8I>
- Google data center security YouTube --> <http://www.youtube.com/watch?v=wNyFhZTSnPg>
- Microsoft GFS Datacenter Tour --> <http://www.youtube.com/watch?v=hOxA1I1pQIw>
- SoftLayer DAL05 Data Center Tour --> <http://www.youtube.com/watch?v=YQERVf9ibzY>
- Huawei - <https://www.youtube.com/watch?v=soVDoqRVP5c>
- IBM BCBS - <https://www.youtube.com/watch?v=PXQpAD203Os>
- Mobile truck DC - <https://www.youtube.com/watch?v=Av8SI21h0-I>

Datacenters modulares



Key Performance Indicators (KPI)

- Profundidade da virtualização
- Número de VM por host
- Utilização de CPUs
- Densidade de energia elétrica e PUE
- Utilização de memória
- Alocação de espaço em disco
- Alocação de espaço físico
- Abrangência “green”

Eficiência energética

- Dimensionamento da energia varia entre alguns KW até vários MW!
- Densidade de energia utilizada: 100 x escritório típico
- Densidades superiores representam 10% do TCO de um DC
- Desafio atual:
 - Reduzir emissão de gases poluentes libertados pelos DCs, responsáveis por 2% das emissões de carbono [smart 2020]
 - Apostar em “green datacenters”, através da diminuição da energia usada para arrefecimento.

Eficiência energética

Power Usage Effectiveness (PUE) – métrica usada para medir a eficiência energética de um datacenter.

$$\text{PUE} = \frac{\text{Energia total consumida}}{\text{Energia consumida em IT}}$$

Hipotético ideal = 1.0

Médio dos DC no EUA = 2.0

[“Data Center Energy Forecast”, Silicon Valley Leadership Group, <http://svlg.org/>]

Médio dos DC state of the art < 1.2

[US Environmental Protection Agency ENERGY STAR Program - <http://www.epa.gov/>]

EU code of conduct for Datacenters

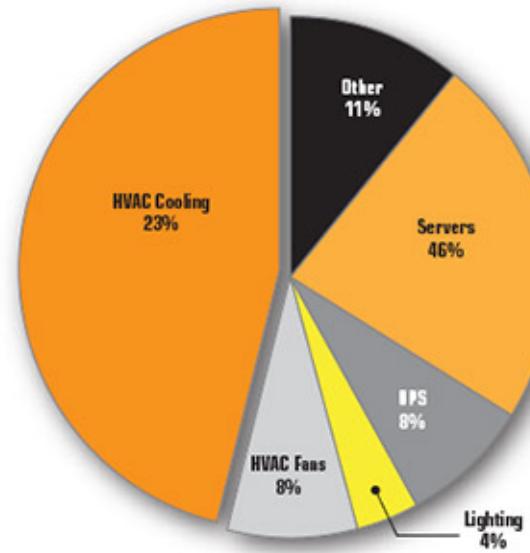
<http://iet.jrc.ec.europa.eu/energyefficiency/>

Eficiência energética – medir/reduzir PUE

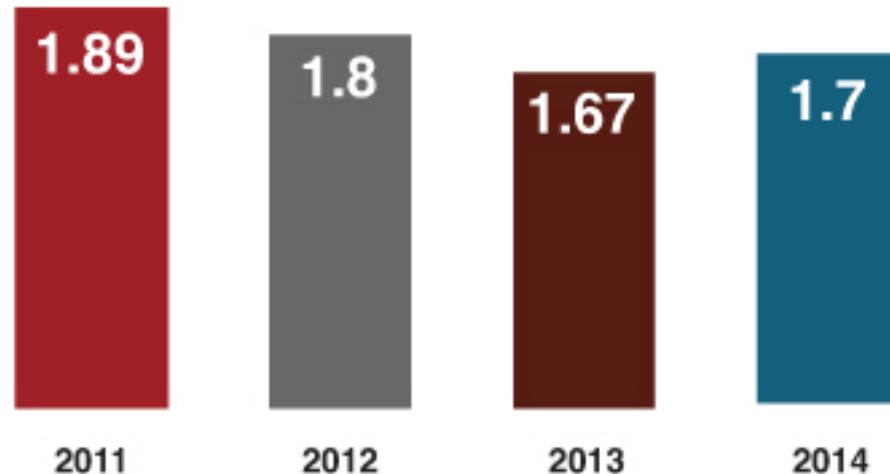
- Medida e análise da energia consumida em TI e AVAC.
- Computational Fluid Dynamics (CFD) analysis:
 - Interpretar condições térmicas do DC
 - Prever temperatura, fluxo de ar e pressão
 - Permite avaliar impacto na distribuição e densidade dos bastidores e nas necessidades de arrefecimento
- Mapeamento térmico com sensores para identificação dos pontos mais quentes do DC
- Reduzir PUE = reduzir consumo no arrefecimento!

Eficiência energética – medir/reduzir PUE

AVERAGE DATA CENTER POWER ALLOCATION



Average self-reported PUEs



DOES YOUR COMPANY MEASURE PUE?



By job function

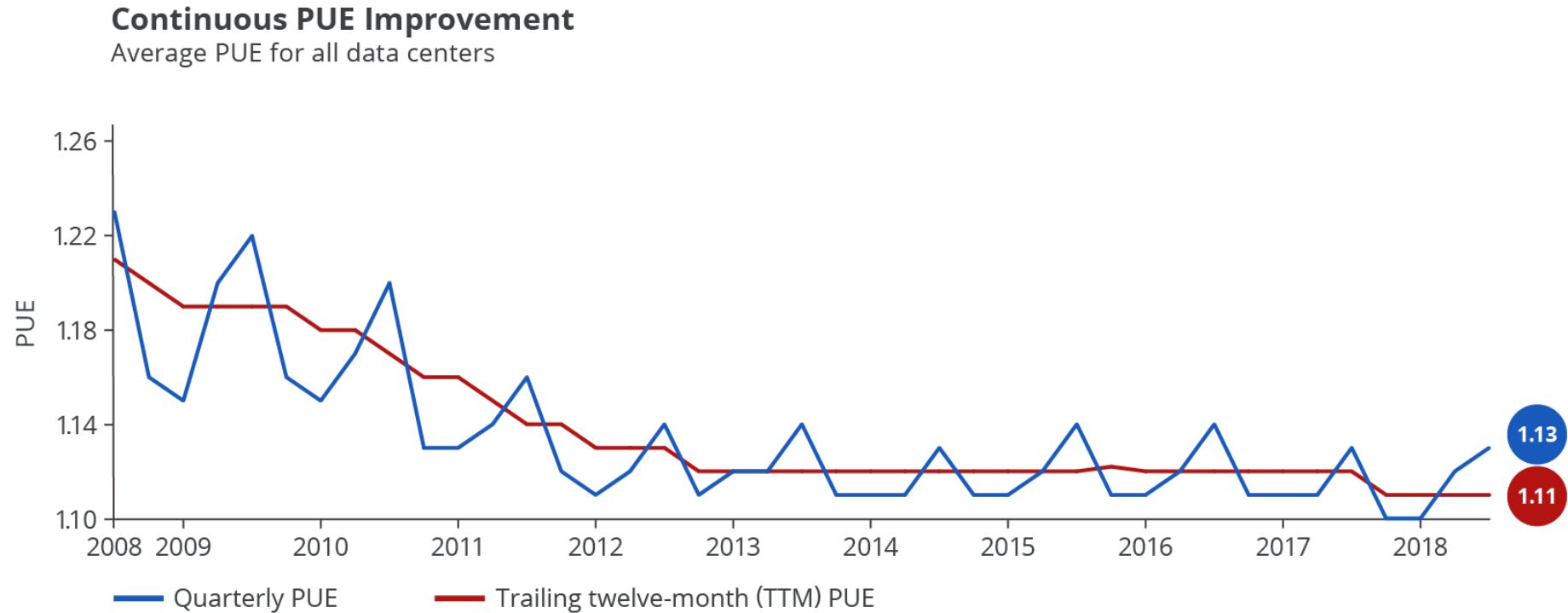


By vertical



Fonte: <https://www.uptimeinstitute.com>

Eficiência energética – o caso da Google



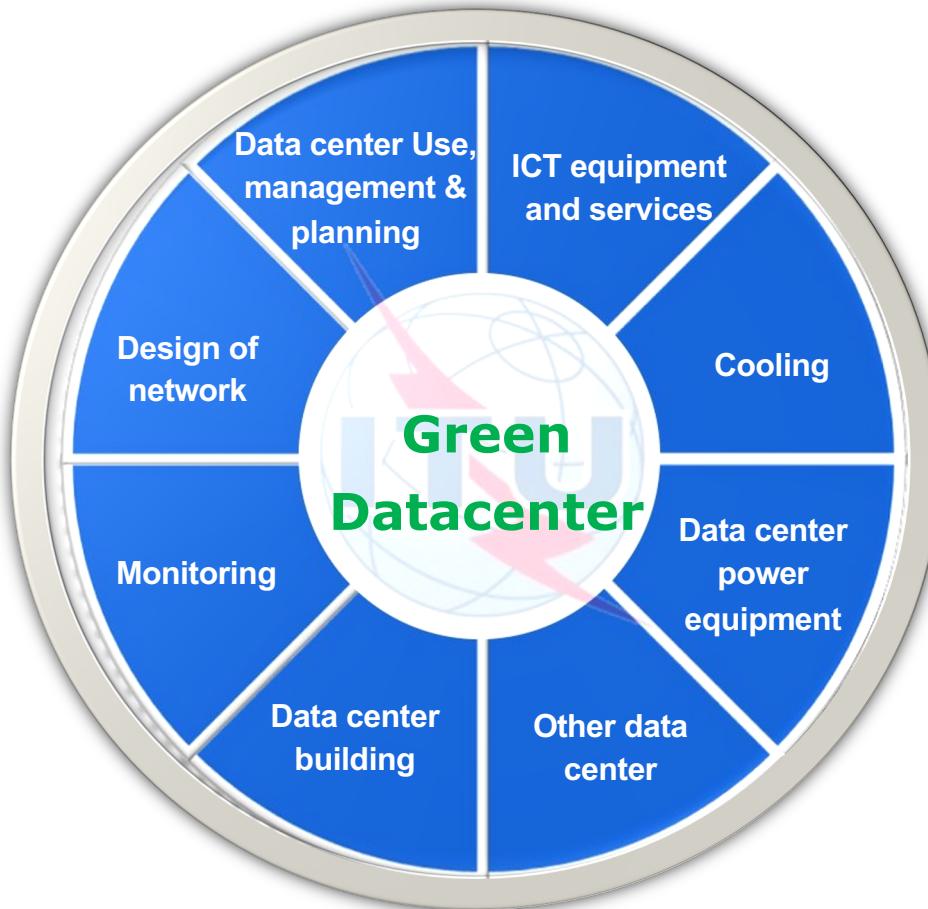
<https://www.google.pt/about/datacenters/>

<https://www.google.com/about/datacenters/efficiency/internal/>

Green datacenter



Recomendação ITU-T L.1300



Green datacenter – algumas boas práticas

- Gestão e planeamento da utilização de energia
- Escolha adequada do equipamento de IT: de acordo com as normas reguladoras REACH e WEEE, bem como consumo energético baixo
- Virtualização de servidores e diminuição do número de máquinas
- Gestão eficiente dos sistemas de aquecimento/arrefecimento
- Adotar a utilização de “energias limpas” (e.g. solar)
- Auditoria continuada aos equipamentos existentes



Segurança física

- Prevenção de crimes através de design ambiental:
 - Instalação de portas, áreas cercadas e paredes
 - Instalação de barreiras naturais e *open spaces*
 - Luminosidade
 - Vigilância permanente (CCTV, detetores de movimento, registo de acessos)
 - Alarmes

Segurança física

Acesso limitado à sala de computadores. Boas práticas:

- Cartões para acesso simultaneamente com chaves e cadeados
- Visitantes devem aceder com escolta.
- Cartões de proximidade
- Passes biométricos
- Palm veins
- Balança para pesagem na entrada e na saída, com antecâmara

Nalgumas salas pode ser exigida a presença de duas pessoas simultaneamente.

Conclusões

- Evolução dos datacenters confunde-se atualmente com a “cloud”
- Normalização assegura classificação dos datacenters independentemente da marca
- Evolução natural para a ubiquidade nas operações (datacenters modulares)
- Importância das boas práticas no planeamento e dimensionamento dos datacenters a M/L prazo
- Aspetos fundamentais da operação: automatização e monitorização.

Conclusões

- Selo “green” tem cada vez mais valor no mercado de DC
- Cálculo do PUE com várias interpretações – PUE com impacto no negócio
- Redução efetiva do PUE consegue-se maioritariamente através do redimensionamento dos sistemas de arrefecimento

Bibliografia

- “Telecommunications Infrastructure Telecommunications Infrastructure- Standard for Data Centers Standard for Data Centers TIA-942” - <http://www.tia-942.org/>
- “Uptime Institute” - <https://uptimeinstitute.com>
- Luiz André Barroso, Jimmy Clidaras, Urs Holzle; “The datacenter as a computer”; Morgan and Claypool Editors; ISBN: 978-1627050098; 2013 [pdf]

A tutorial on high availability clusters

Fundamentals



**Public businesses
Unacceptable outage
Uninterrupted services**



Fundamentals



Negative impact in companies' profit and business
Unacceptable in E-commerce and E-business companies
Colateral damages in global companies and economies

Business Continuity and Disaster Recovery

Fundamentals



Some Exchange customers are experiencing email delays, we are working to resolve, please see the SHD for service status

Reply Retweet Favorite More

Follow

facebook.com

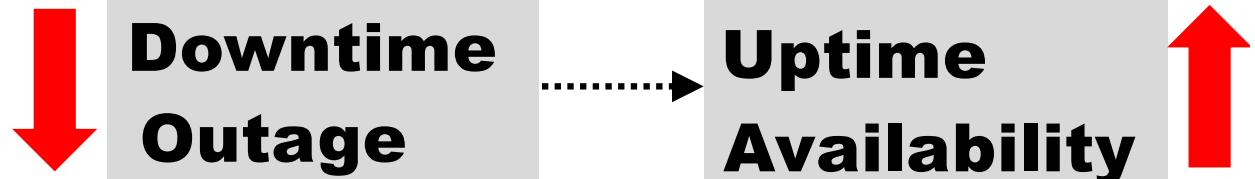
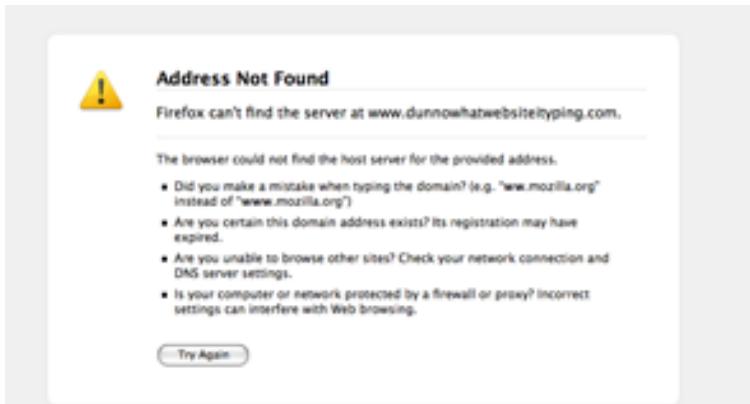
facebook

Sorry, something went wrong.

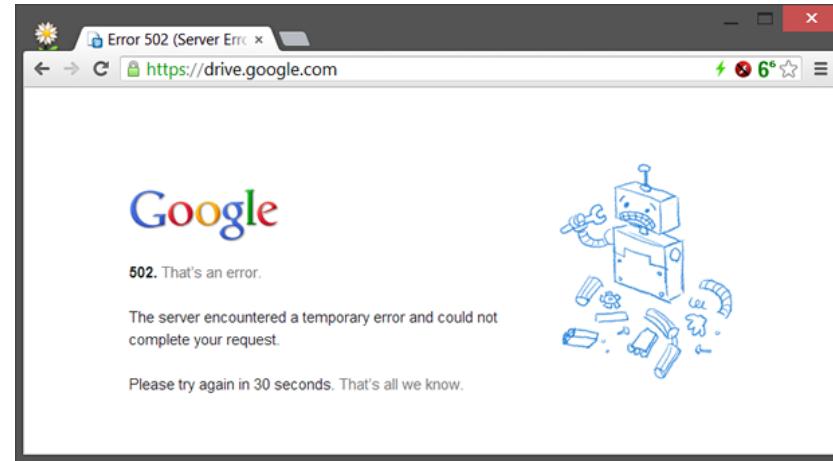
We're working on getting this fixed as soon as we can.

[Go Back](#)

Facebook © 2013 · [Help](#)



Fundamentals



We're sorry, but your Gmail account is temporarily unavailable. We apologize for the inconvenience and suggest trying again in a few minutes. You can view the [Apps Status Dashboard](#) for the current status of the service.

If the issue persists, please visit the [Gmail Help Center](#).

[Try Again](#) [Sign Out](#)

[Show Detailed Technical Info](#)

©2016 Google - [Gmail Home](#) - [Privacy Policy](#) - [Program Policies](#) - [Terms of Use](#) - [Google Home](#)

http://www.google.com/appsstatus

Fundamentals – a definition for availability

- Measure the percentage of time (hour, day, month) in which the service is available for the end-user.
- Should be globally analysed and not by the components separately.
- Should be measured in a user perspective.
- Its value has positive (or negative) impact in the business.

Fundamentals – a definition for availability



Fundamentals – a definition for availability

$$D = \frac{\text{Uptime}}{\text{Operation}} \quad \text{with } D \in [0, 1]$$

Uptime = duration of uptime period (h, min, week, day, month,...)

Operation = duration of total period of operation (h, min, week, ...)

Example: Availability in a week (168h) for a uptime of 165h.

$$D = \frac{165}{168} = 0.9821 = 98.21\%$$

Fundamentals – a definition for availability

	Per Hour	Per Day	Per Week	Per Year
99.999%	.0006	.01	.10	5
99.98%	.012	.29	2	105
99.95%	.03	.72	5	263
99.90%	.06	1.44	10	526
99.70%	.18	4.32	30	1577

Values for *downtime* (minutes)

- 24x60x365 operation:**
- 525600 minutes per year
- 24x7x60 operation:**
- 10080 minutes per week

An availability of **99.999%** means 5 minutes of *downtime* in a year!

At least three decimal digits should be used ("The myth of nines")

A common metric widely used to assess infrastructure effectiveness

Fundamentals – mean availability

- **Measures for availability (mean time)**

Mean Time Between Failures (MTBF) = $\frac{\text{Operation}}{\text{Total failures}}$
Mean duration of component (hardware) downtime.

Mean Time to Repair (MTTR) = $\frac{\sum \text{Repair}}{\text{Total failures}}$
Mean time to repair a component.

When applied to
network services

Mean Time Between Service Outage (MTBSO)
Mean Time To Service repair (MTTSR)

Fundamentals – mean availability

$$\text{Mean availability} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}$$

MTBF=1000h



MTTR=1h

$$D_{\text{mean}} = \frac{1000}{1001} = 99,90\%$$

$$\text{Mean availability} = \frac{\text{MTBSO}}{\text{MTBSO} + \text{MTTSR}}$$

MTBSO=1000 h



MTTSR=3h

$$D_{\text{mean}} = \frac{1000}{1003} = 99,70\%$$

$$\text{Annualized Failure Rate (AFR)} = \frac{365 \times 24}{\text{MTBF}} = \frac{8760}{\text{MTBF}}$$

Example: Standard S.M.A.R.T for disks

S.M.A.R.T. = Self-Monitoring, Analysis and Reporting Tech.

- Available for HDD and SSD devices
- It detects and reports several disks' fiability indicators
- Goal: to antecipate hardware failures

In Linux:

```
smartctl -i /dev/sda
```

```
smartctl -a /dev/sda
```

Fundamentals – common downtime causes



Planned

Proactive maintenance

Hardware replacement

Hardware upgrade

Software upgrade

Users are usually warned.



Unplanned

Reactive response

Hardware, Natural, Power and network failures

Web and DB server down

DNS server down

Vulnerabilities exploits

No time to warn users.
Backup strategies should start

Fundamentals – downtime costs

Considering:

- 24x7 operation
- $D_{mean} = 98.1\%$
- Cost of downtime per hour = 10,000€



Then:

- Downtime = 3.192 hours per week
- Total cost of downtime $\approx \underline{31,920\text{€}}$ per week

If $D_{mean} = 99.9\%$ then downtime ≈ 10 minutes (0.166h) = 1660€

Gain = 31.920€ - 1660€ = **30.260€ per week!**

Fundamentals – downtime costs



Direct

Business activities

Productivity

Intranet and internal processes



Indirect

Clients' dissatisfaction

Stock options

Negative publicity

Legal processes

Company reliability

External reputation

Worker's performance impact



Fundamentals – downtime costs

- How does it cost to reduce downtime from 3.2h to 10 minutes?
- What if we reduce from 3.2h to 1 h?
- The benefits worth the investment?

What is the ROI on applying the measures?

- Reduce the risk (**R**) before (**b**) and after (**a**) the investment
- Assess potential gains (**G**) after the investment (**I**)

$$G = R_b - R_a$$

$$ROI = \frac{G - I}{I} , \text{ being } I \text{ the cost of preventive measures}$$

Fundamentals – calculating the risk

- Probability (P) of an event
- Duration (D) of the downtime event
- Impact (I), means the percentage of affected users

The effect of an event (E_x) is measured by its value before (b) and after (a) of applying the preventive measures.

$$E_{ax} = P_{ax} \times D_{ax} \times I_{ax} \quad \text{Downtime cost}$$

$$E_{dx} = L_{dx} \times D_{dx} \times I_{dx} \quad \text{Implementation cost}$$

$$R_{\text{before}} = C_D \times (E_{b1} + E_{b2} + \dots + E_{bx})$$

$$R_{\text{after}} = I + (C_D \times (E_{a1} + E_{a2} + \dots + E_{ax}))$$

Fundamentals – calculating the risk

$$G = R_a - R_d$$

$$R_a > R_d$$

$$G = C_D \times (E_{a1} + E_{a2} + \dots + E_{ax}) - I + (C_D \times (E_{d1} + E_{d2} + \dots + E_{dx}))$$

$$G > 0$$

$$ROI = \frac{G - I}{I} \%$$

(annual basis or per cycle)

Examples:

Marcus E, Stern H., “*Blueprints for high availability*”; 2003; Wiley; ISBN: 0471430269;
pp. 42-46

Fundamentals – calculating the risk

Calculating the effect before applying the measures:

Table 3.2 Effects of Outages before Clustering Software Is Installed

OUTAGE TYPE	BEFORE DURATION (D)	BEFORE LIKELIHOOD (L)	BEFORE IMPACT (I)	BEFORE EFFECT (D × L × I)
Crash and reboot	60 minutes*	10 [†]	100%	$E_{B1} = 600$ (during the day)
Crash and reboot (off-hours)	120 minutes [‡]	10 [†]	75% [§]	$E_{B2} = 900$
Scheduled reboot	30 minutes	60	50% [§]	$E_{B3} = 900$
Motherboard or other major hardware failure	24 hours (1,440 minutes)*	2	100%	$E_{B4} = 2,880$
Network card failure	4 hours (240 minutes)**	2	100%	$E_{B5} = 480$
Application failure	60 minutes	20 ^{††}	100%	$E_{B6} = 1,200$
Scheduled maintenance	4 hours (240 minutes) [#]	20	50%	$E_{B7} = 2,400$
Failover testing	0 ^{§§}	0	0	$E_{B8} = 0$

Total effect of outages:

9,360 minutes (99.644 percent availability over 5 years)

Marcus E. Stern H., “Blueprints for high availability”; 2003; Wiley; ISBN: 0471430269;

Fundamentals – calculating the risk

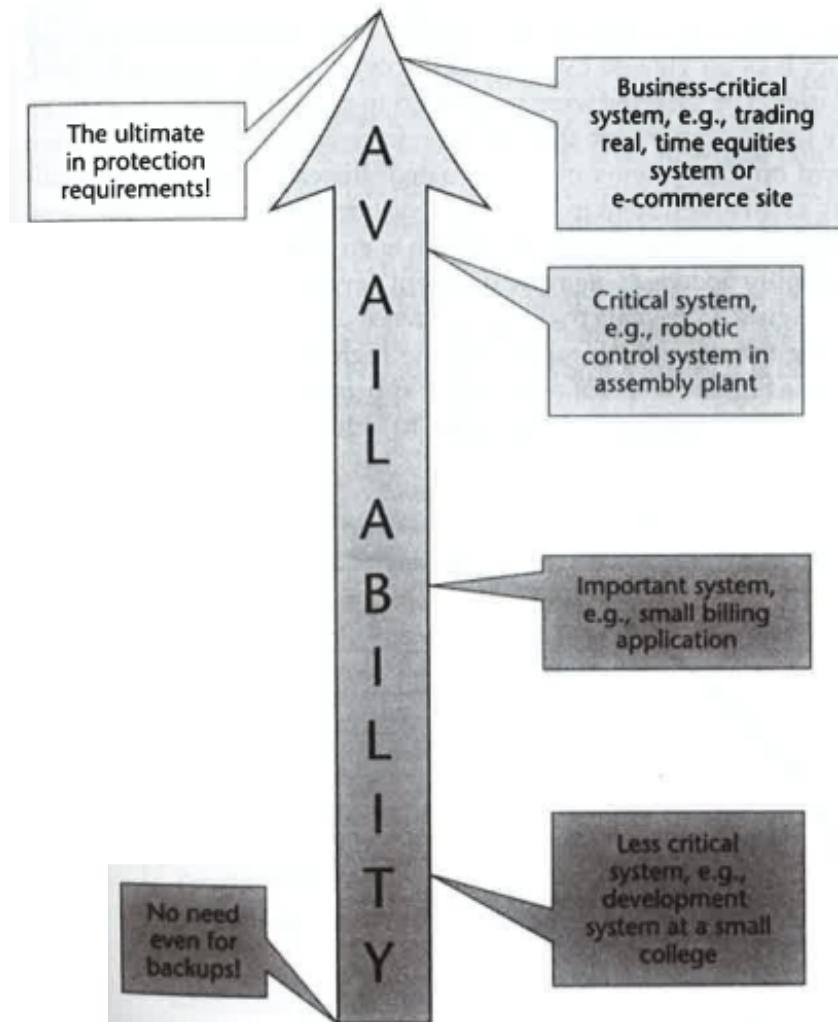
Calculating the effect after applying the measures:

Table 3.3 Effects of Outages after Clustering Software Is Installed

OUTAGE TYPE	AFTER DURATION (D)	AFTER LIKELIHOOD (L)	AFTER IMPACT (I)	AFTER EFFECT (D × L × I)
Crash and reboot	5 minutes [†]	10	100%	$E_{A1} = 50$ (during the day)
Crash and reboot (off-hours)	5 minutes [†]	10	75%	$E_{A2} = 37.5$
Scheduled reboot	5 minutes	60	50%	$E_{A3} = 150$
Motherboard or other major hardware failure	5 minutes	2	100%	$E_{A4} = 10$
Network card failure	2 minutes, then 5 minutes [‡]	2	100% then 50%	$E_{A5} = 9$
Application failure	3 minutes [§]	20	100%	$E_{A6} = 60$
Scheduled maintenance	5 minutes	20	50%	$E_{A7} = 50$
Failover testing	5 minutes	20	50%	$E_{A8} = 50$
Total effect of outages:				416.5 minutes (99.984 percent availability over 5 years)

Marcus E, Stern H., "Blueprints for high availability"; 2003; Wiley; ISBN: 0471430269;

Fundamentals – calculating the risk



Hospitals
Aviation systems
Other highly critical systems

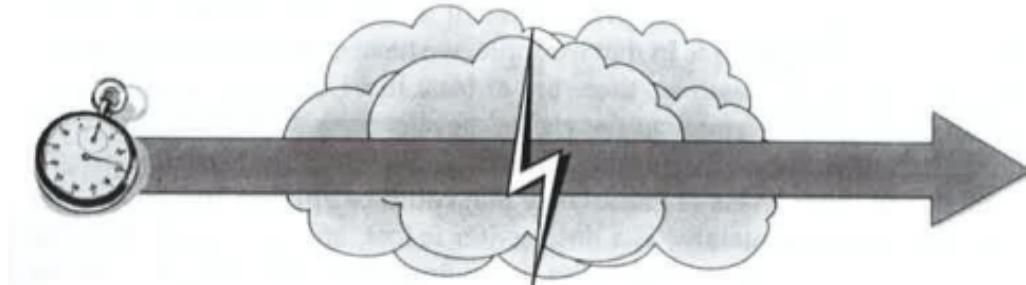
Web-based businesses
Industrial-based businesses

Universities and schools
Other less critical businesses

Small businesses
Inactive computers

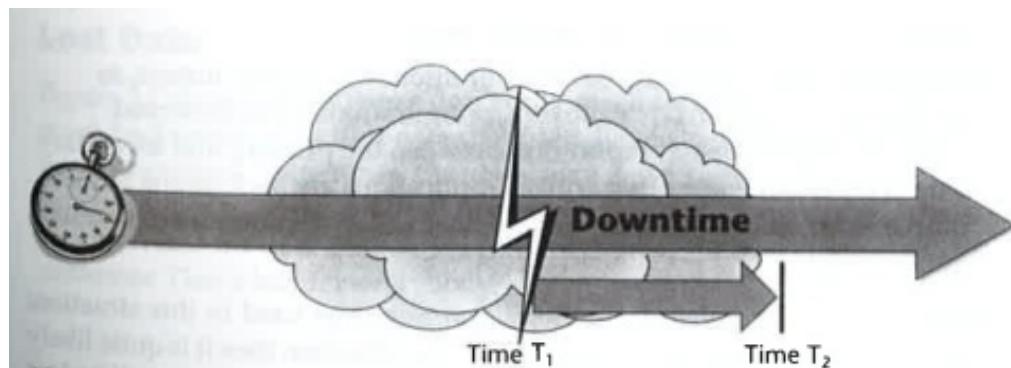
Marcus E, Stern H., "Blueprints for high availability"; 2003; Wiley; ISBN: 0471430269;

Outage lifecycle



Begin of an outage

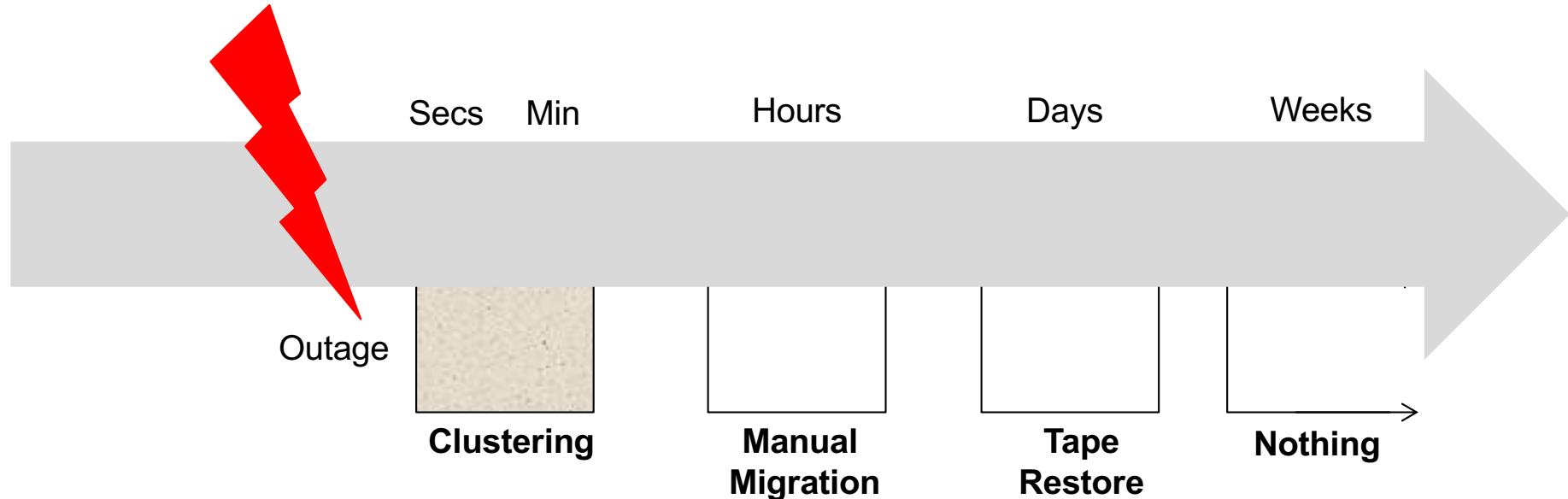
Marcus E, Stern H., "Blueprints for high availability"; 2003; Wiley; ISBN: 0471430269;



[T₁; T₂] - Downtime

Marcus E, Stern H., "Blueprints for high availability"; 2003; Wiley; ISBN: 0471430269;

Outage lifecycle – outage mitigation

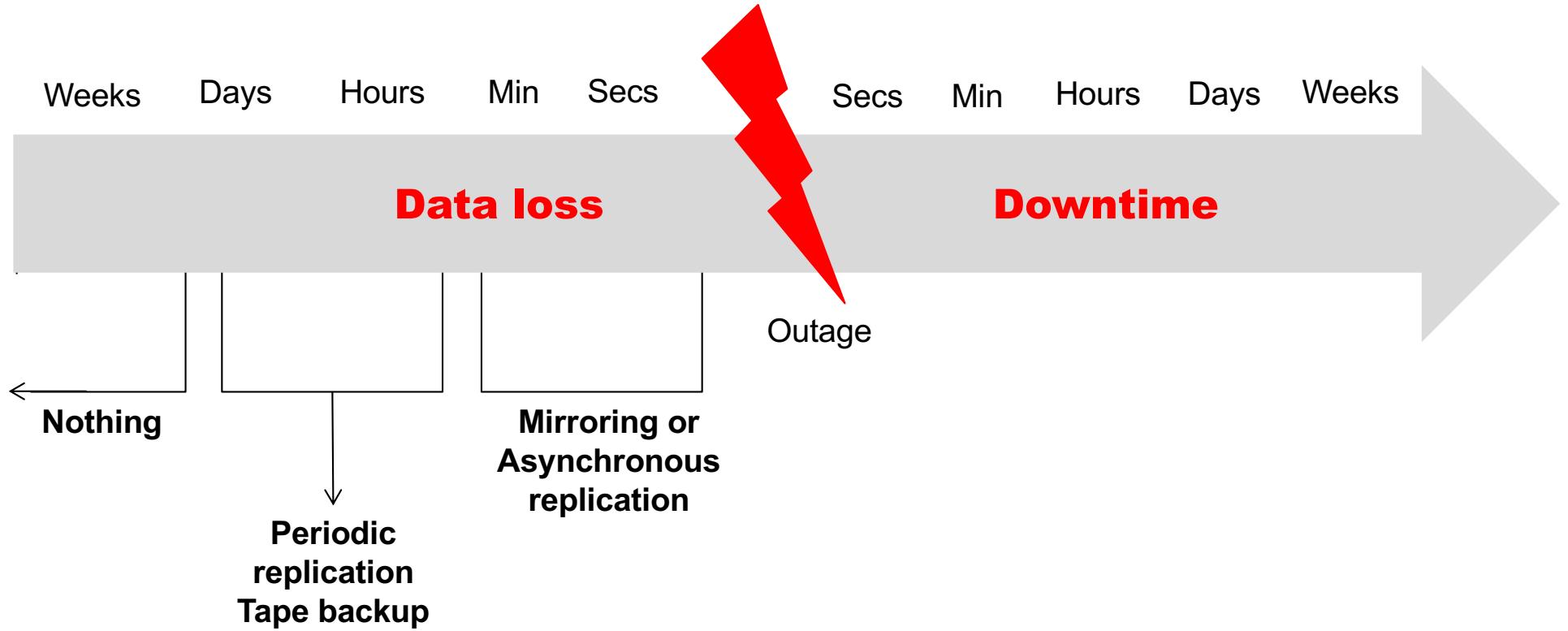


Time is an important variable

Downtime will happen in the presence of an outage

Goal: to mitigate outage in a minimum period of time

Outage lifecycle – data loss mitigation

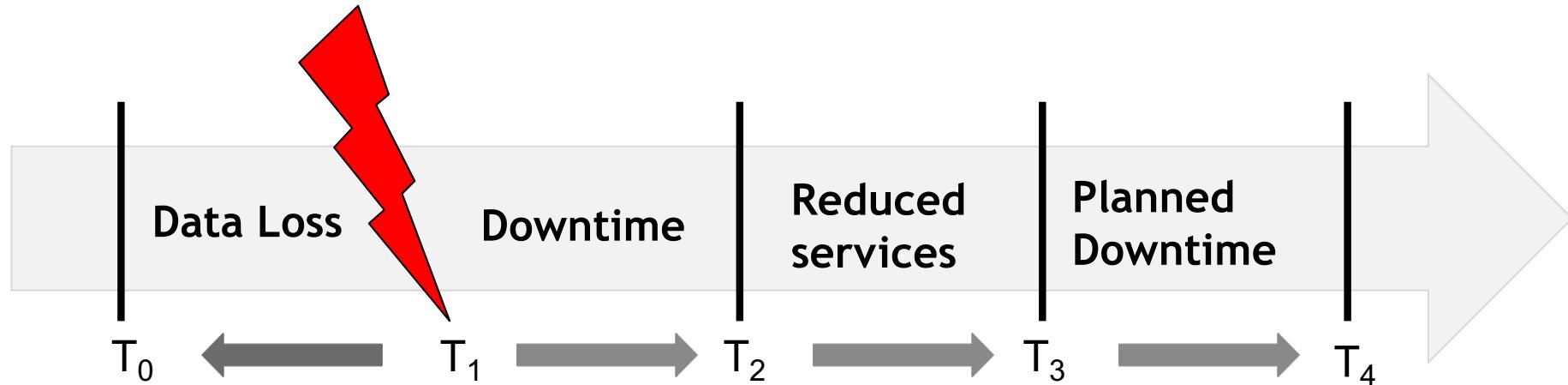


Time is again an important variable

Outage will cause data loss

Goal: to minimize data loss and to assure system consistency

Outage lifecycle



HA implementation is a business decision.

How much does it cost the infrastructure downtime?

How much does it cost to implement HA procedures to mitigate downtime?

Impact on the organization

- To define clear and tangible goals
- To define a physical environment
- To automate processes
- To define environment for testing and QA
- To create a stock of physical components
- To adjusts contracts for critical components
- To schedule processes
- To plan catastrophic scenarios
- To train
- To document everything!

Impact on the organization - vulnerabilities

VULNERABILITY	LIKELIHOOD (1-3)	IMPACT (1-3)	LEVEL OF CONCERN (LIKELIHOOD × IMPACT)	COMMENTS
Failed disk	3	1	3	Critical systems already have mirrored disks.
Blown CPU	2	2	6	Systems are not clustered; a failed CPU will result in major downtime for one server.
Database corruption	2	3	6	Corruption in a critical database could shut down the web site for hours.
Unreadable backups	1	2	2	Only an issue if we lose data from our disks. Then it could be quite serious.
Network component failure	2	2	4	We have a very complex network, with many single points of failure.
Data center fire	1	3	3	Could cause the loss of our entire computing infrastructure.
Extended power outage	2	2	4	Won't damage data, but could keep us down for a long time.
Flooding	2	3	6	This area has a history of flooding. With the data center in a low floor, results could be catastrophic.
Chemical spill	1	3	3	An interstate highway goes within 200 yards of the front door. Always a small risk.
Tornado	1	2	2	Would have to hit the building to be a major problem.
Earthquake	2	3	6	Can, of course, be a major disaster.
Bioterrorism	1	3	3	Unlikely, but if it happened, could be serious.

Marcus E, Stern H., "Blueprints for high availability"; 2003; Wiley; ISBN: 0471430269;

HA design – 20 goals

1. Don't be cheap (€ £ \$)
2. Assume nothing from constructors, trades, etc...
3. Remove single points of failure (SPOF)
4. Enforce security (physical, logical)
5. Redefine number of servers
6. Performance measurements
7. Enforce changes to the configuration

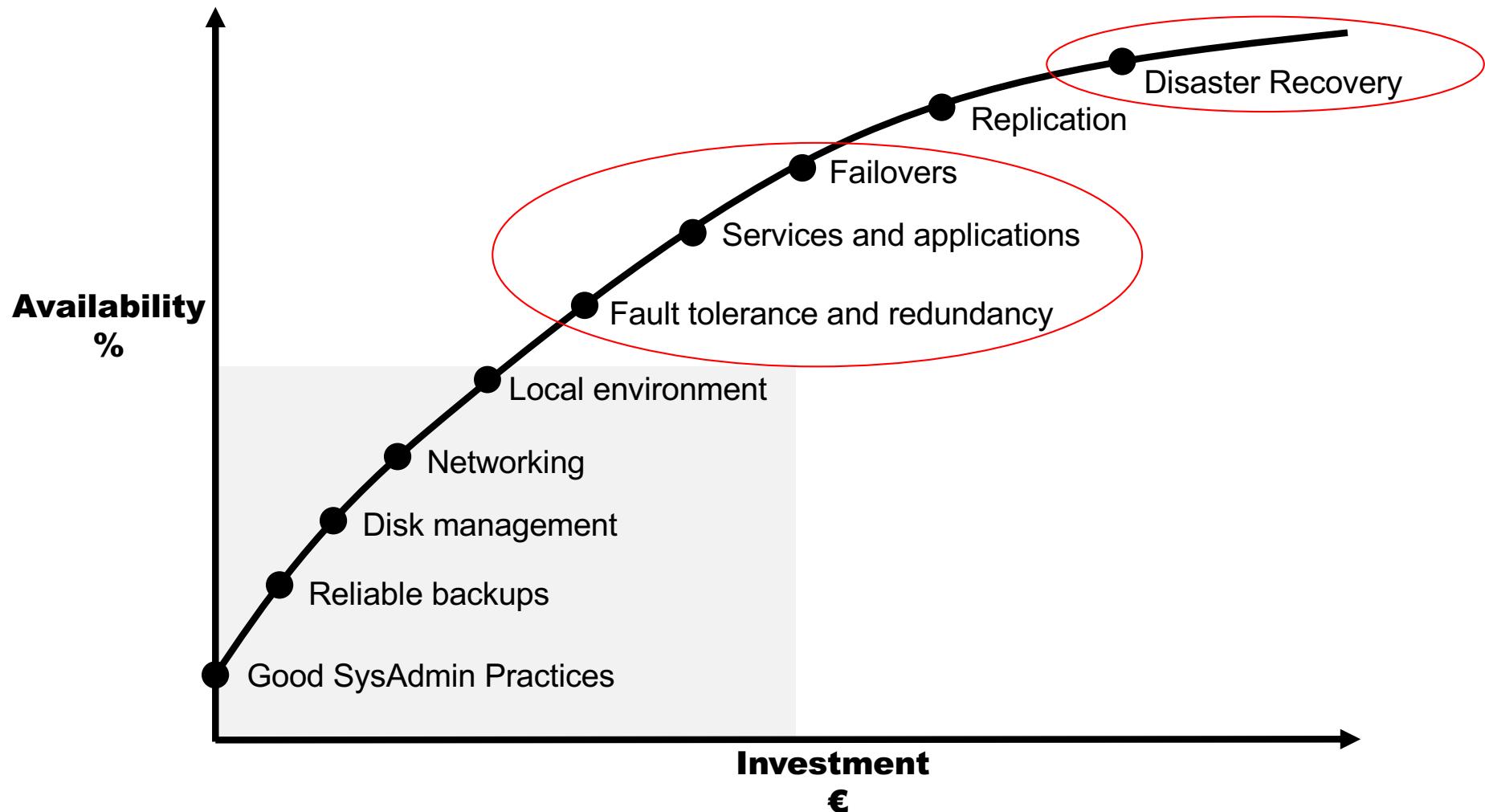
HA design – 20 goals

8. Document everything
9. Define and apply SLA
10. Proactive planning
11. Test everything
12. Separate environments (production, test, QA, dev,...)
13. Learn from history
14. Design for growth

HA design – 20 goals

15. Choose mature software with support
16. Choose mature and reliable hardware
17. Reuse configurations
18. Resources (papers, BCPs, bibliography, ...)
19. One problem, one solution!
20. “Keep it simple!”

Availability index

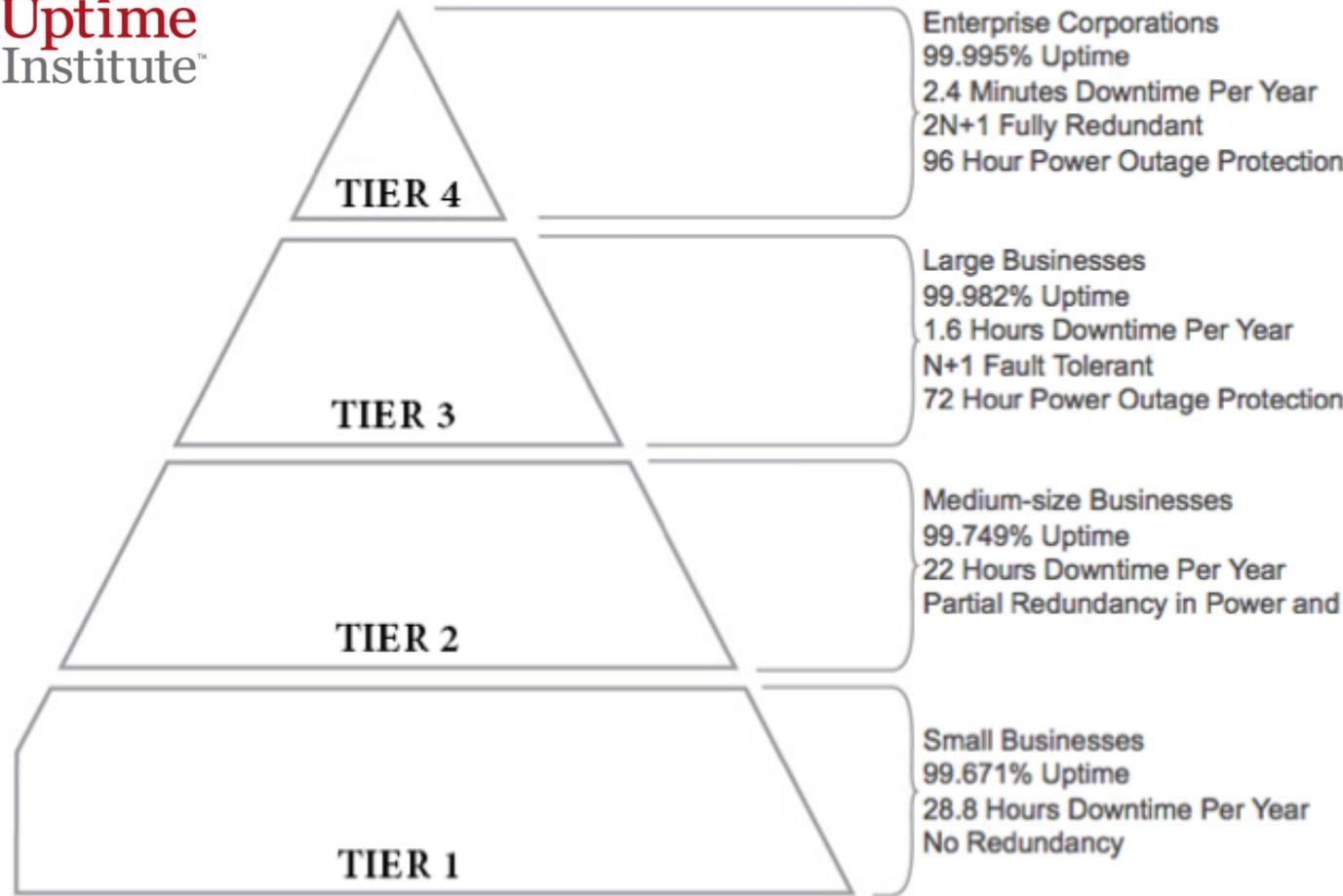


Adapted by Marcus E, Stern H., "Blueprints for high availability"; 2003; Wiley; ISBN: 0471430269;

Availability index

Availability measure is used to evaluate datacenters

Uptime
Institute™



Source: www.datacenters.com

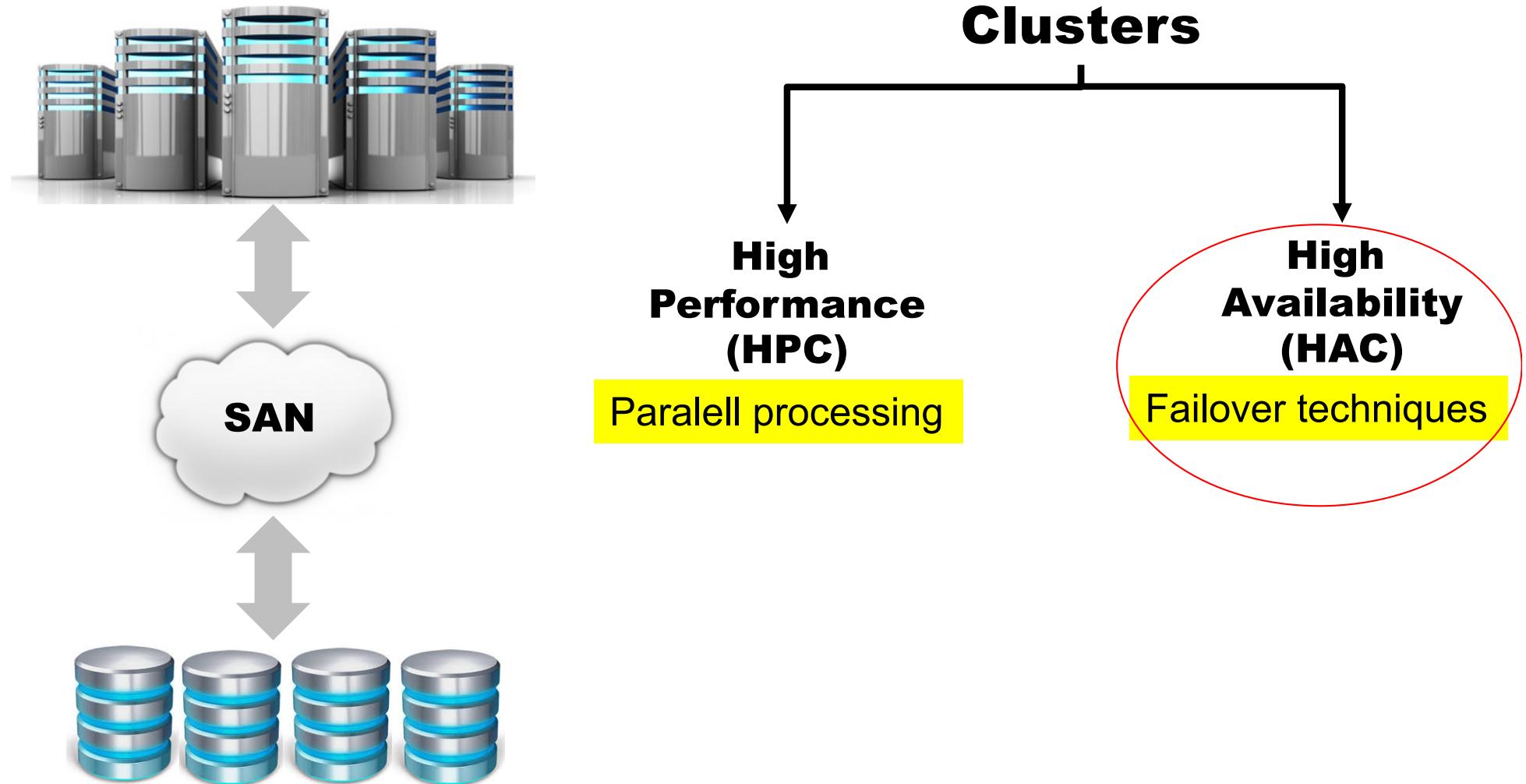
Fault tolerance
and continuous
availability

Continuous
maintenance

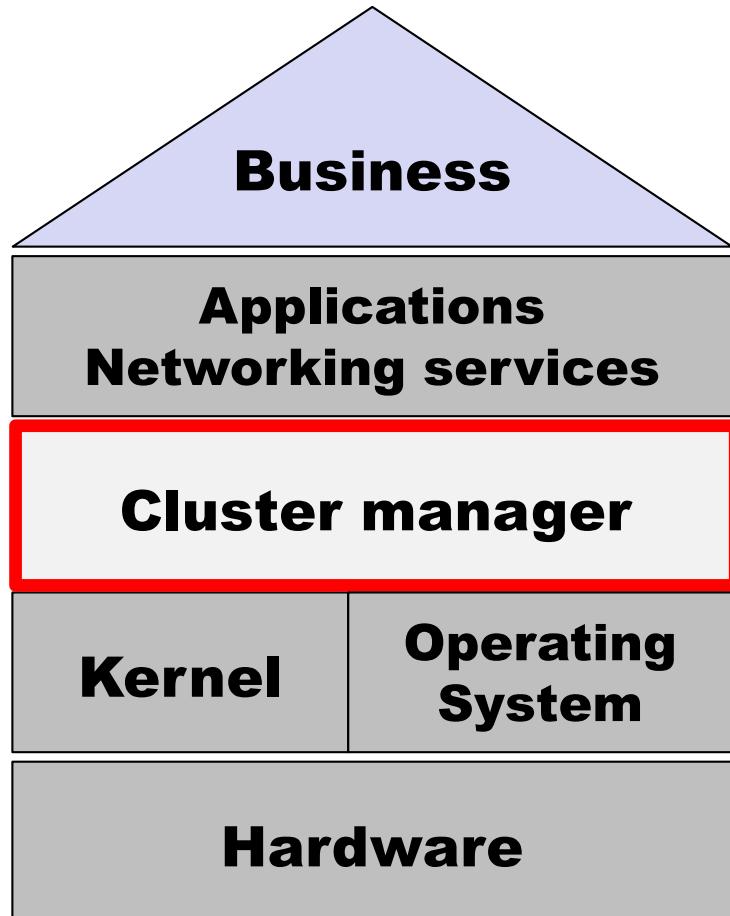
Hardware
redundancy

Basic
facilities

Clustering technologies



Clustering technologies - HA



Cluster managers

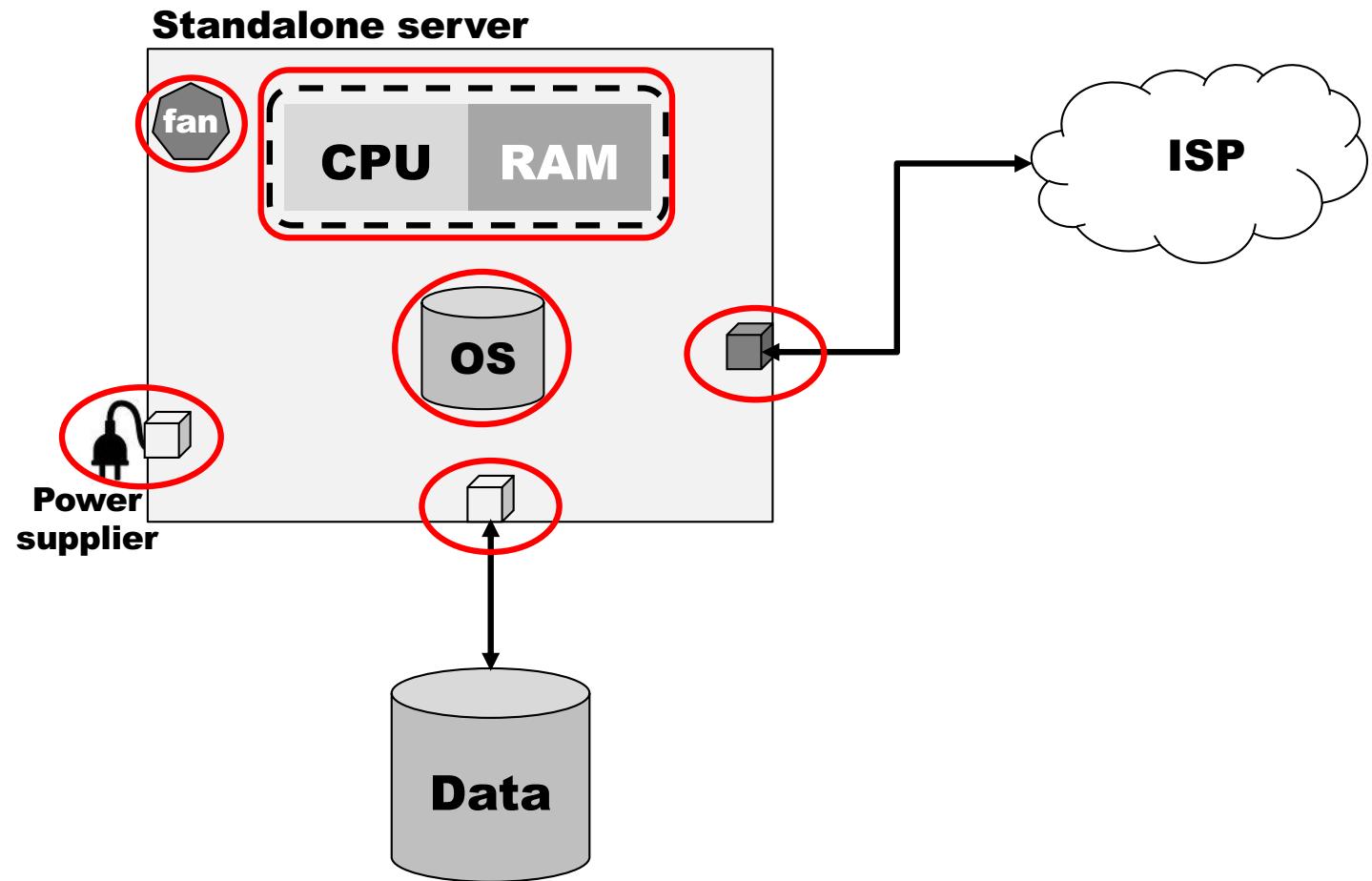
- OS dependent
- Mandatory to be in the market!
- Manufacturers awareness

Opensource cluster managers

- Mainly for Linux OS
- Linux Virtual Server (LVS)
- Heartbeat: www.linux-ha.org

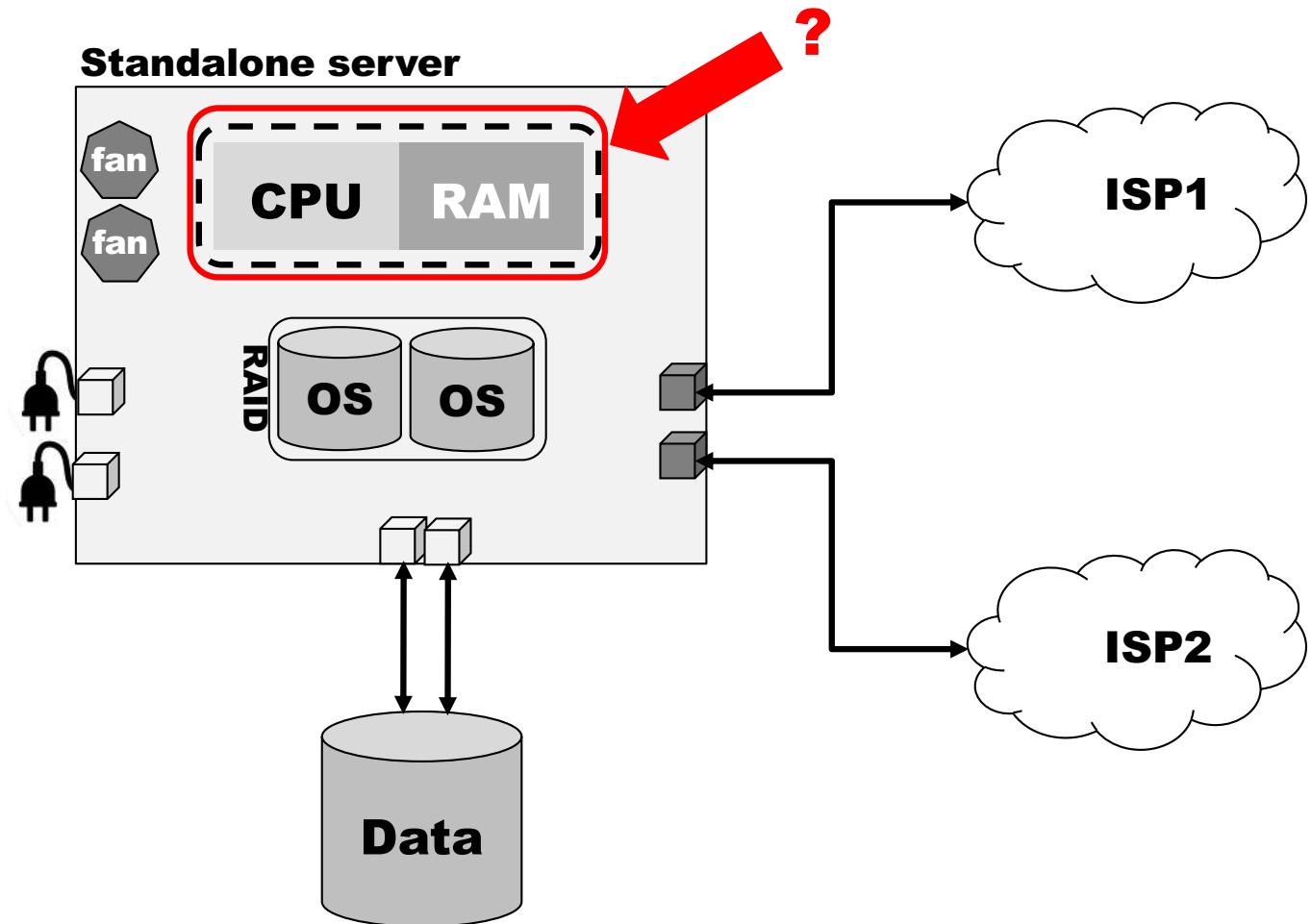
Clustering technologies – HA

Identify Single Points of Failure (SPoF)



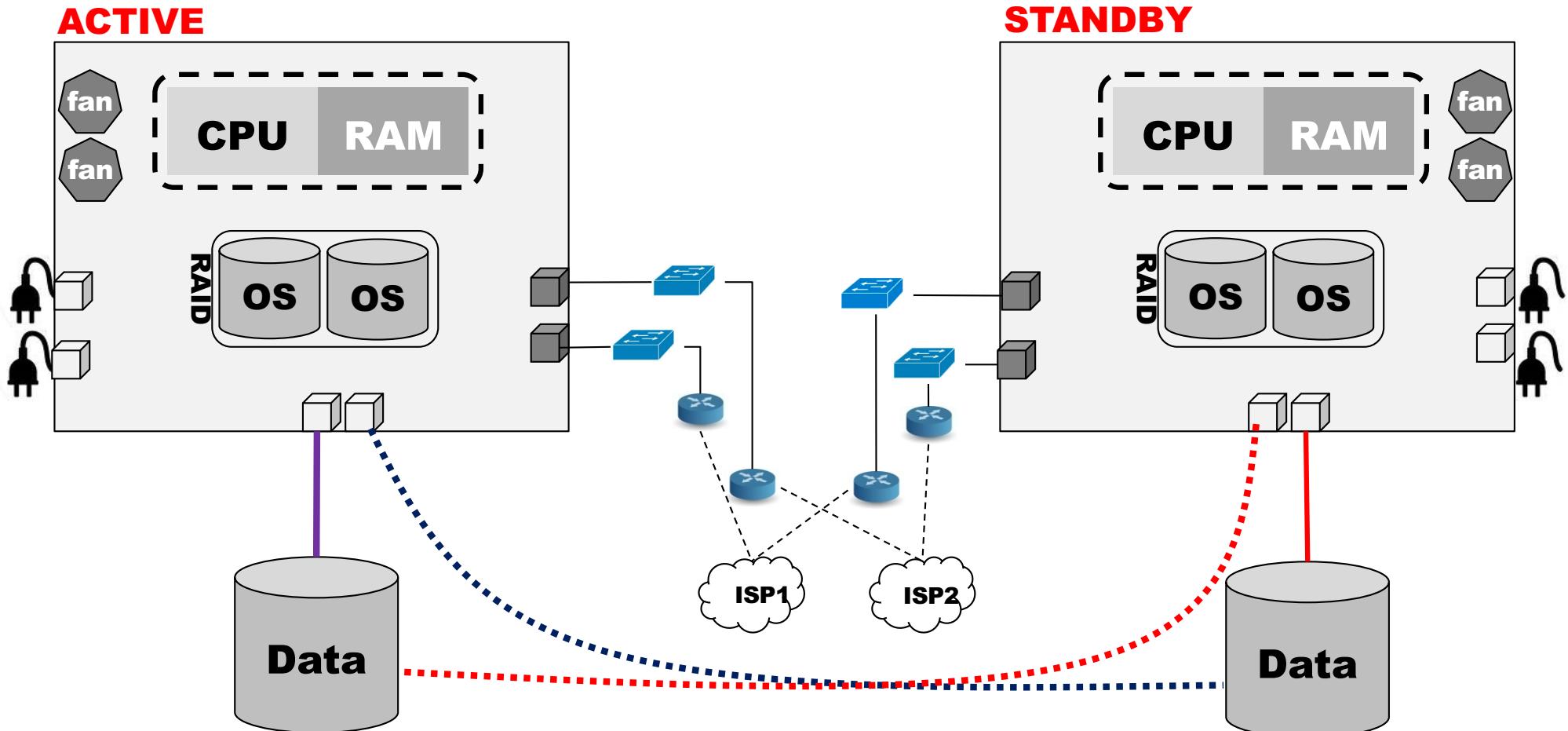
Clustering technologies - HA

Eliminate (mitigate) SPoF (1)



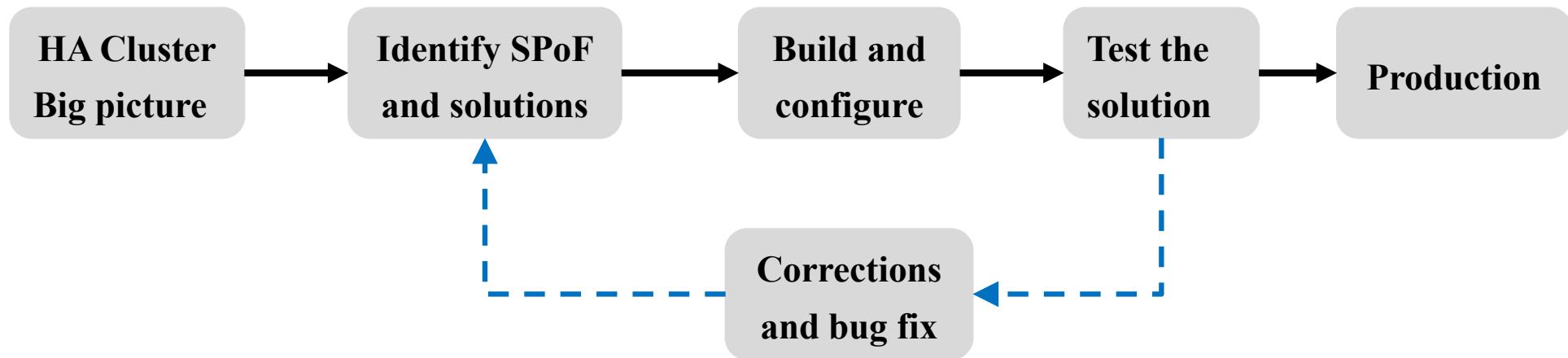
Clustering technologies - HA

Eliminate (mitigate) SPoF (2)



Clustering technologies – HA - planning

General methodology to setup a HA cluster



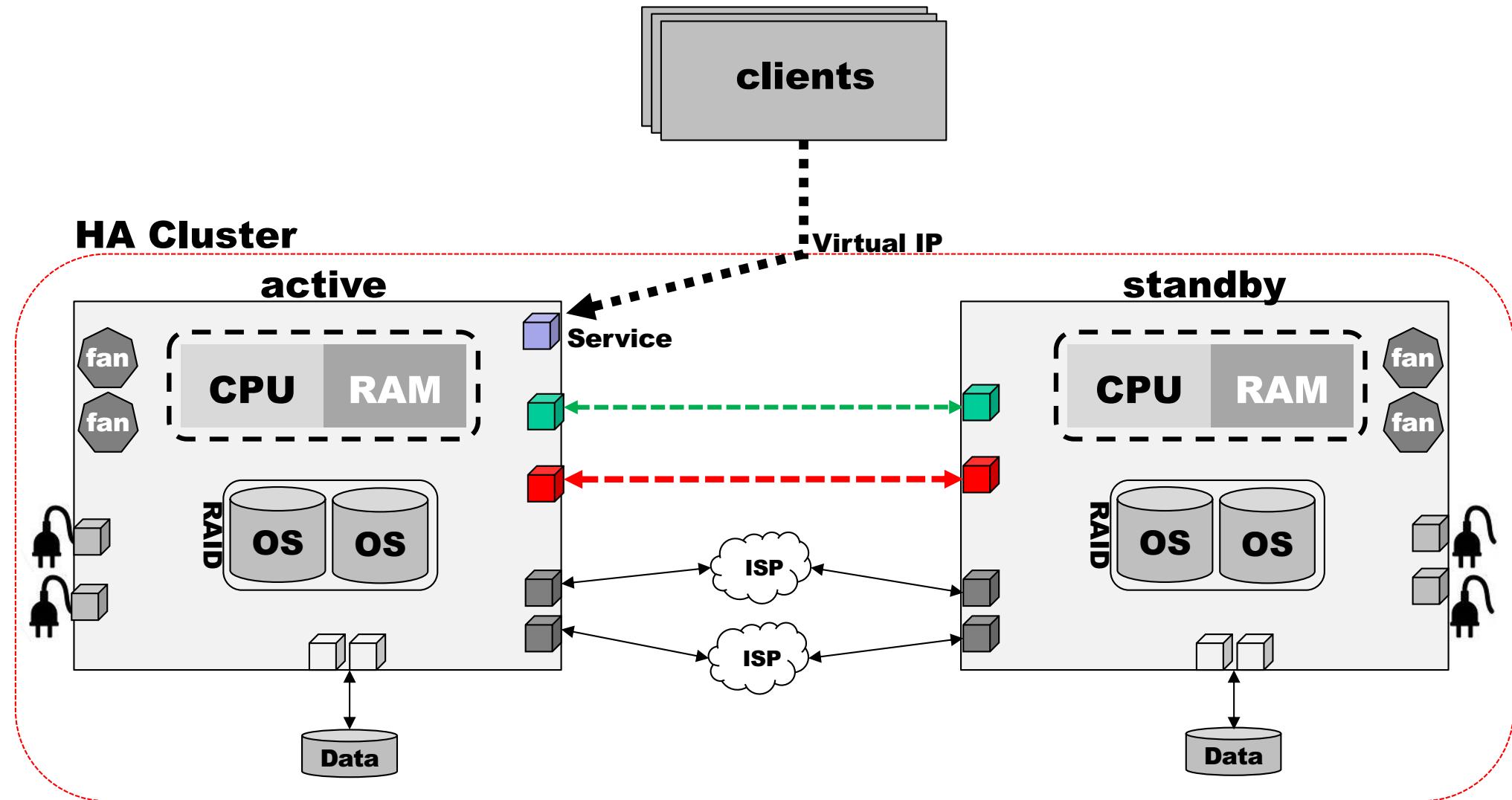
- Planning is crucial
- Level of availability may required mixed solutions
- There is not one solution that fit all problems
- Practice ... practice and more practice!

Clustering technologies - HA

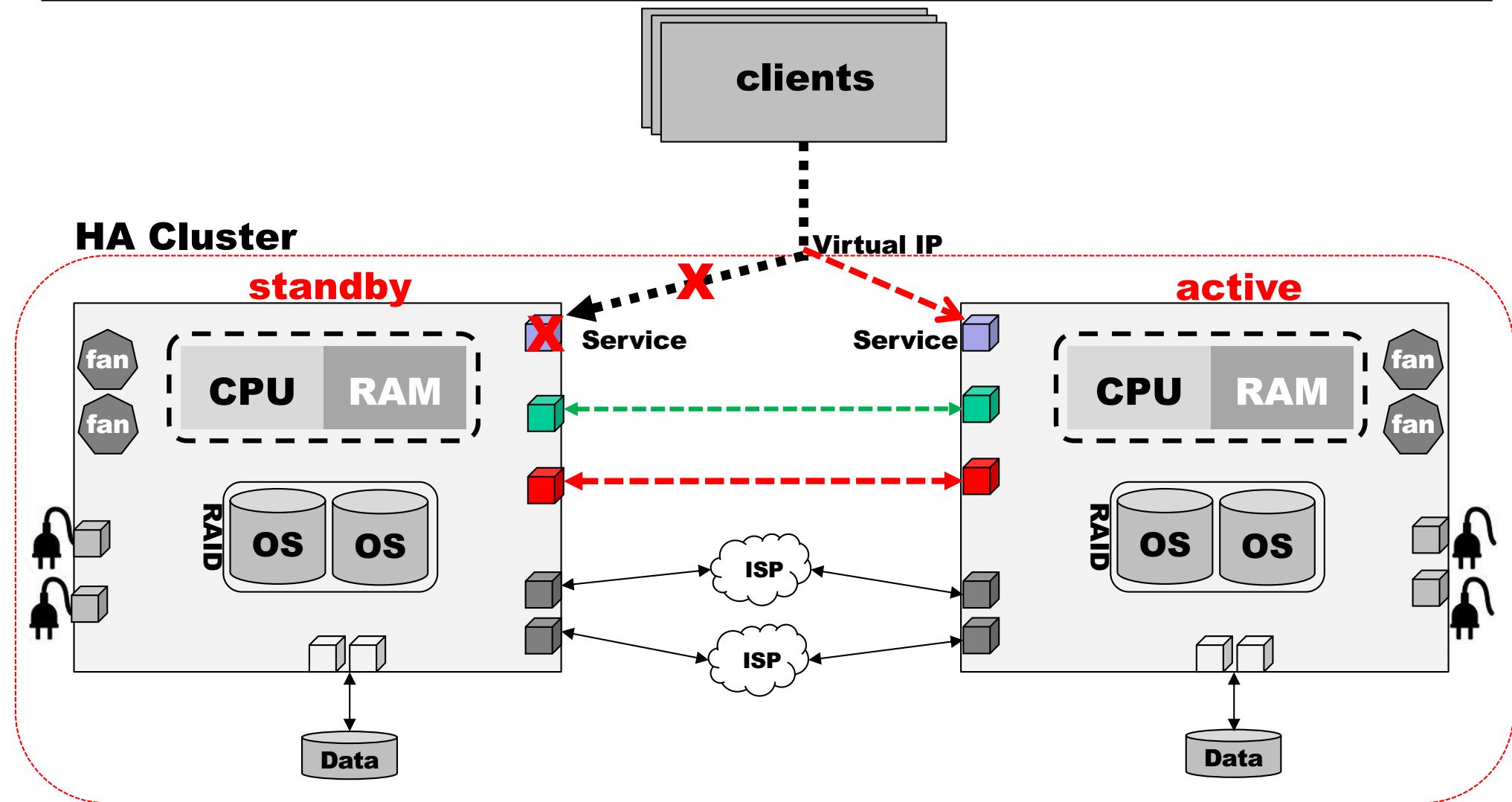
To have in mind:

- Define attainable goals
- Define and test different types of scenarios
- Different strategies: “*Active-Active*” or “*Active-Standby*”
- Network paths should also be replicated: racks, switches, routers, ISP...
- Applications should be “*HA ready!*”
- Organizations should be “*HA aware*”

Cluster Resource Manager

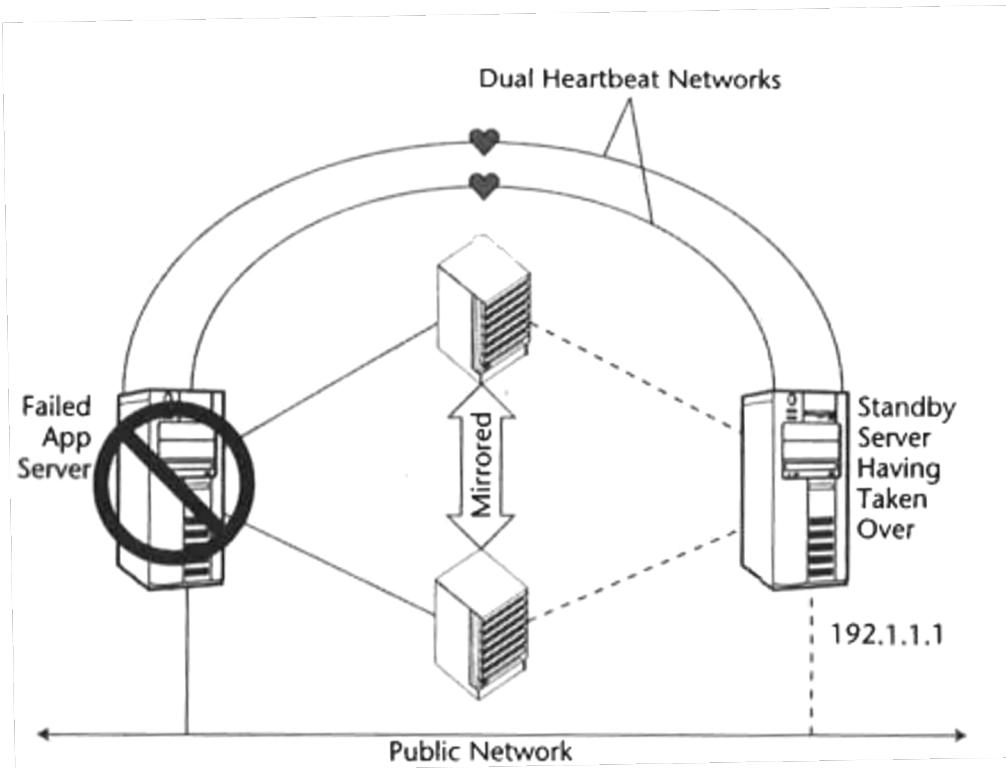


Cluster Resource Manager



Cluster Resource Manager

“Active-Passive” configuration



- A standby node
- Automatic recover after failure
- heartbeat between two nodes

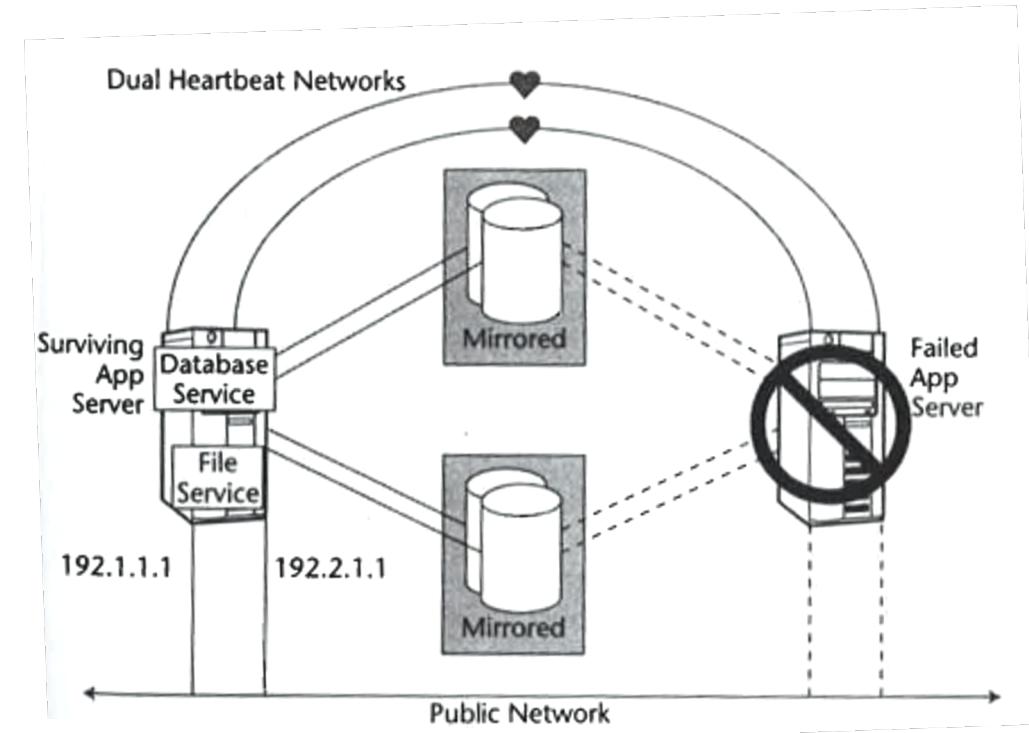
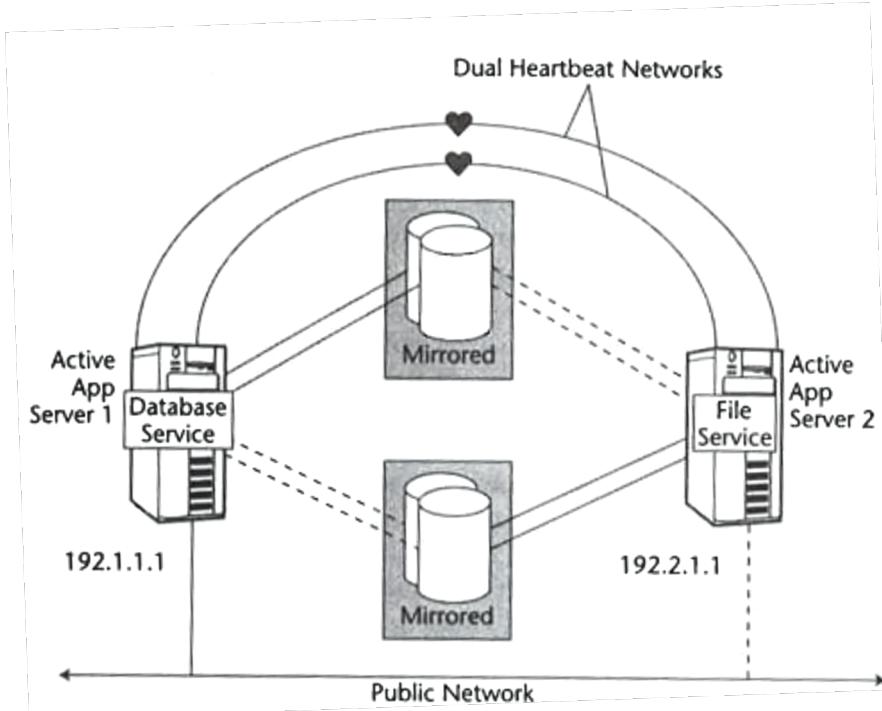
How to use standby nodes:

- ✓ software development
- ✓ Other applications
- ✓ QA and/or test system
- ✓ Solely standby node

Marcus E, Stern H., "Blueprints for high availability"; 2003; Wiley;
ISBN: 0471430269;

Cluster Resource Manager

“Active-Active” configuration



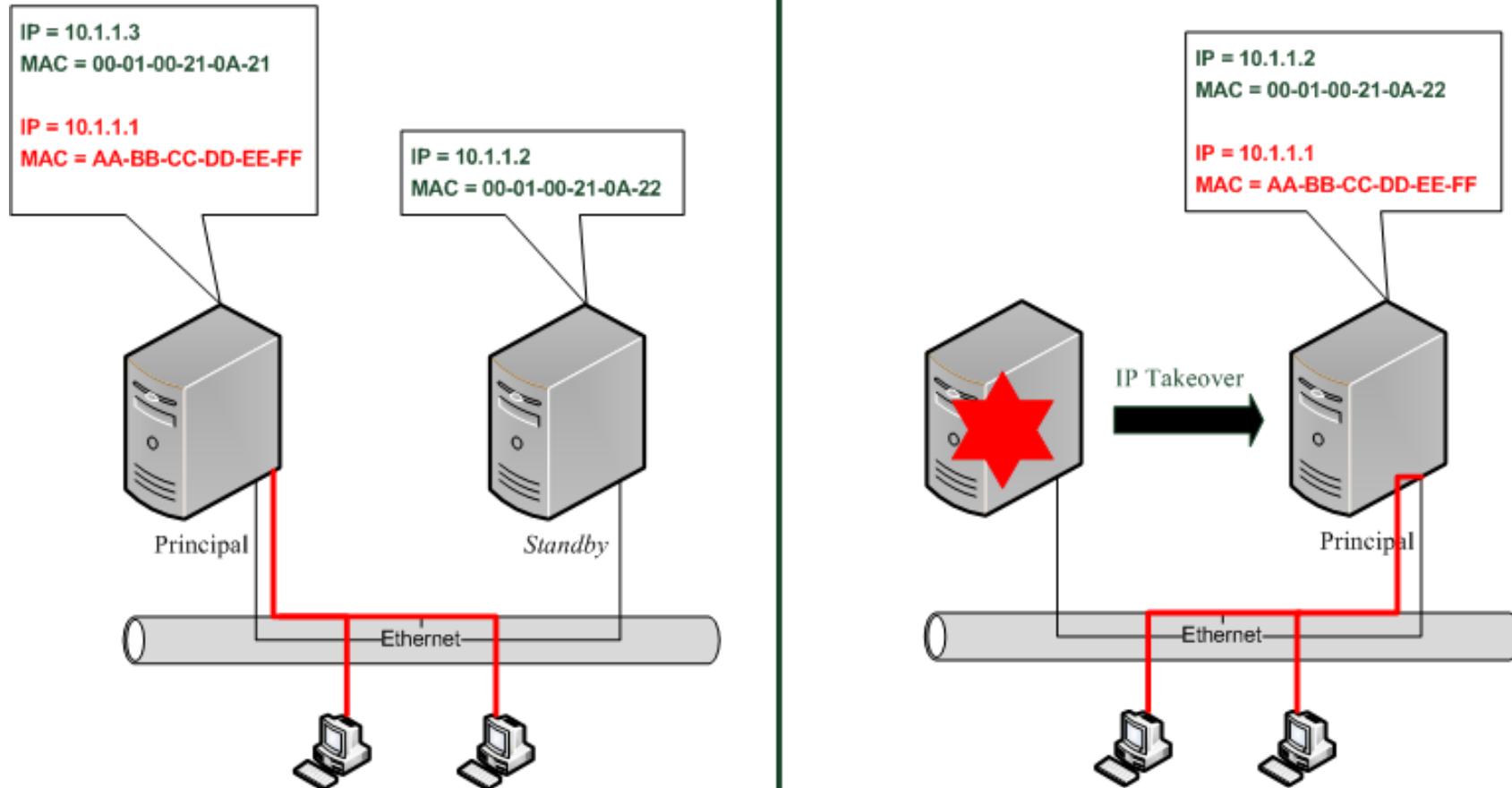
Better use of hardware

Marcus E, Stern H., “Blueprints for high availability”; 2003; Wiley;
ISBN: 0471430269;

Well tested and independent applications
Low performance after takeover
Management is more complex

Cluster Resource Manager

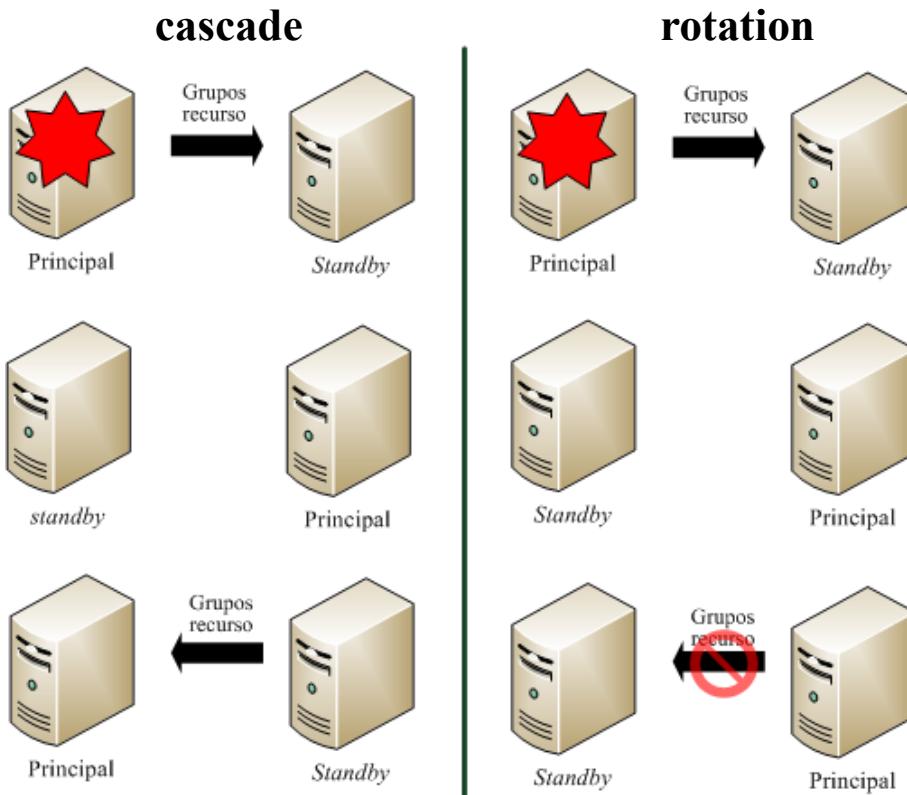
Address takeover



In "Gestão de Projetos TI e administração centralizada de sistemas e redes – cenários práticos em contexto empresarial";
Mário Antunes; IPLeiria; 2010

Cluster Resource Manager

Resource groups – takeover strategies

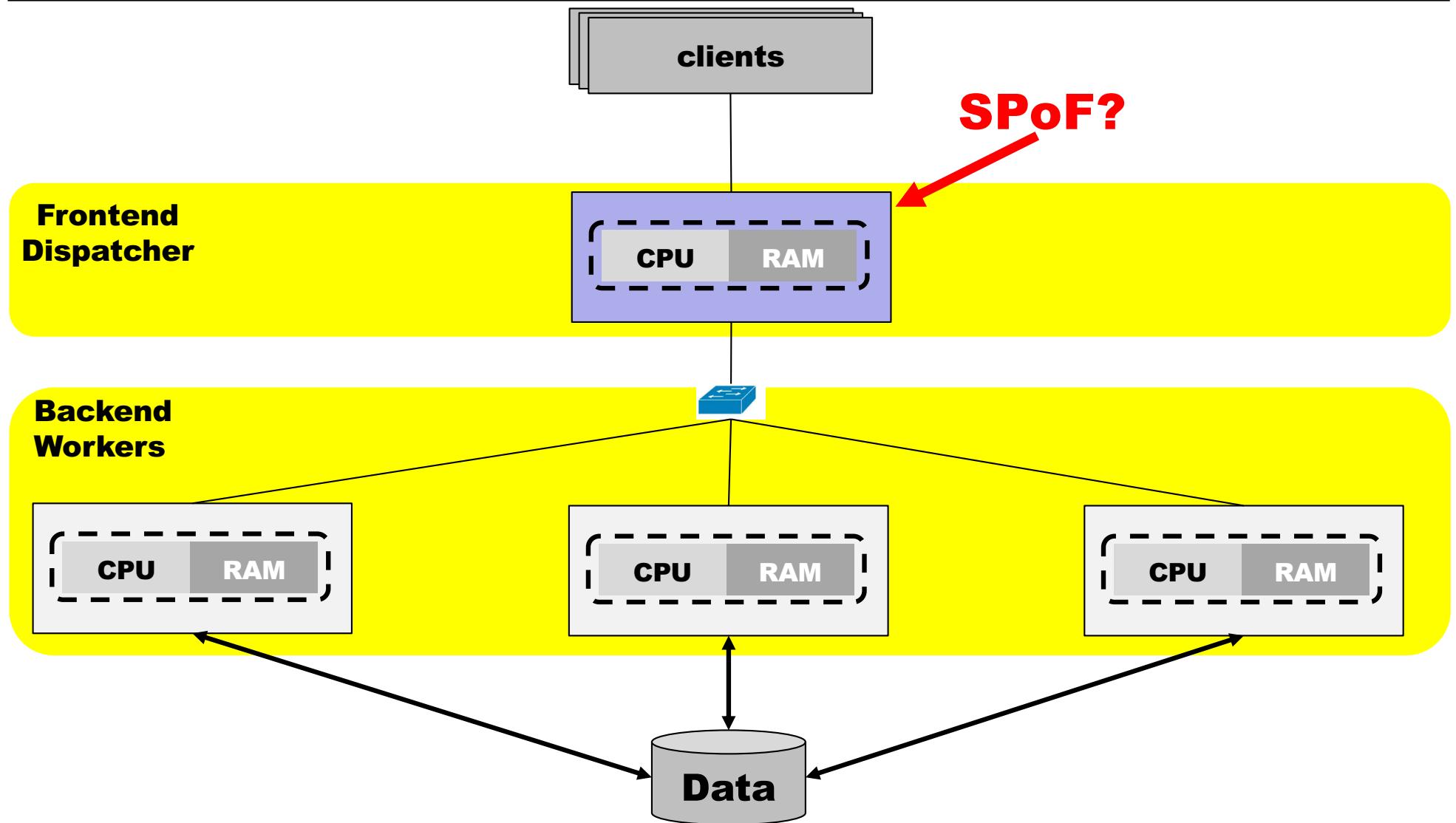


Resource group
critical applications
interfaces

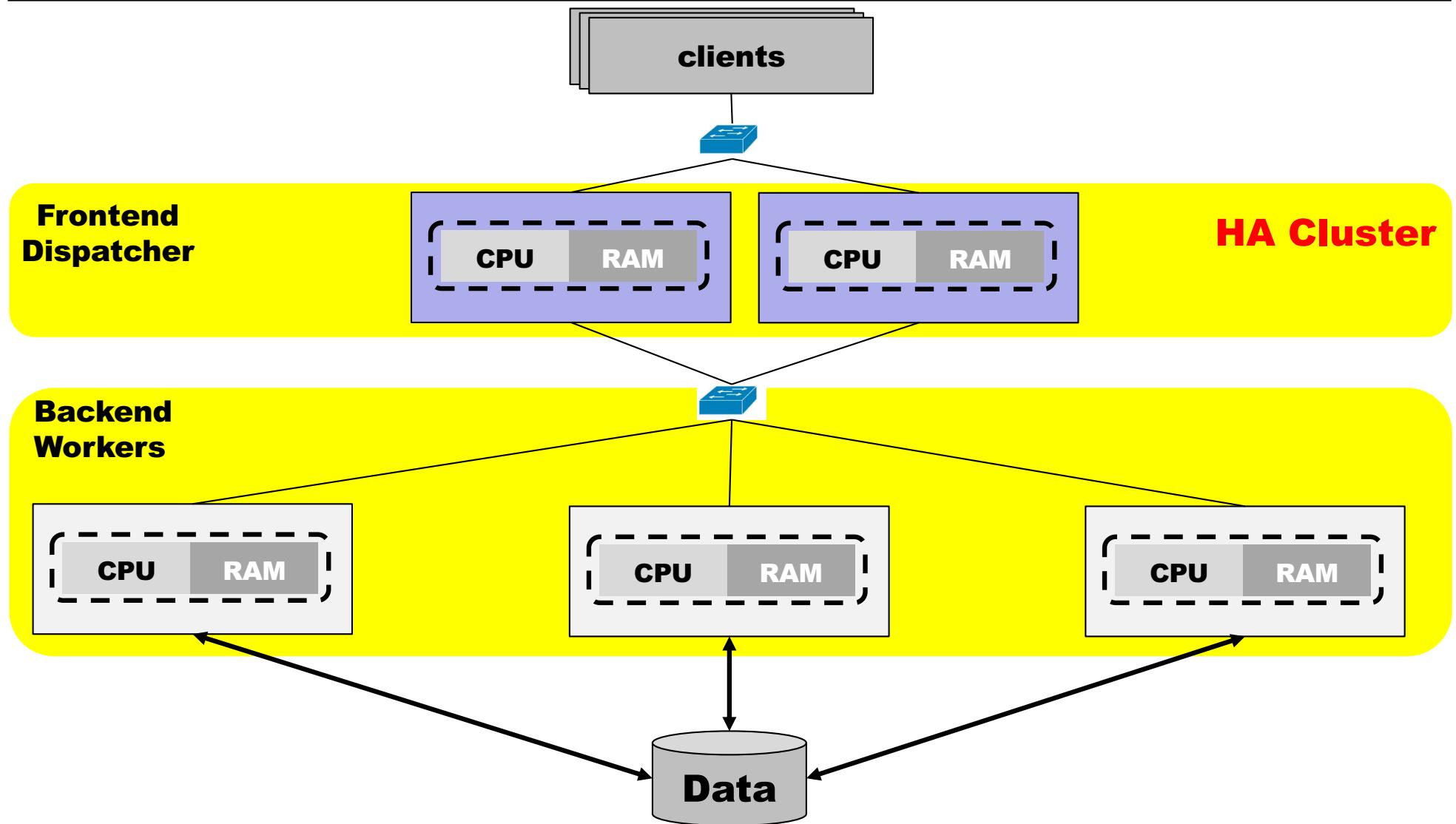
**Which method should
we choose?**

In "Gestão de Projetos TI e administração centralizada de sistemas e redes – cenários práticos em contexto empresarial";
Mário Antunes; IPLeiria; 2010

Cluster Resource Manager - Load balancing



Cluster Resource Manager - Load balancing



Cluster Resource Manager - Challenges

- Geographical distribution of the cluster nodes
- Infrastructure monitoring effectiveness
 - Cluster manager tools
 - Applications monitoring tools
 - Customized monitoring applications
- “*split-brain*” syndrome and how to mitigate it
- How to use backup node during idle period?

Final remarks

- Business are highly IT dependent
- Availability is a *must* and a *continuous challenge*
- Companies and businesses are too aware to HA thinking
- Basic concepts to cover core business and IT demands
- Mixed topologies to cover HA and LB features
- Keyword: **investment** (\$£€).

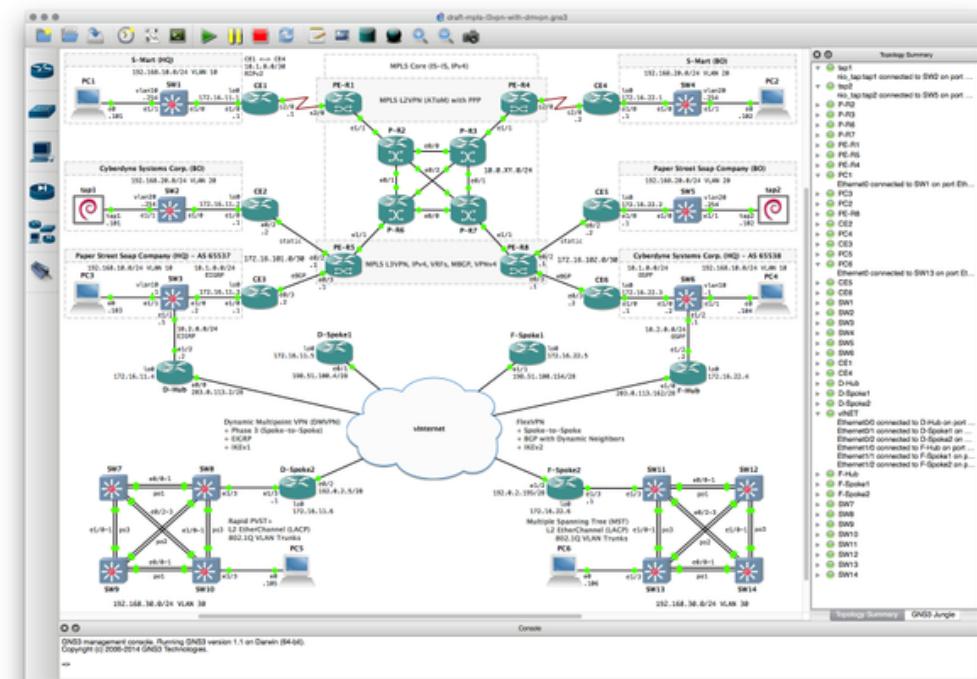
IT professionals should be *HA aware!*

High availability clusters

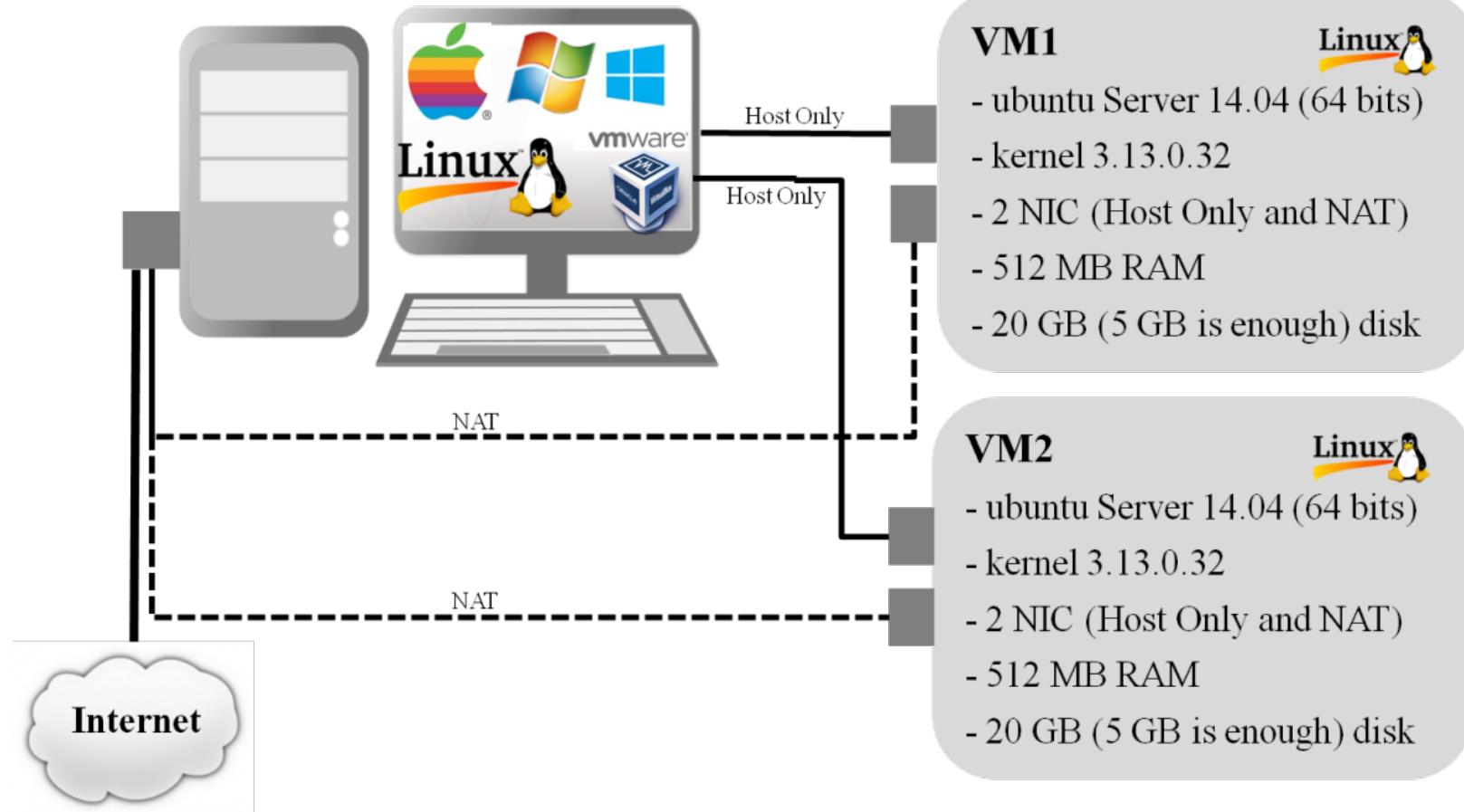
- case study with Heartbeat -

Lab setup – Visualization tool

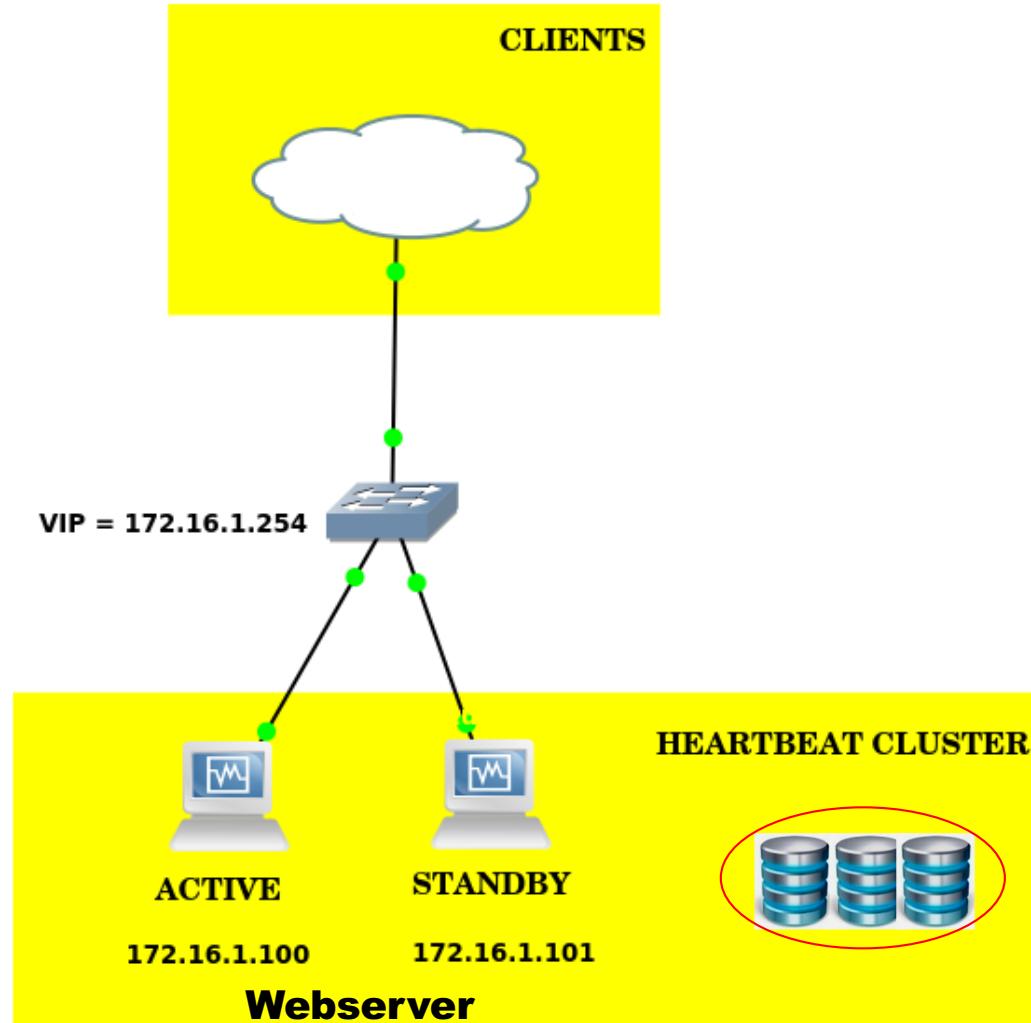
- Virtualization and emulation of network equipments and servers
- Integrates easily with Virtualbox
- Native hypervisor – run dynamips
- Graphical and visualization features
- Opensource and free!



Lab setup – Visualization tool



Lab setup - heartbeat



Network setup

Webserver setup

Heartbeat setup

Logging

Config files (`/etc/ha.d/`)

authkeys

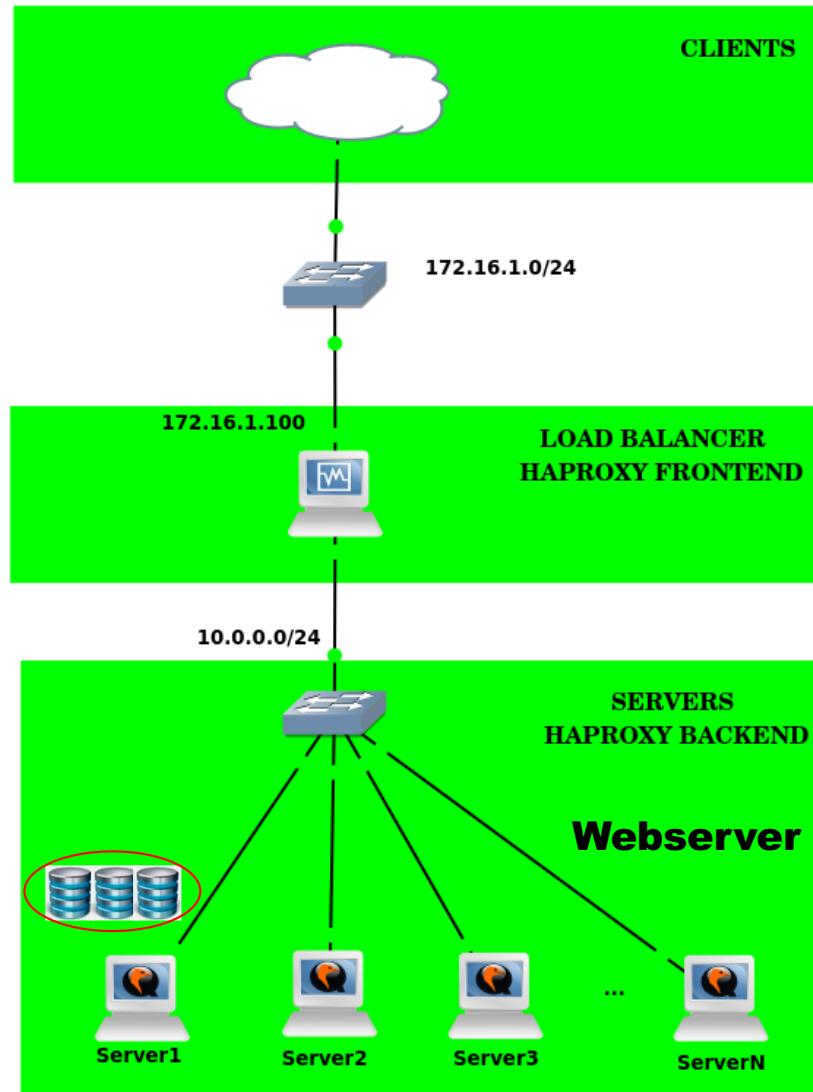
haresources

ha.cf

High availability clusters

- case study with HAProxy -

Lab setup - HAProxy



Web clients

- Browser launches on “host” system

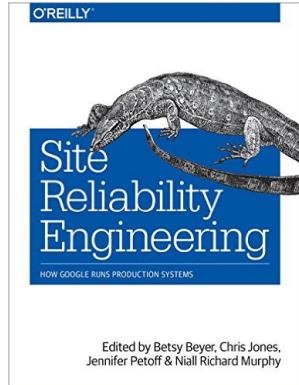
HAProxy Server

- Forward Web requests/replies
- Monitoring and configuration rules
- `/etc/haproxy/haproxy.conf`

Web servers

- Web server configuration rules
- Centralized storage access

Final remarks - bibliography



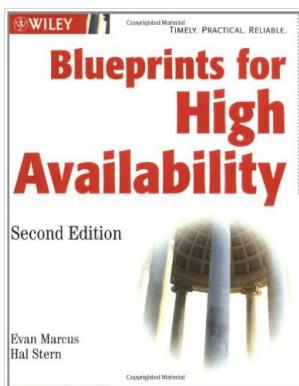
Site Reliability Engineering

Jennifer Petoff, Niall Richard Murphy, Betsy Beyer, Chris Jones
How Google Runs Production Systems
O'Reilly Media; 1 edition (April 16, 2016)
ISBN-13: 978-1491929124

<http://www.wired.com/2016/04/google-ensures-services-almost-never-go/>



<http://www.uptimeinstitute.com>
Reports and research publications



Blueprints for high availability

Marcus E. Stern H.
Wiley; 2003
ISBN: 0471430269

Redundancy

LB and HA in routing protocols

Dedicated HA and LB protocols

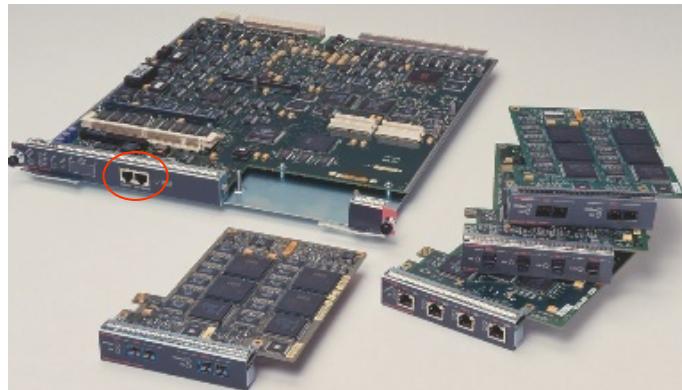
Mário Antunes
mario.antunes@ipleiria.pt

Redundancy

Hardware level



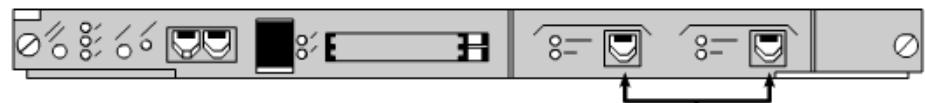
Catalyst 5000,5500, 6000, 6500



Uplinks redundantes

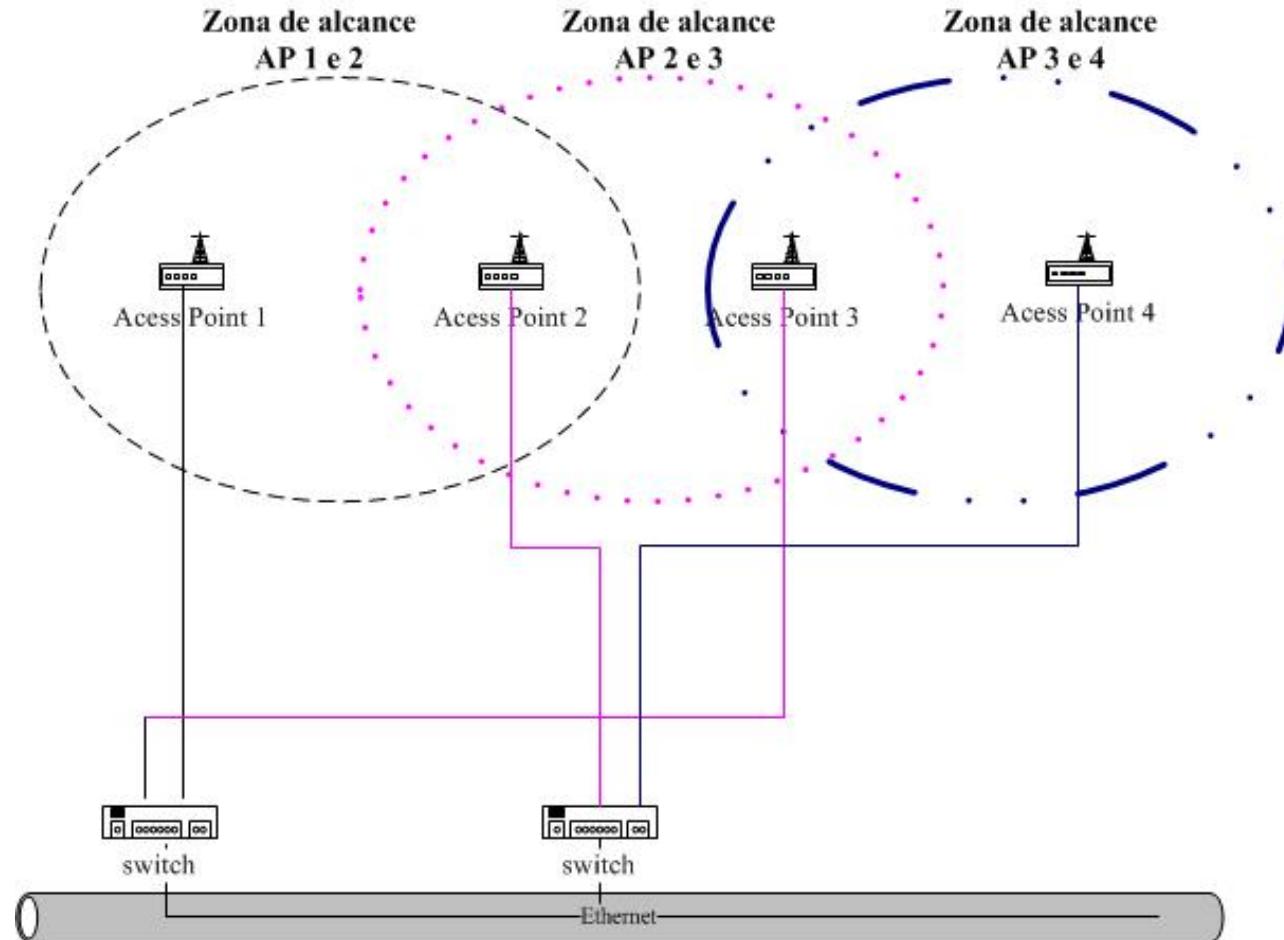


Power Supply



10/100BaseTX Fast EtherChannel
MDIX RJ-45 connections

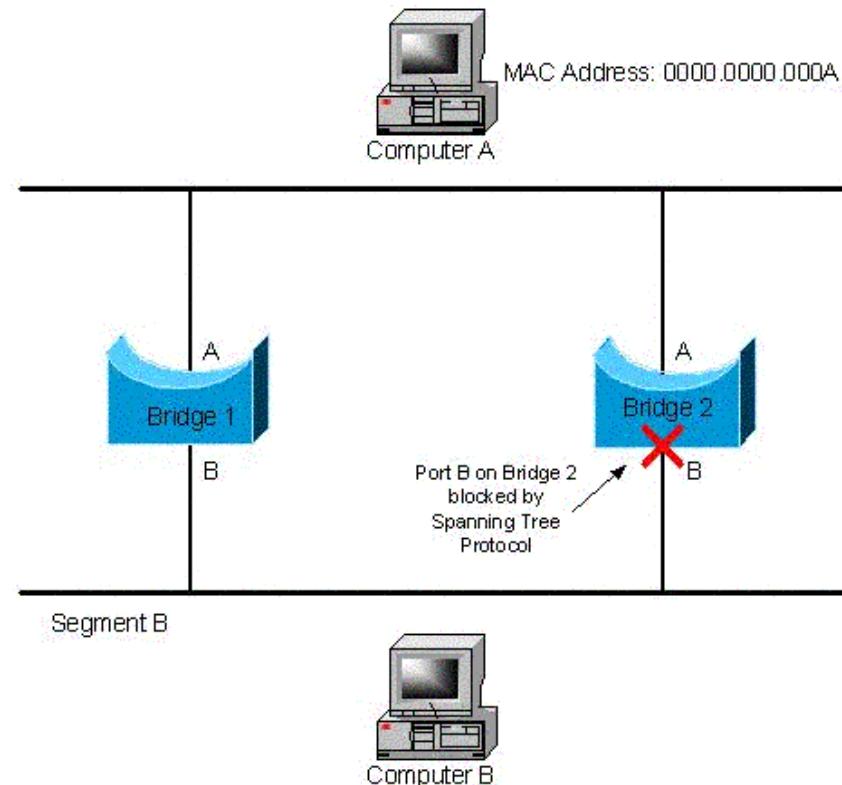
Redundancy - examples



In “Gestão de Projetos TI e administração centralizada de sistemas e redes – cenários práticos em contexto empresarial”,
Mário Antunes; IPLEiria; 2010

Redundancy - examples

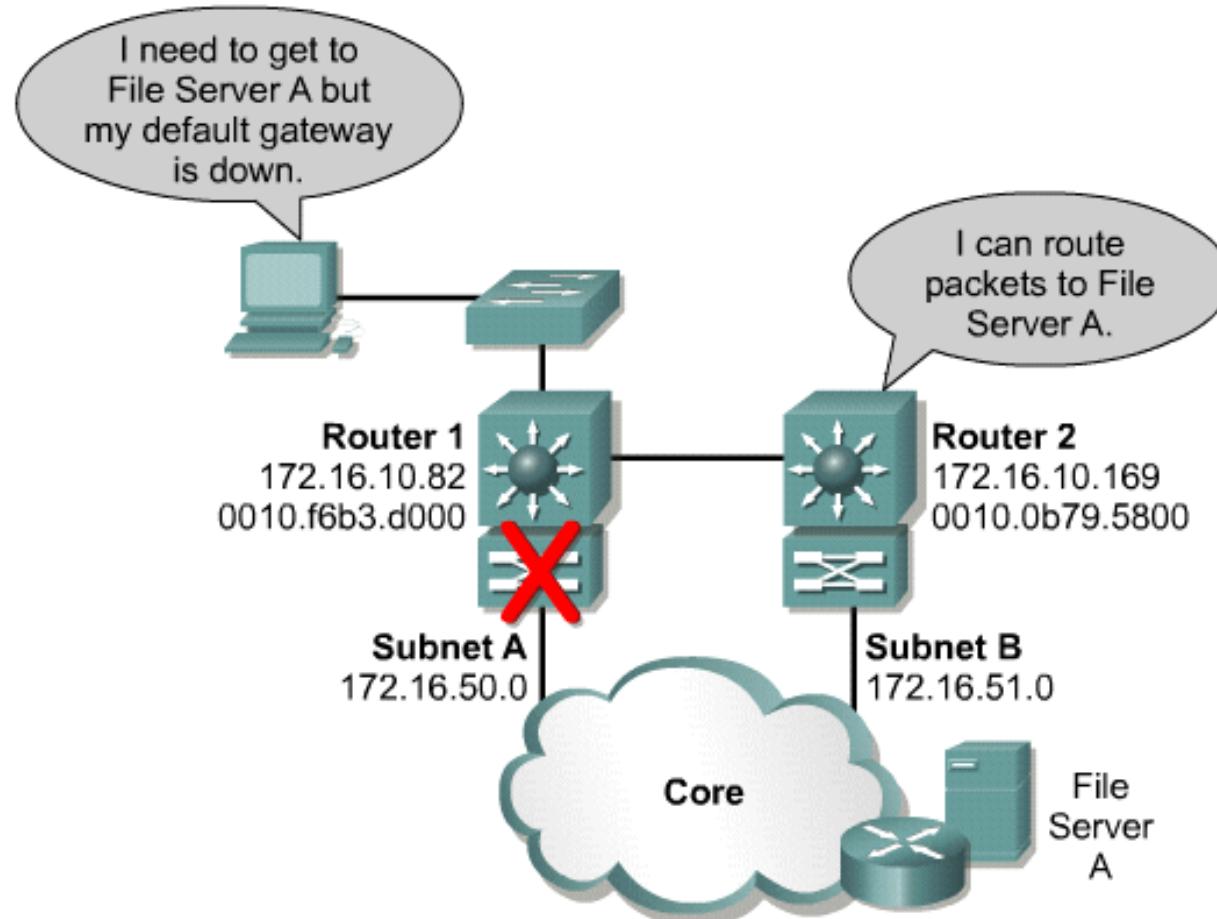
Redundancy L2 – Spanning Tree Protocol (STP)



<http://ipsit.bu.edu>

Case study – L3

The problem:



Case study – L3

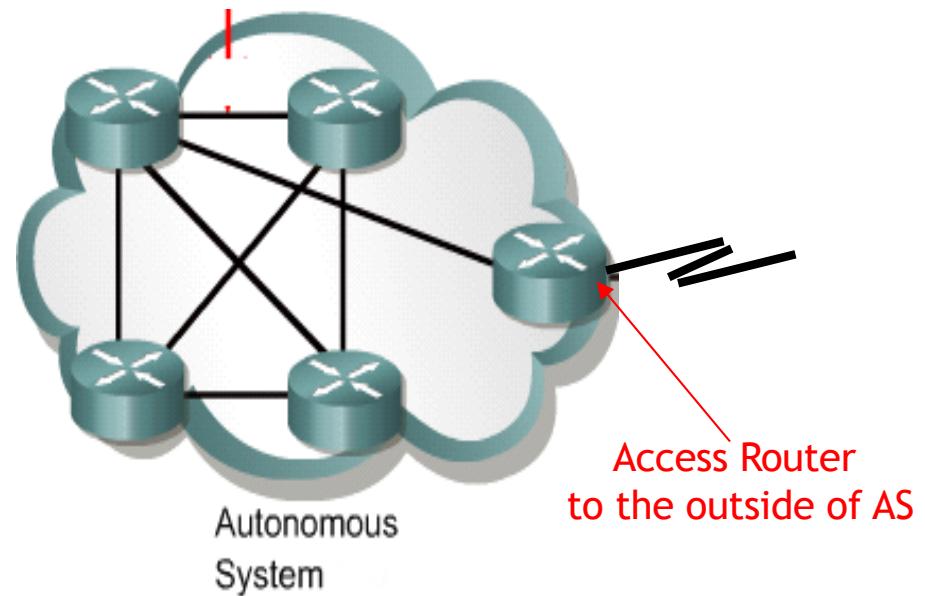
Main topics:

- Dynamic routing
- ICMP Redirect (IR)
- NAT with TCP Load Distribution
- Hot Standby Router Protocol (HSRP)
- Virtual Router Redundancy Protocol (VRRP)
- Gateway Load Balancing Protocol (GLBP)
- Single Router Mode (SRM)
- Server Load Balancing (SLB)

Routing fundamentals

Autonomous System (AS)

- Networks that share the same routing politics
- Usually under the same administrative control
- Identified by a unique identifier (AS Id):
 - 32 bits
 - Assigned by RIR



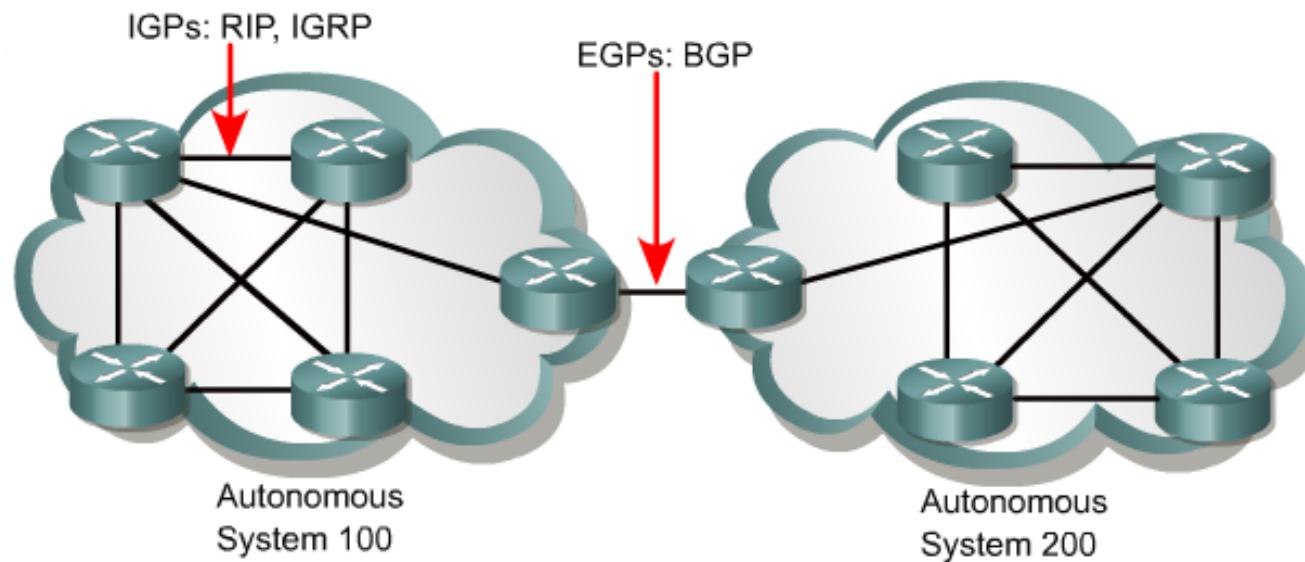
Routing fundamentals

IGP

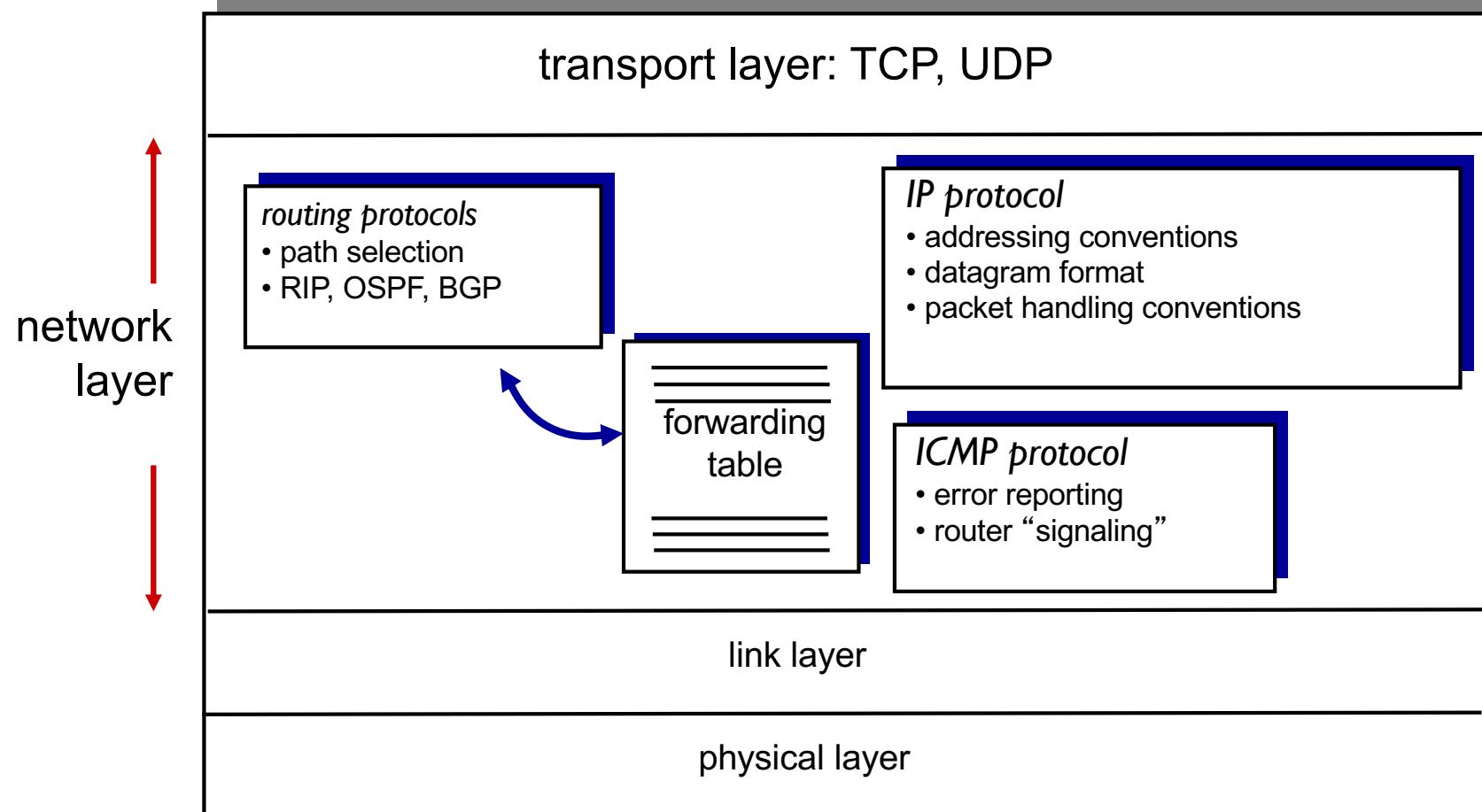
- *Routing inside AS*
- Scalability in the AS
- RIP, IGRP, EIGRP, OSPF

EGP

- *Routing between two AS*
- Hierarchy in large networks
- Management policies
- BGP



Routing fundamentals

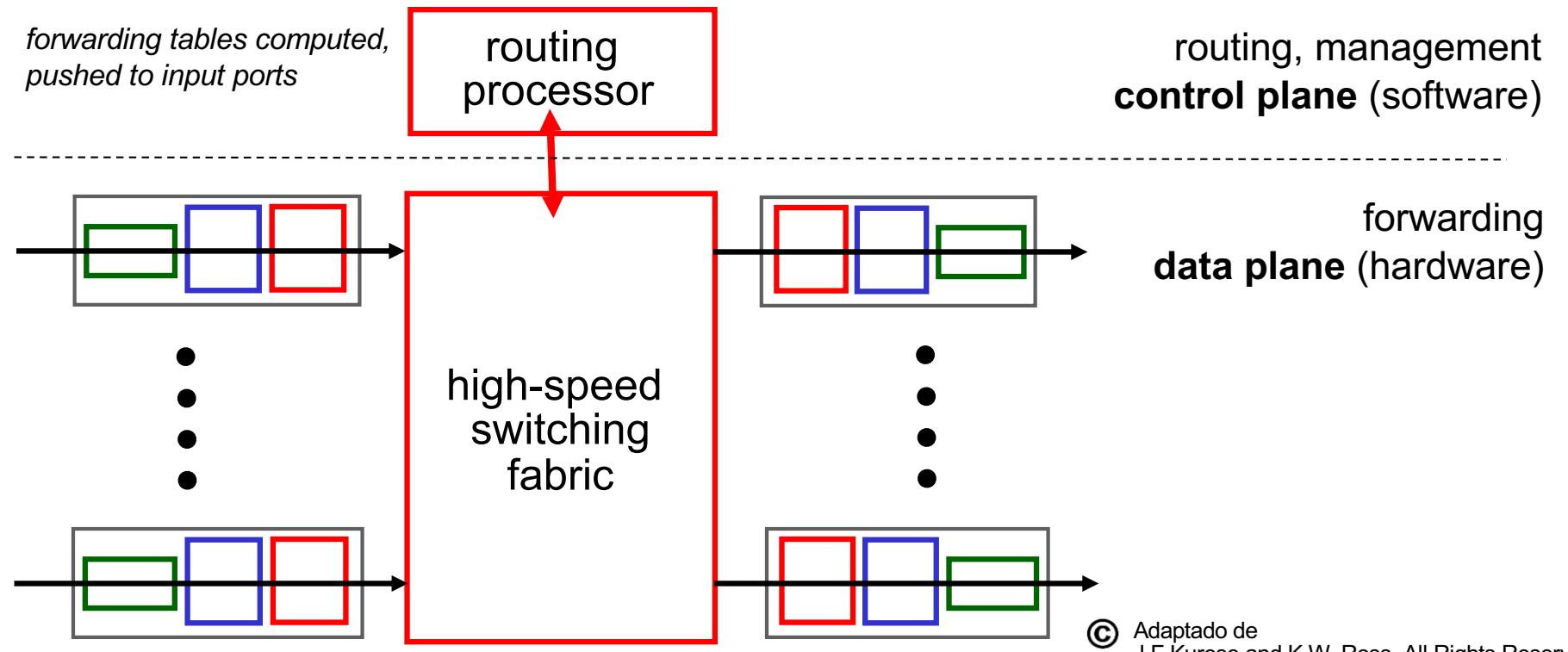


© All material copyright 1996-2012
J.F Kurose and K.W. Ross, All Rights Reserved

Routing fundamentals

Main functions:

- Execute routing algorithms (RIP, OSPF, BGP)
- Route (*forwarding*) packets to the destination IP by an interface



Routing fundamentals

- Non-adaptive (static)
- Adaptive (dynamic)
 - Link State
 - Distance Vector

Routing – RIP protocol

RIP

- Through routes with the **same cost** or alternative routes learned by RIP
- Selective adjust of existing timers: *update, invalid, holddown, flush*
- Load balance by routes with the same cost
- Maximum number of connections:

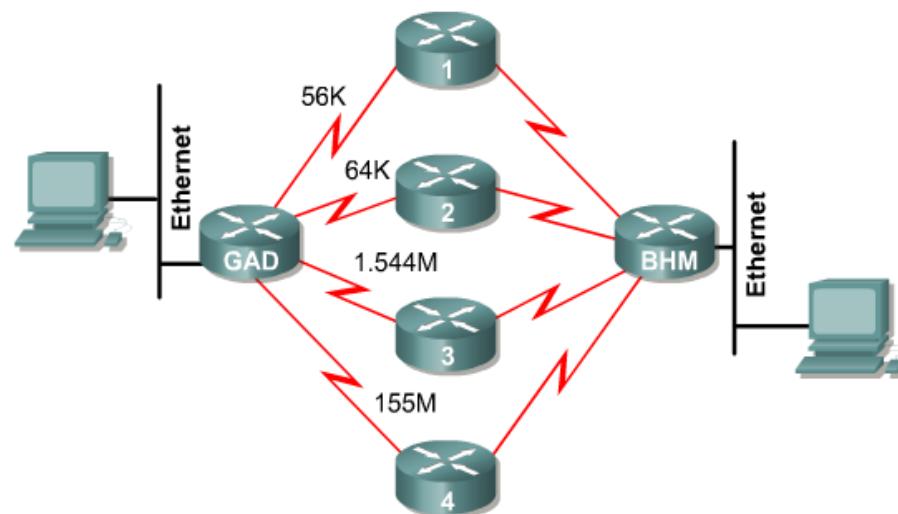
```
R1 (config)#router rip
```

```
R1 (config-router)#maximum-path 2
```

Routing – RIP protocol

Load balancing

- Load balancing between connections with the better equal cost
- RIP uses up to 32 connections (default=4)
(router(config-router) #**maximum-paths N**)
- Method used is “*round-robin*”



```
RouterC#show ip route 192.168.2.0
Routing entry for 192.168.2.0/24
Known via "rip", distance 120, metric 1
Redistributing via rip
Last update from 192.168.4.2 on FastEthernet0/0,
00:00:18 ago
Routing Descriptor Blocks:
192.168.4.1, from 192.168.4.1, 00:02:45 ago, via
FastEthernet0/0
Route metric is 1, traffic share count is 1
* 192.168.4.2, from 192.168.4.2, 00:00:18 ago,
via FastEthernet0/0
Route metric is 1, traffic share count is 1
```

Routing – EIGRP protocol

- Enhanced Interior Gateway Routing Protocol
- Distance vector
- Cisco proprietary
- Periodic updates: 90 seconds
- Main features:
 - Operates well in complex networks
 - Flexibility in networks with links that have distinct characteristics
 - Scalability in large scale networks

Routing – EIGRP protocol

Metric

- Default: BW e DLY
- Composed metric:
 - BW
 - DLY
 - LOAD
 - Fiability
 - MTU

$$\text{Metric} = [K1 * \text{BW} + (K2 * \text{BW}) / (256 - \text{LOAD}) + K3 * \text{DLY}]$$

Se $K5 \neq 0 \rightarrow \text{Metric}^* = [K5 / (\text{RELIABILITY} + K4)]$

Default = **BW + DLY**

```
Router>show ip protocols
Routing Protocol is igrp 300
  Sending updates every 90 seconds, next due in 55
  seconds
  Invalid after 270 seconds, hold down 280, flushed
  after 360
  Outgoing update filter list for all interfaces is
  not set
  Incoming update filter list for all interfaces is
  not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  IGRP maximum hopcount 100
  IGRP maximum metric variance 1
  Redistributing igrp 300
```

“K” parameters (default)

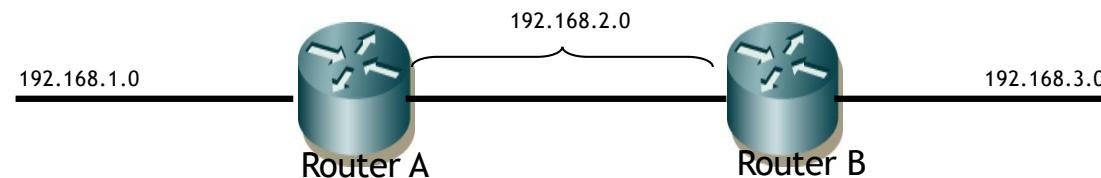
- **K1 = BW = 1**
- **K2 = fiability = 0**
- **K3 = DLY = 1**
- **K4 = LOAD = 0**
- **K5 = MTU = 0**

Routing – EIGRP protocol

Configuration:

EIGRP on AS 101
RouterA(config)#**router igrp 101**
Interfaces RouterA(config-router)#**network 192.168.1.0**
RouterA(config-router)#**network 192.168.2.0**

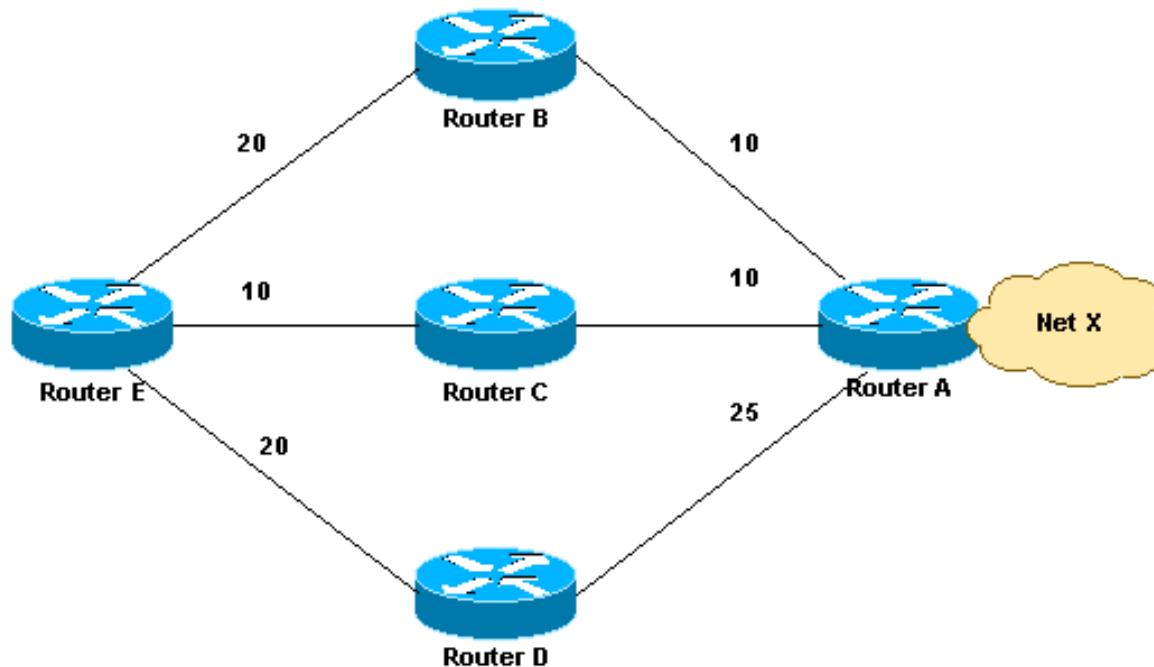
RouterB(config)#**router igrp 101**
RouterB(config-router)#**network 192.168.2.0**
RouterB(config-router)#**network 192.168.3.0**



Routing – EIGRP protocol

Load balance:

- Routes with equal costs (maximum-paths)
- Routes with different costs (variance)



E-B-A → 30
E-C-A → 20
E-D-A → 45

router eigrp 1
network *x.x.x.x*
variance 2

E-B-A → 30
E-C-A → 20

Routing – other protocols

OSPF

- Hierarchy with several areas
- Designated router (DR) and Backup Designated Router (BDR)
- Faster convergence after failure. Routers learn the whole network topology.

BGP

- Hierarchical organization
- Use “route reflectors” and confederations.

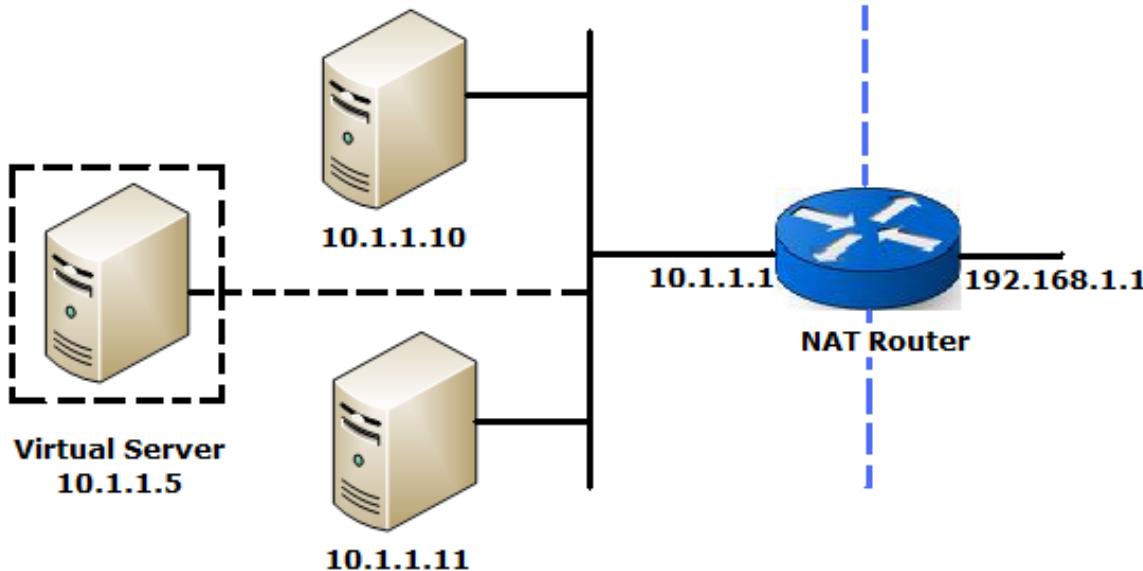
Routing – other protocols

- By default, router caches the routes previously used
- Load balancing → deactivate cache!

```
[no] ip route-cache [same-interface | flow | distributed | cef | policy]  
[no] ip cef
```

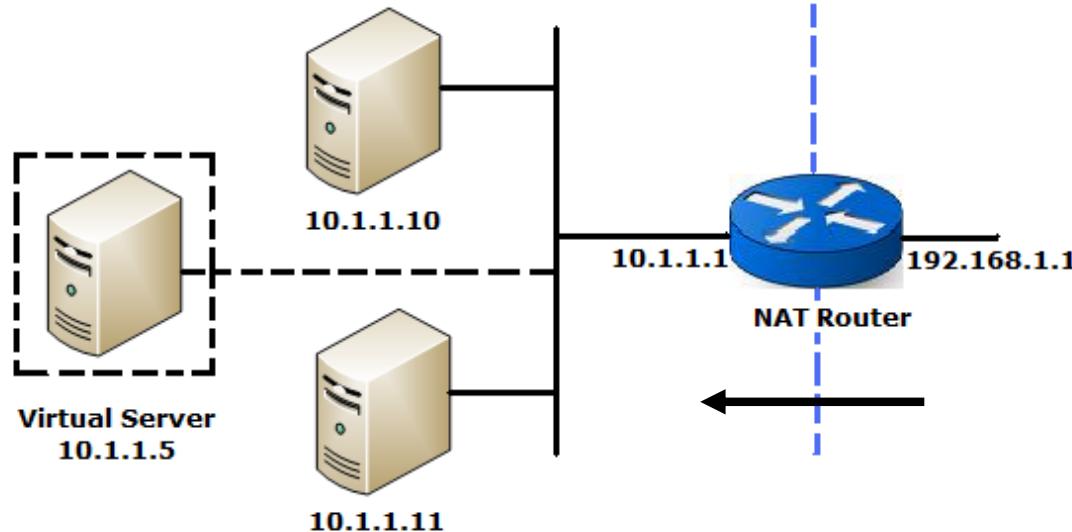
- fast switching
- Load balancing by destination

NAT with TCP Load Balancing



1. External requests are routed alternately between servers (p.e. web, telnet)
2. Assure balanced and rotative balancing between servers.

NAT with TCP Load Balancing



```
ip nat pool teste 10.1.1.10 10.1.1.11 prefix-length 24 type  
    rotary  
ip nat inside destination list ALL_TCP pool teste  
ip alias 10.1.1.5 23  
ip alias 10.1.1.5 80  
!
```

NAT with TCP Load Balancing

```
ip access-list extended ALL_TCP  
permit tcp any host 10.1.1.5 eq telnet  
permit tcp any host 10.1.1.5 eq www
```

```
ip nat inside  
ip nat outside
```

Alternative in Cisco IOS:

To explore Server Load Balancing (SLB) features.

First Hop Redundancy Protocols

- Hot Standby Redundancy Protocol (HSRP)
- Virtual Router Redundancy Protocol (VRRP)
- Global Load Balancing Protocol (GLBP)

Hot Standby Router Protocol (HSRP)



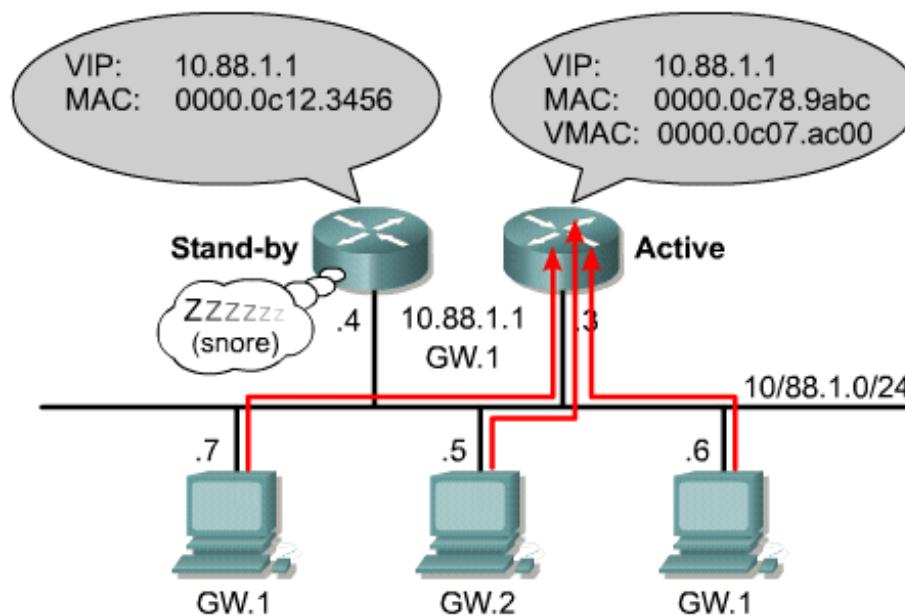
- Packets are redirected automatically to a *standby* router
- Transparently to the end-user
- Functioning:
 - A routers set share a MAC and IP addresses (Virtual Router)
 - One *router* is elected as active
 - Routers exchange control messages of HSRP state
 - ARP assignes MAC to the MAC Virtual
 - If active *router* fails, standby router functions as active router.

Hot Standby Router Protocol (HSRP)

HSRP Operation

FIGURE

1
2
3
4



All contents copyright © 2003 Cisco Systems, Inc. All rights reserved.

Hot Standby Router Protocol (HSRP)

Designating an Active Router

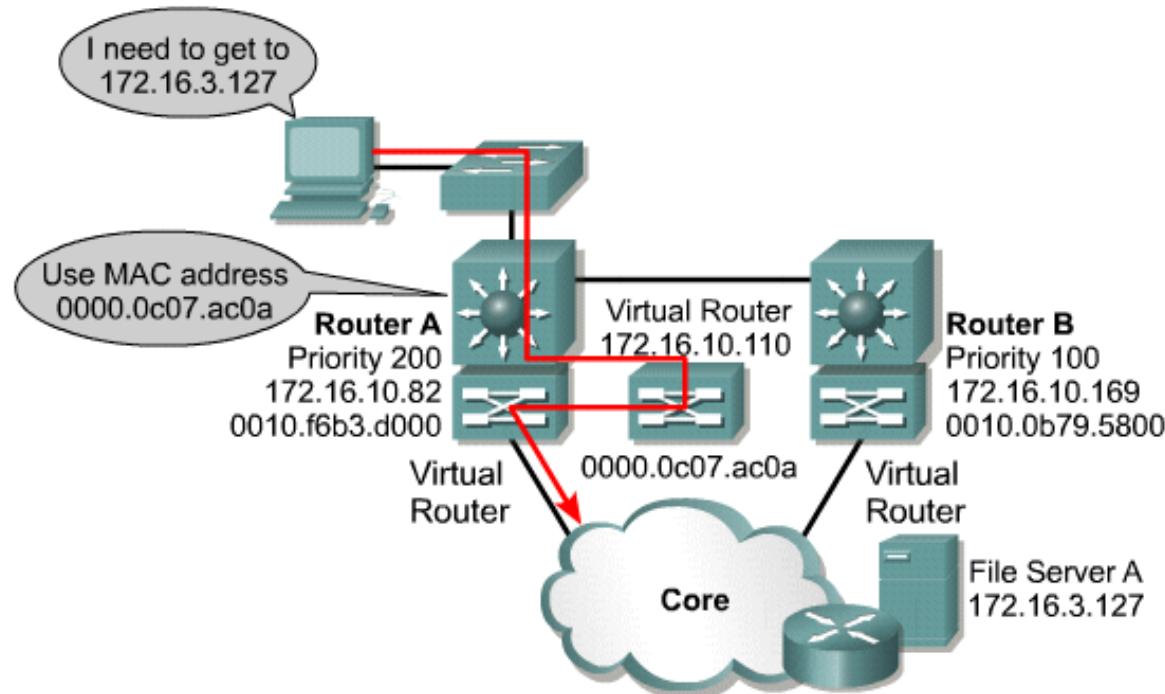
FIGURES

1

2

3

4



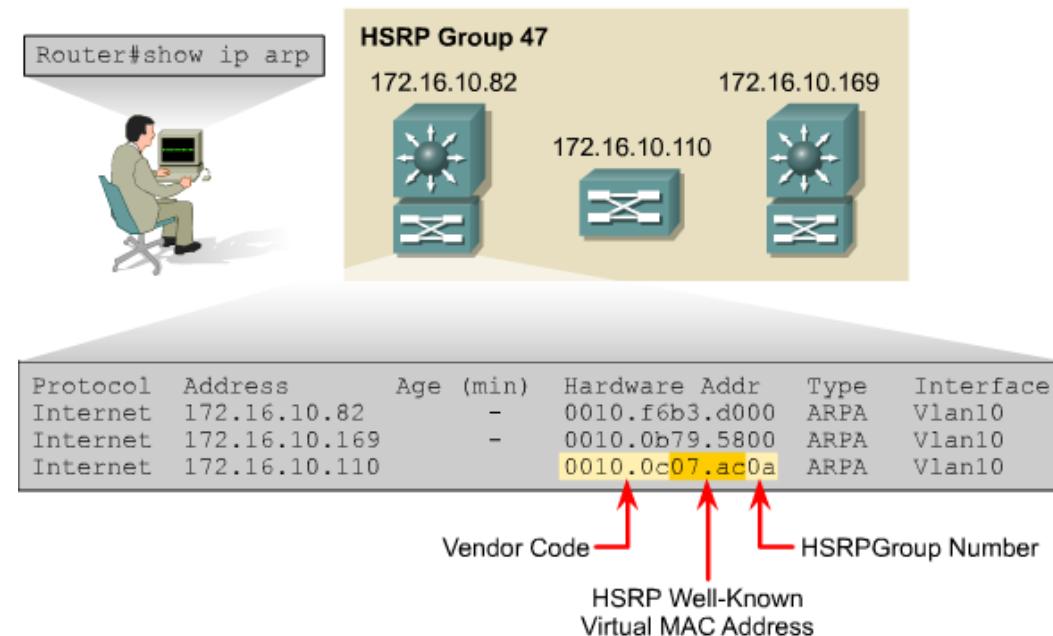
The router with the highest HSRP priority becomes the active router. The active router responds to ARP requests with the MAC address of the virtual router.

All contents copyright © 2003 Cisco Systems, Inc. All rights reserved.

Hot Standby Router Protocol (HSRP)

Virtual MAC address used at HSRP:

- Vendor ID – MAC address (24 bits)
- HSRP Code – 16 bits (“07.ac”)
- Group ID – last 8 bits of MAC endereço



Hot Standby Router Protocol (HSRP)

HSRP messages

1 Octet	1 Octet	1 Octet	1 Octet
Version	Op Code	State	HelloTime
Holdtime	Priority	Group	Reserved
Authentication Data			
Authentication Data			
Virtual IP Address			

Eleição de routers activo e standby

Initial
Stanby
Active

0 – Hello
1 – Coup
2 – Resign

[0 ... 255]

Intervalo de Hello

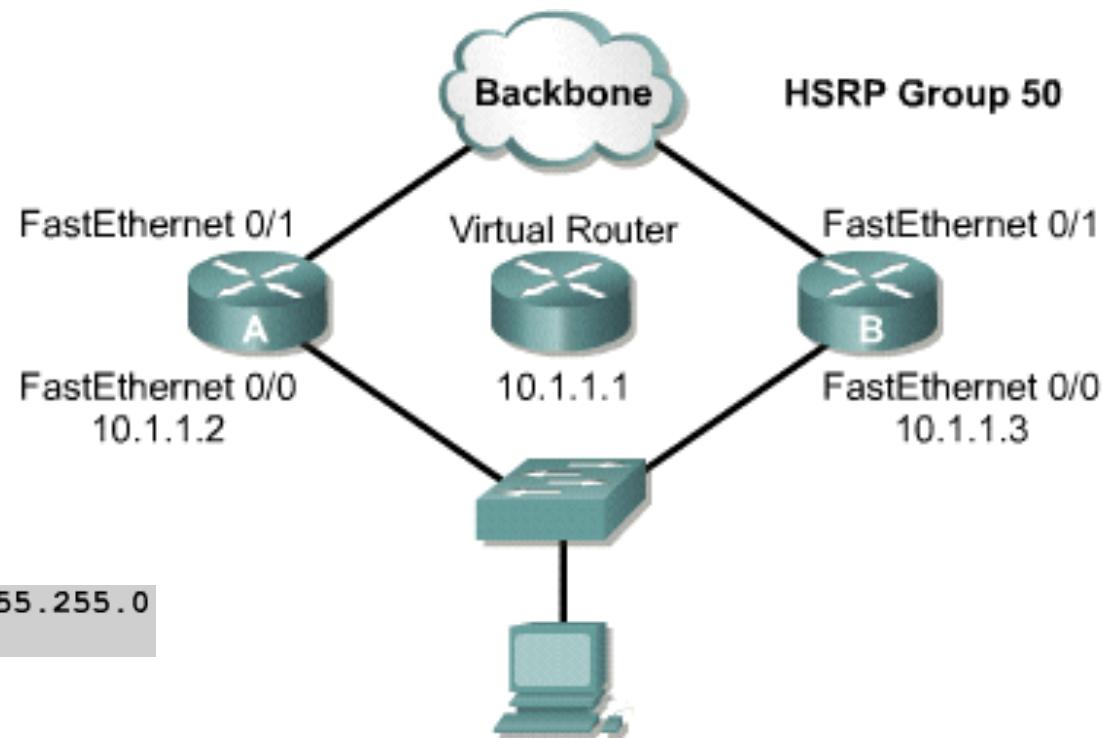
Transport protocol: UDP
Port: 1985
Destination IP : endereço 224.0.0.2
TTL = 1

Possible states:

- Initial, Learn, Listen, Speak, Stanby, Active

Hot Standby Router Protocol (HSRP)

Configuration



Router A

```
A(config-if)#ip address 10.1.1.2 255.255.255.0
A(config-if)#standby 50 ip 10.1.1.1

A(config-if)#standby 50 priority 150

A(config-if)#standby 50 preempt

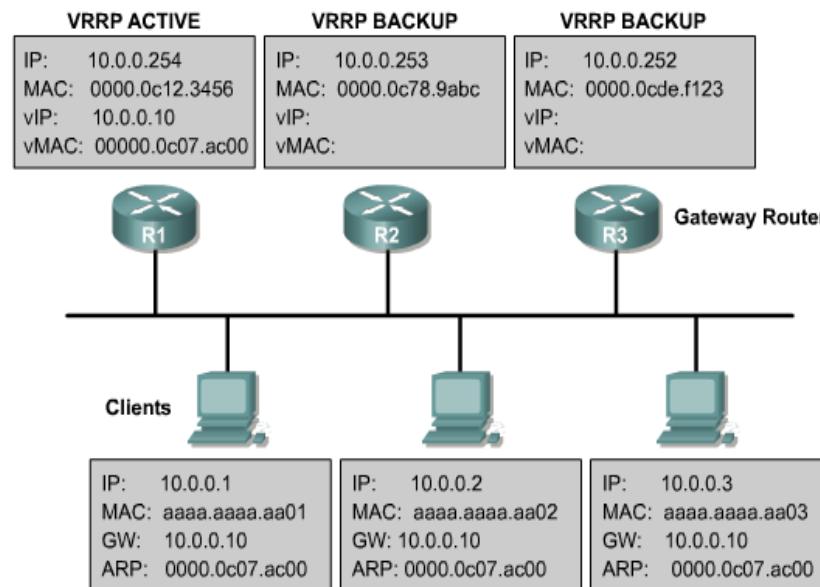
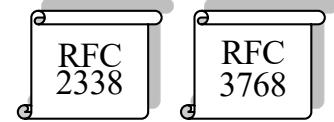
A(config-if)#standby 50 timers 5 15

A(config-if)#standby 50 track fastethernet 0/1 55
```

IP Address: 10.1.1.50
Default Gateway 10.1.1.1

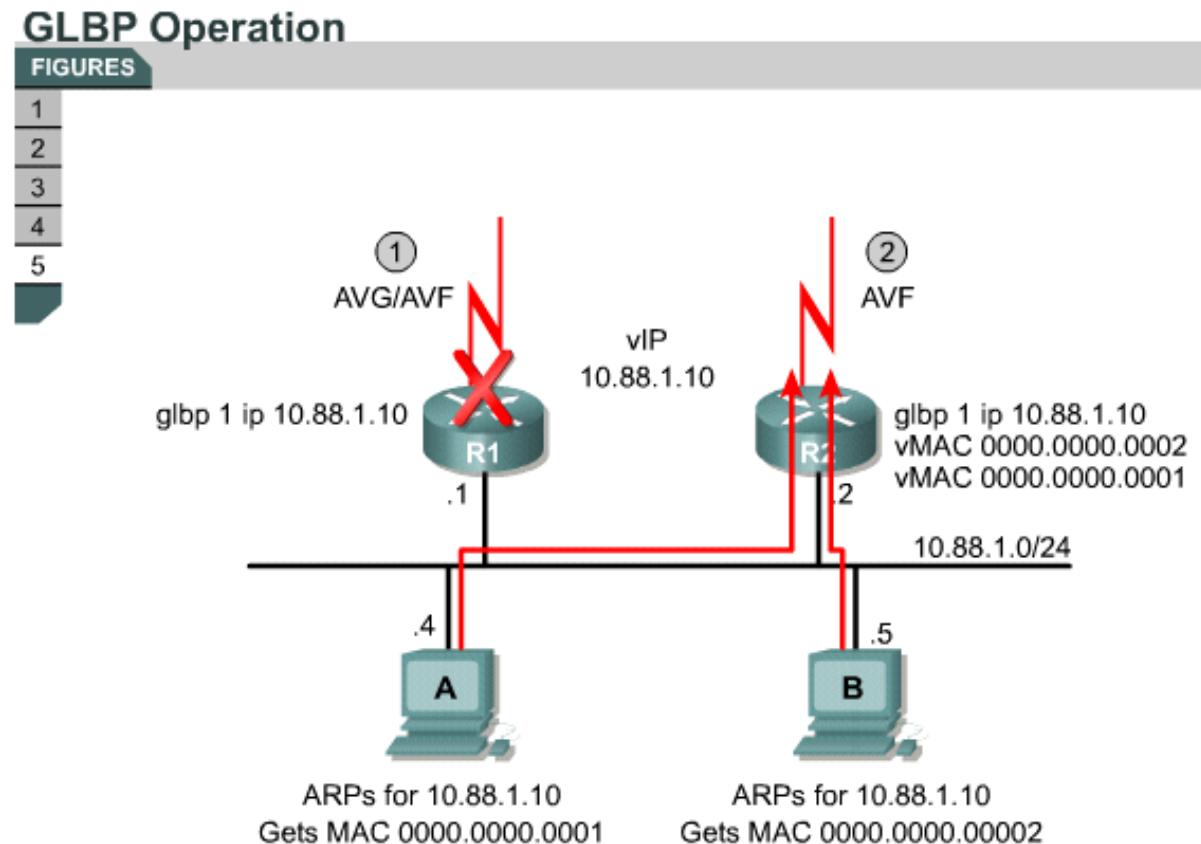
Virtual Router Redundancy Protocol (VRRP)

- Similar to HSRP
- Interoperability between equipments of distinct vendors
- A “Master” *router* and several “Backup” *routers*
- Periodic updates sent by Master *router*
- VRRP should be used when ot all routers are Cisco.



Gateway Load Balance Protocol (GLBP)

- Functions: Redundancy + Load Balance



All contents copyright © 2003 Cisco Systems, Inc. All rights reserved.

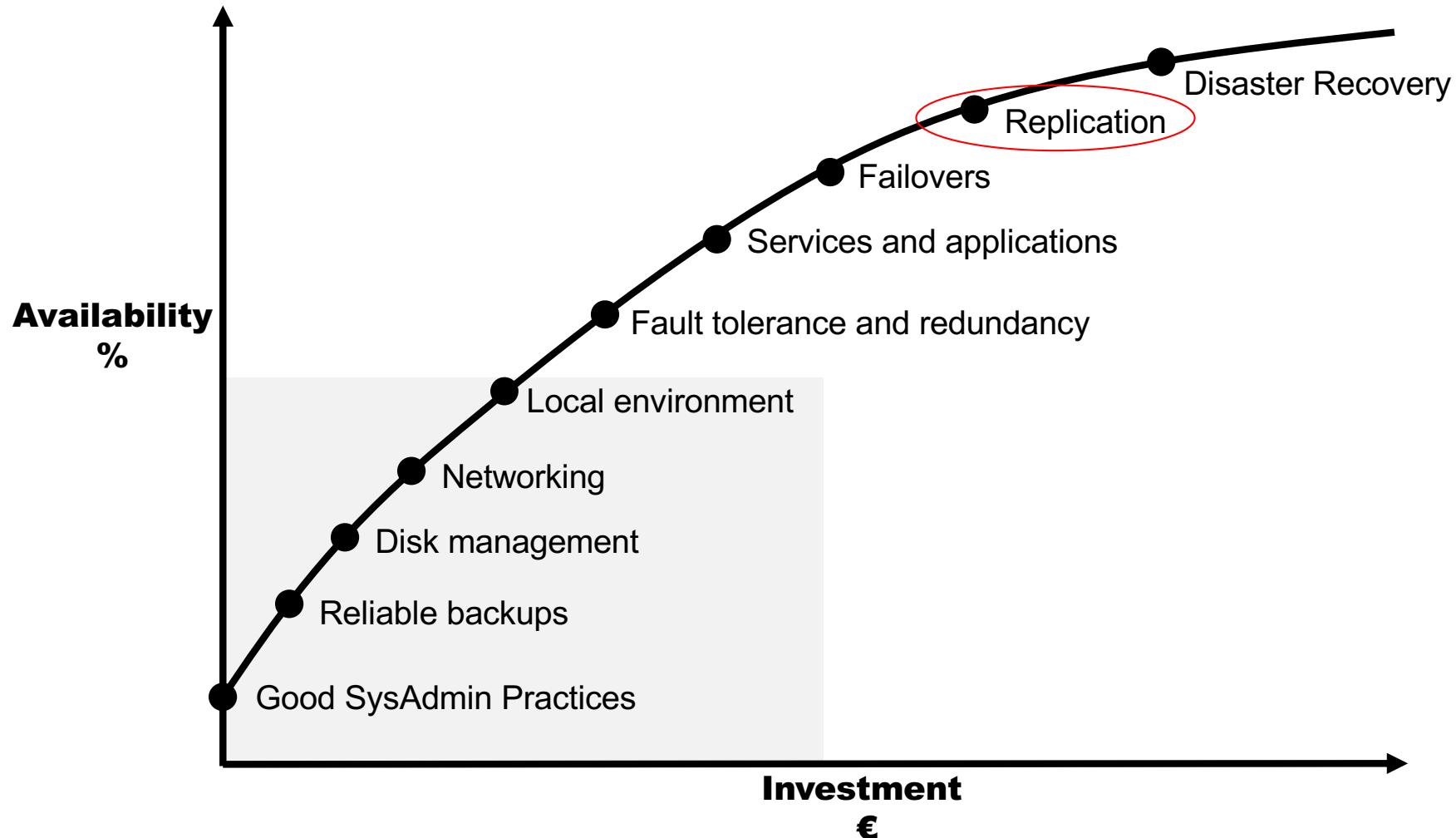
Bibliografia

- RFCs 2281, 2378 e 3768
- Mário Antunes; “*Gestão de Projetos TI e administração centralizada de sistemas e redes – cenários práticos em contexto empresarial*”; IPLeiria; 2010

Replicação de dados

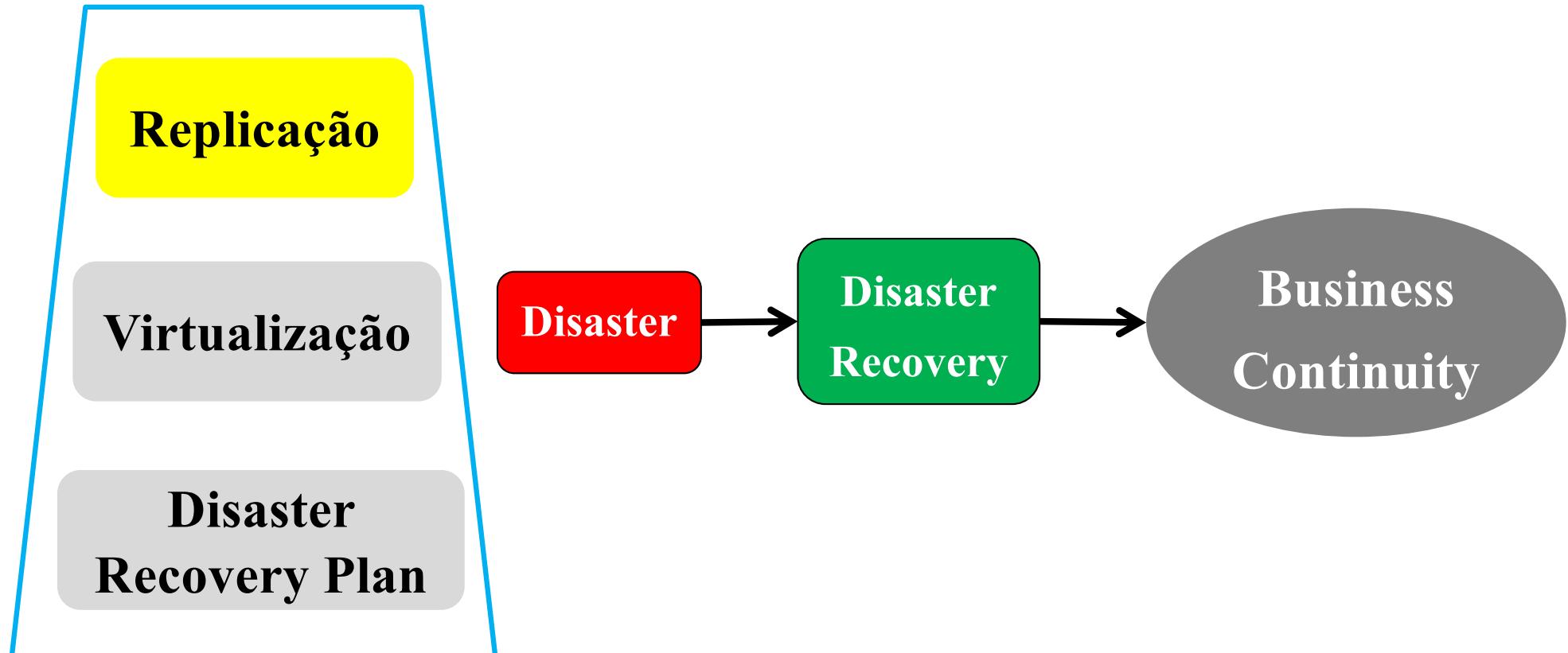
1. Tipos de replicação de dados
2. Tecnologias e protocolos mais utilizados
3. RAID
4. Noção de SAN
5. SCSI
6. iSCSI
7. Fiber-Channel

Enquadramento

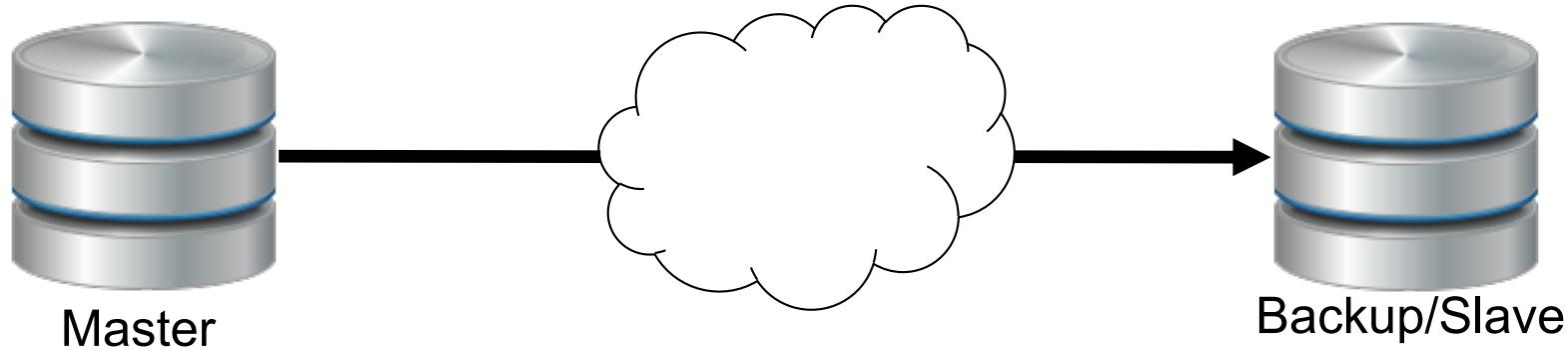


Adapted by Marcus E, Stern H., "Blueprints for high availability"; 2003; Wiley; ISBN: 0471430269;

Enquadramento



Enquadramento



REPLICAÇÃO \neq **MIRRORING** \neq **PARTILHA**

- A replicação trata os conjuntos de discos separadamente
- Os discos de cada site podem ter uma configuração em RAID
- Replicação assegura a existência de duas cópias consistentes
- Numa estratégia de DR, cópias estão fisicamente distantes.

Motivação

- Operações de disaster recovery. Recuperação dos dados do negócio após falha do site principal
- Dados no site de backup podem ser usados para outras tarefas, sem comprometer site principal (p.e. reports, data-mining, ...)
- Nalgumas situações, site de backup pode ser usado para estratégias de *failover*.

Tipos de replicação

Latency-based

- Síncrona
- Assíncrona
- Periódica

Initiator-based

- Hardware
- Software
- Filesystem
- Aplicação (p.e. DB)
- Transações

Tipos de replicação – latency-based - síncrona

- Cópia simultânea entre os nós master e slave
- Latência entre a cópia dos dados pela rede e a respetiva confirmação
- Distância pode variar de acordo com a tecnologia usada
- Garante sincronismo entre as cópias dos site principal e do de DR
- Consistência garantida pela atomicidade das operações.
- Exemplo: BD distribuídas, via cloud (Google, Amazon, ...)

Solução que garante o mínimo de perda em caso de desastre

Tipos de replicação – latency-based - assíncrona

- Dados são guardados localmente no servidor master
- Cópia para o destino é feito de acordo com condições definidas: largura de banda, carga do servidor, etc...
- Diminuição da periodicidade de cópia melhora atualização do slave

Perda de dados como compromisso do tempo de latência

Tipos de replicação – latency-based - periódica

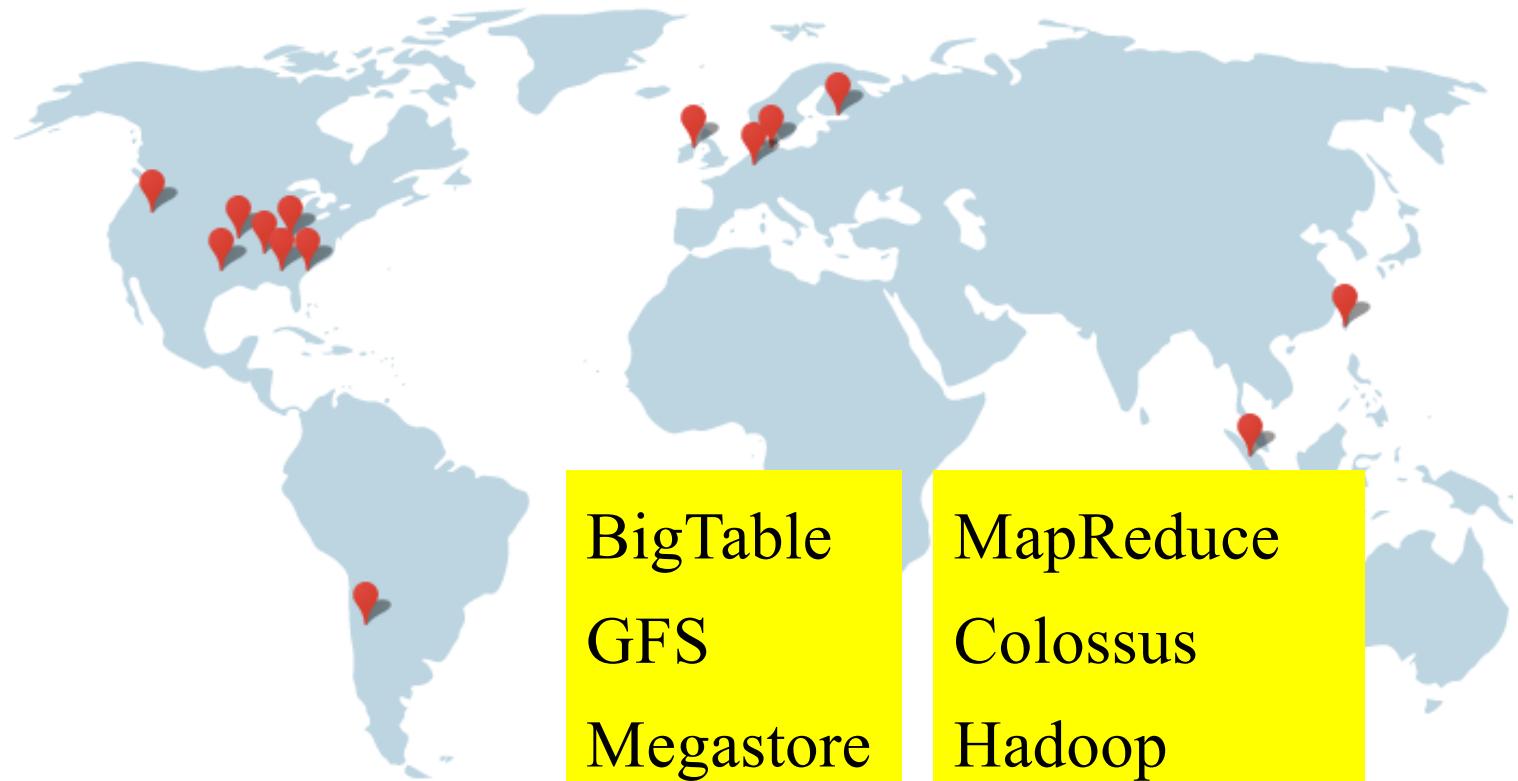
- Backup do master é realizado periodicamente e enviado pela rede para o slave.
- O modo de envio dos dados pela rede é manual.
- A periodicidade de realização do backup é definida manualmente

Perda de dados como compromisso da periodicidade da cópia

Tipos de replicação – exemplo da Google

Americas

Berkeley County, South Carolina
Council Bluffs, Iowa
Douglas County, Georgia
Quilicura, Chile
Jackson County, Alabama
Mayes County, Oklahoma
Lenoir, North Carolina
The Dalles, Oregon



Asia

Changhua County, Taiwan
Singapore

Europe

Hamina, Finland
St Ghislain, Belgium
Dublin, Ireland
Eemshaven, Netherlands

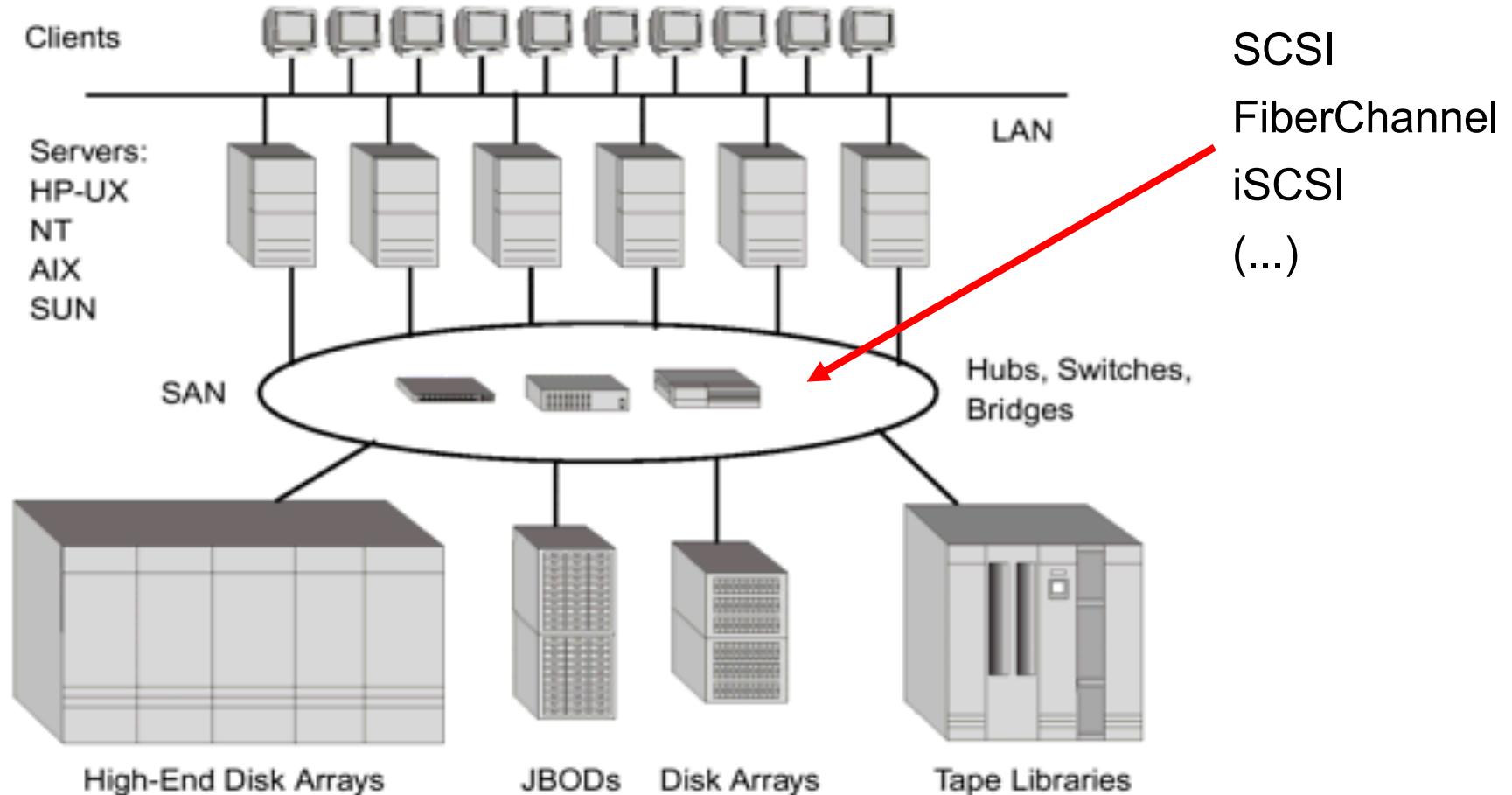
<http://www.google.com/about/datacenters/inside/locations/>

<http://www.datacentermap.com>

Tipos de replicação – failover remoto

- Deteção automática da falha no site principal
 - Promoção automática do site de backup a principal
 - Disponibilizar automaticamente os recursos principais
 - Arrancar com as aplicações críticas no site de DR
-
- Clusters remotos de HA com monitorização dedicada
 - Aplicam-se os conceitos tradicionais de clusters de HA

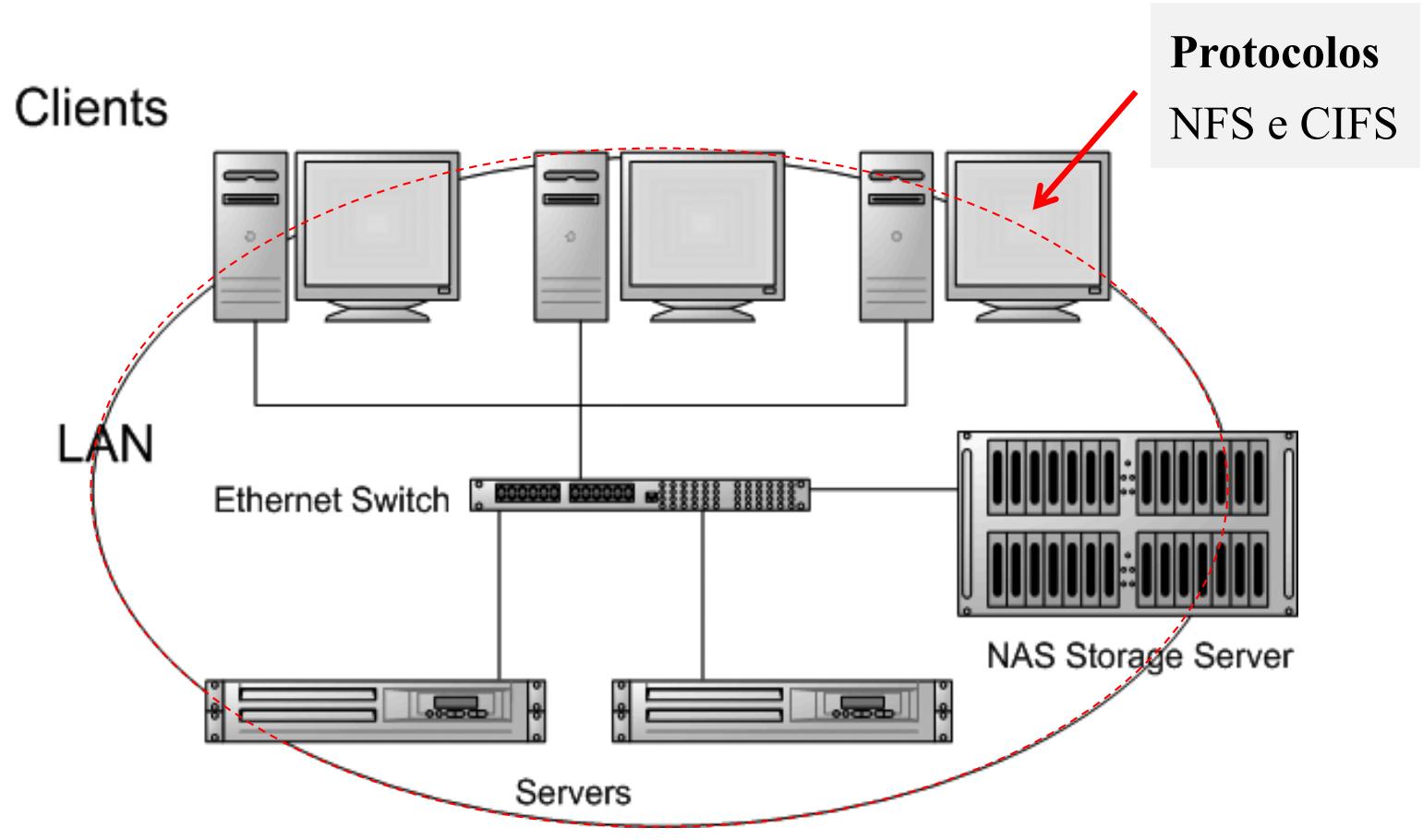
Noção de SAN



Noção de SAN

- Acesso partilhado ás unidades de storage (discos, tapes, ...)
- Acesso ao storage numa perspetiva block-based
- Acesso transparente para os utilizadores
- Facilita a gestão de storage e é fator chave na replicação de dados e em *disaster recovery*
- Protocolos mais utilizados: FiberChannel (FC) e SCSI.
- Implementação “over IP” (iFCP e iSCSI) permite topologias de área alargada.

Noção de NAS



Noção de NAS

- Centralização do storage num servidor dedicado, com RAID e outras funções de redundância disponibilidade.
- Acesso pela rede local, essencialmente sobre a rede TCP/IP
- Acesso ao storage numa perspetiva file-based.
- Acesso transparente para os utilizadores por protocolos NFS e CIFS
- Servidores dedicados para NAS: FreeNAS, NAS4Free, ...

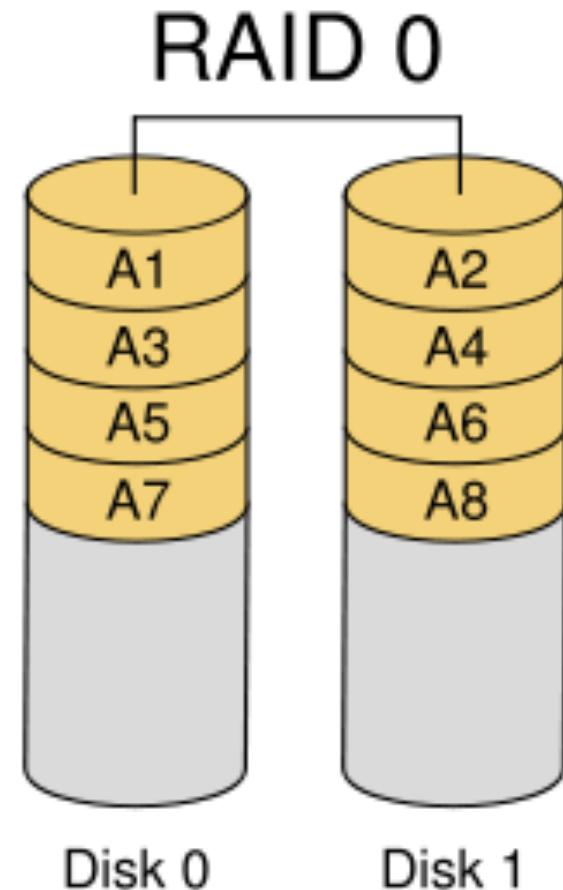
Sistema RAID

- Redundant Array of Independent/Inexpensive Drives
- Os dados são replicados por vários discos
- RAID
 - Hardware: transparente ao sistema operativo
 - Software: implementado ao nível do sistema operativo
- Conceitos chaves
 - Replicação (*mirroring*)
 - Particionamento dos dados por vários discos (*stripping*)

Níveis de RAID

RAID 0 (*striping*)

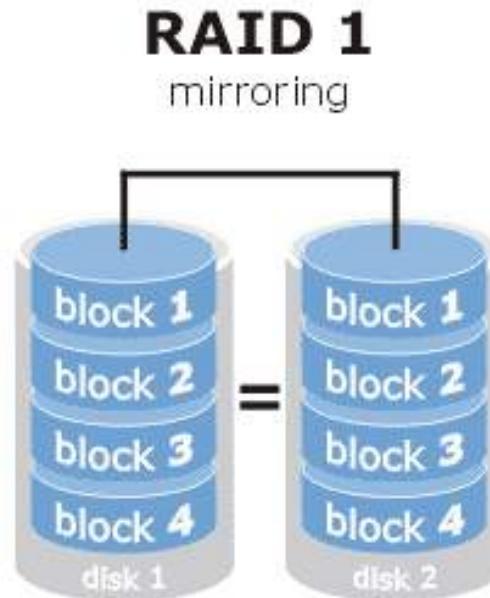
- Cada ficheiro é particionado
- Respectivos blocos (e.g. 1,A2,A3,...) guardados em cada um dos discos
- Aumenta o desempenho - A leitura de um ficheiro pode ocorrer em paralelo (A1 e A2 podem ser lidos ao mesmo tempo, dado que estão em discos diferentes)
- Não oferece redundância adicional
Se um disco falhar, os dados ficam perdidos...



Níveis de RAID

- **RAID 1 (*mirroring*)**

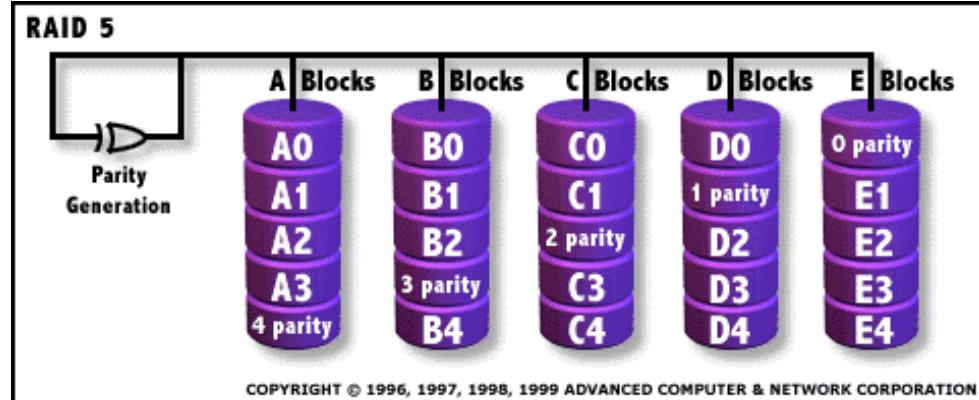
- O disco 1 é uma réplica do disco 0
- Não há melhoria do desempenho
- Há melhoria da tolerância a falhas



Níveis de RAID

- **RAID 5**

- Mínimo 3 discos
- Paridade distribuída



- Para cada bloco de dados existe um bloco de paridade ****noutro**** disco
- Tolera a falha de um disco
Se um disco avariar, o sistema mantém-se operacional. O disco em falta pode ser recuperado através da paridade
- É contudo necessário recuperar o sistema (sistema está vulnerável à falha de um segundo disco)

Ainda sobre o RAID

Um sistema RAID só protege de falha(s) de hardware:

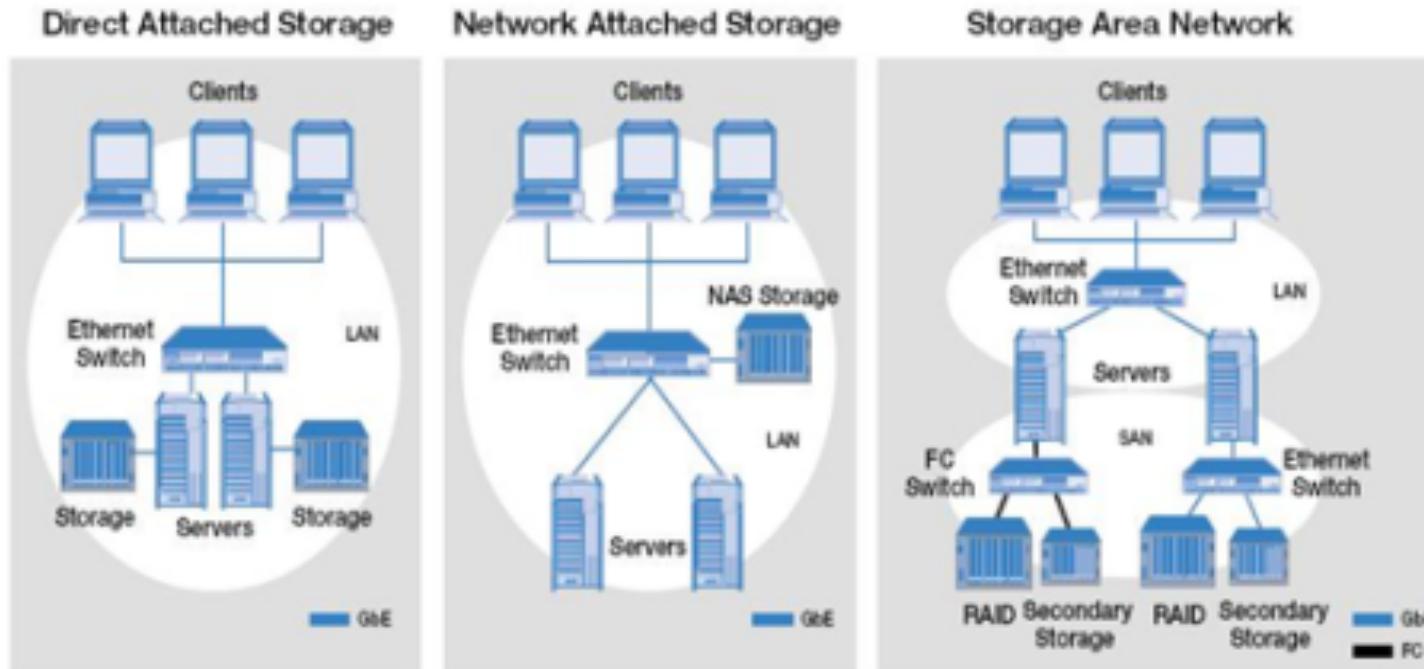
→ Não protege de acidentes provocados por humanos/software, ...

Portanto há sempre necessidade de complementar RAID com sistemas de salvaguarda da informação

→ O RAID aumenta a disponibilidade e induz alguma tolerância a falhas ...

→ ...mas NÃO substitui os backups!

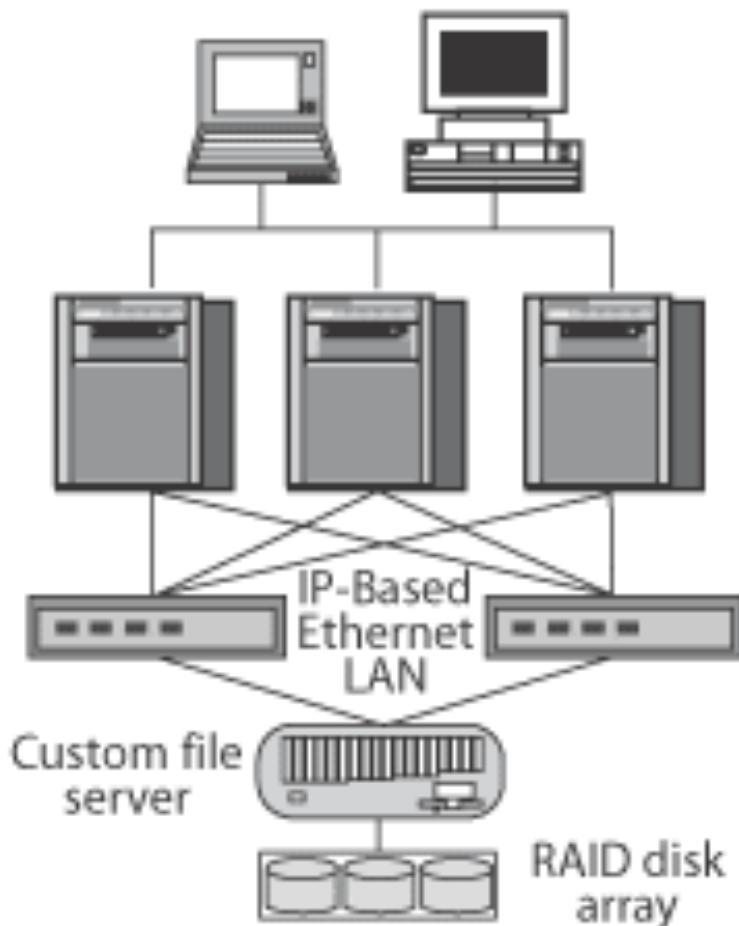
Evolução do storage distribuído/partilhado



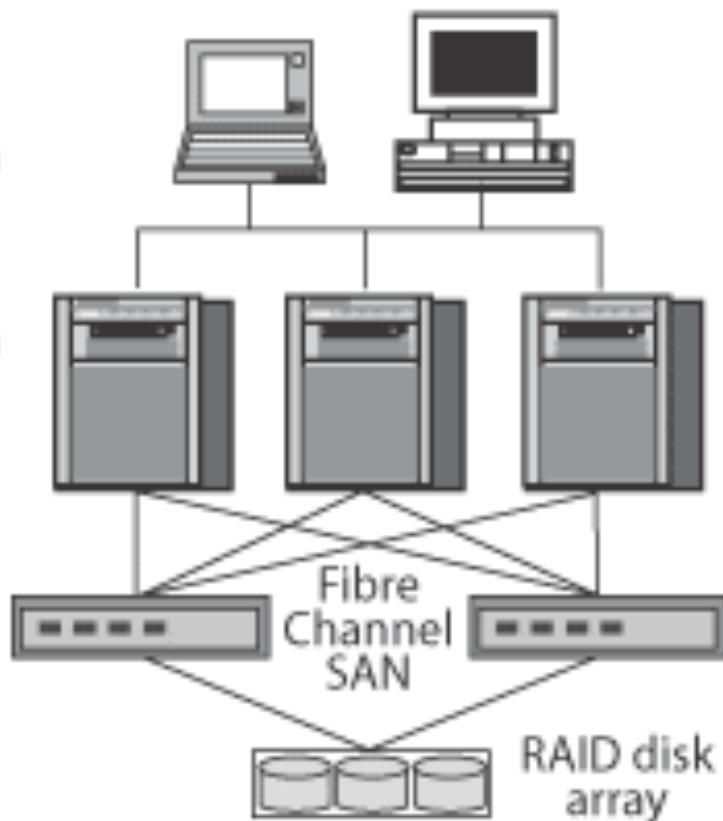
<https://sandipbagwe.wordpress.com>

Evolução do storage distribuído/partilhado

Network Attached Storage (NAS)

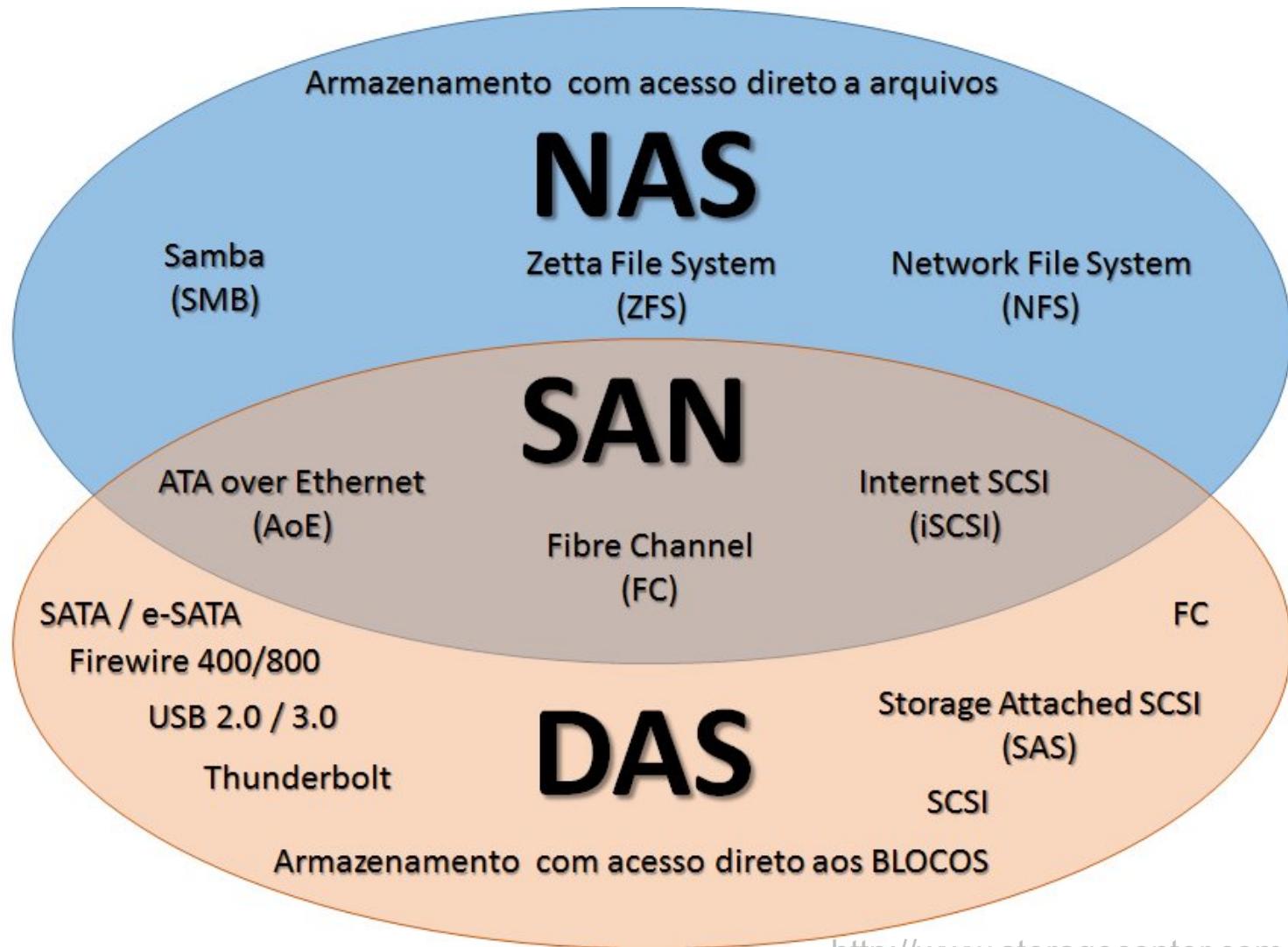


Storage Area Network (SAN)



<http://www.getdomainvids.com>

Evolução do storage distribuído/partilhado



Hardware



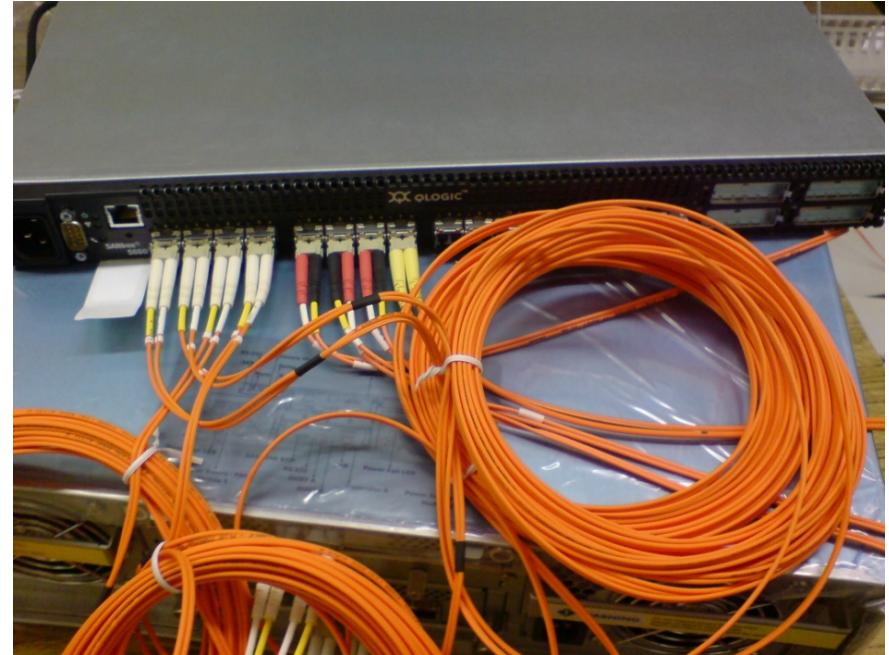
Synology DS1813+ 8-Bay Scalable NAS



FC cable – Cat6

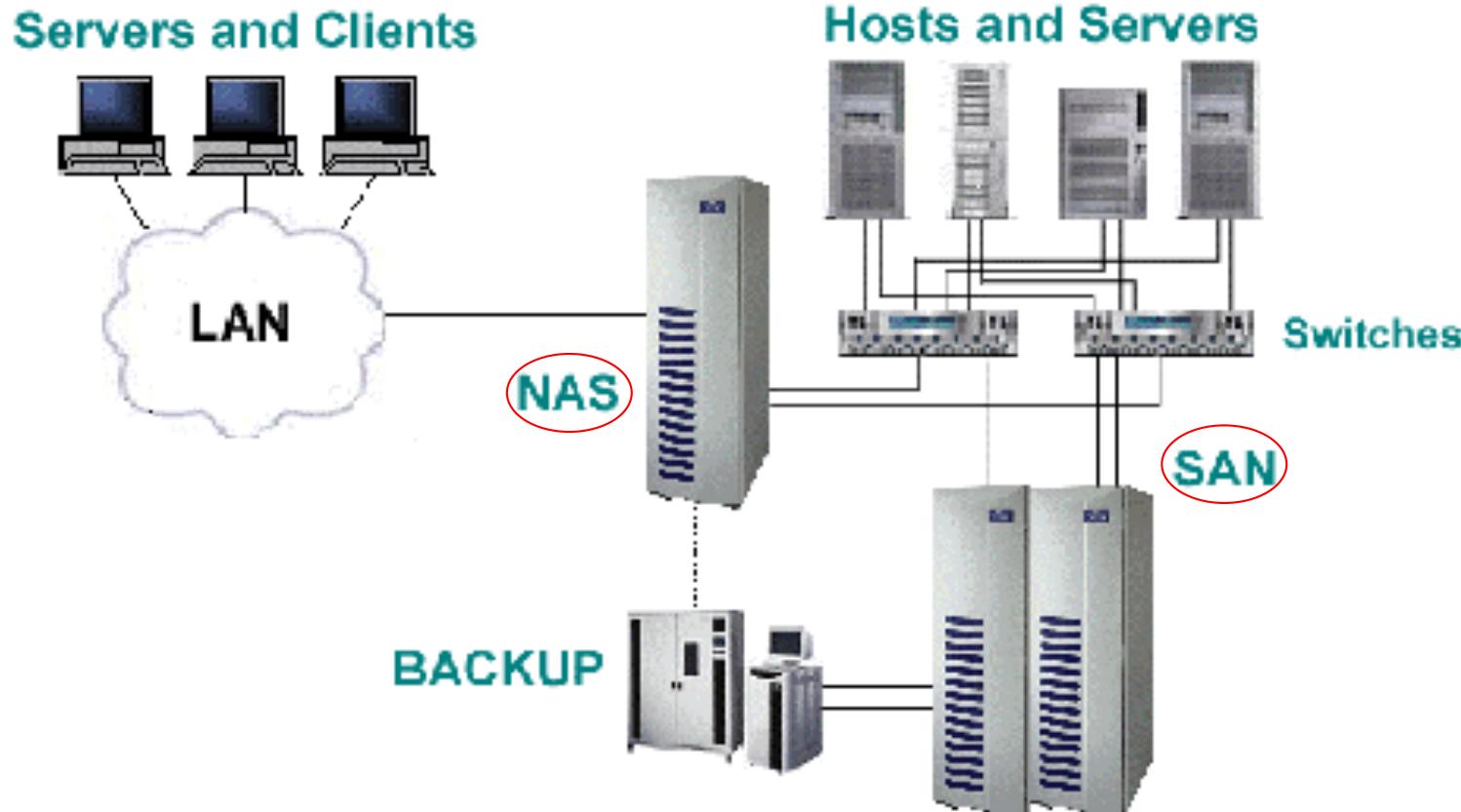


FC cable – optical fiber



Fiber Channel switch

Soluções híbridas - SAN / NAS



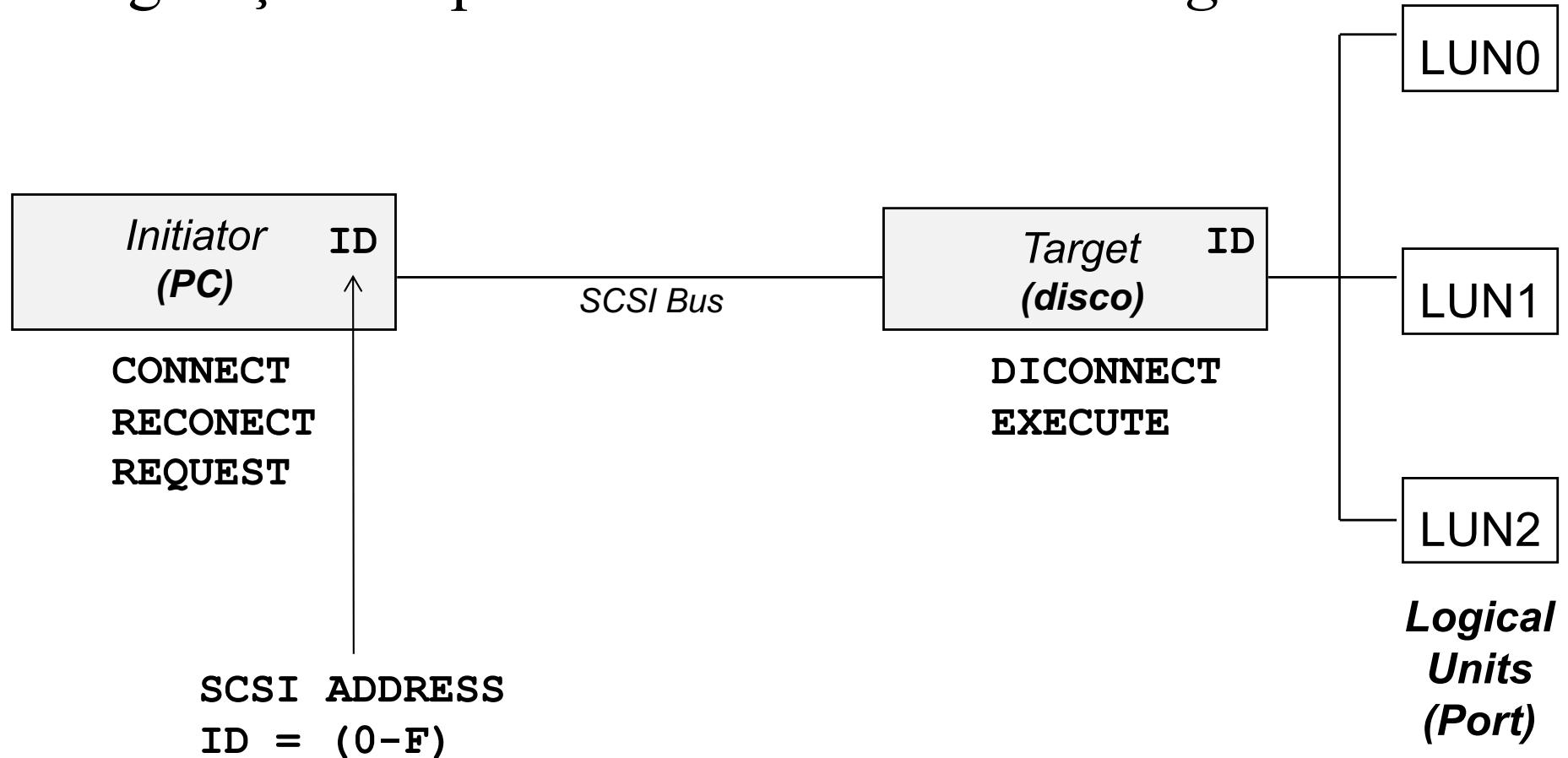
<http://www.cityu.edu.hk>

Tecnologia SCSI

- Small Computer System Interface
- Inicialmente desenvolvido pela Shugart Associates - SASI (Shugart Associates System Interface)
- Atualmente denominado SCSI e com um ANSI standard (T10)
- 3 versões: SCSI-1, SCSI-2 e SCSI-3
- Dispositivos comunicam através de um bus.
- Acesso dos hosts aos dispositivos: block based
- Principais limitações: comprimento (25 m); número de dispositivos suportados;

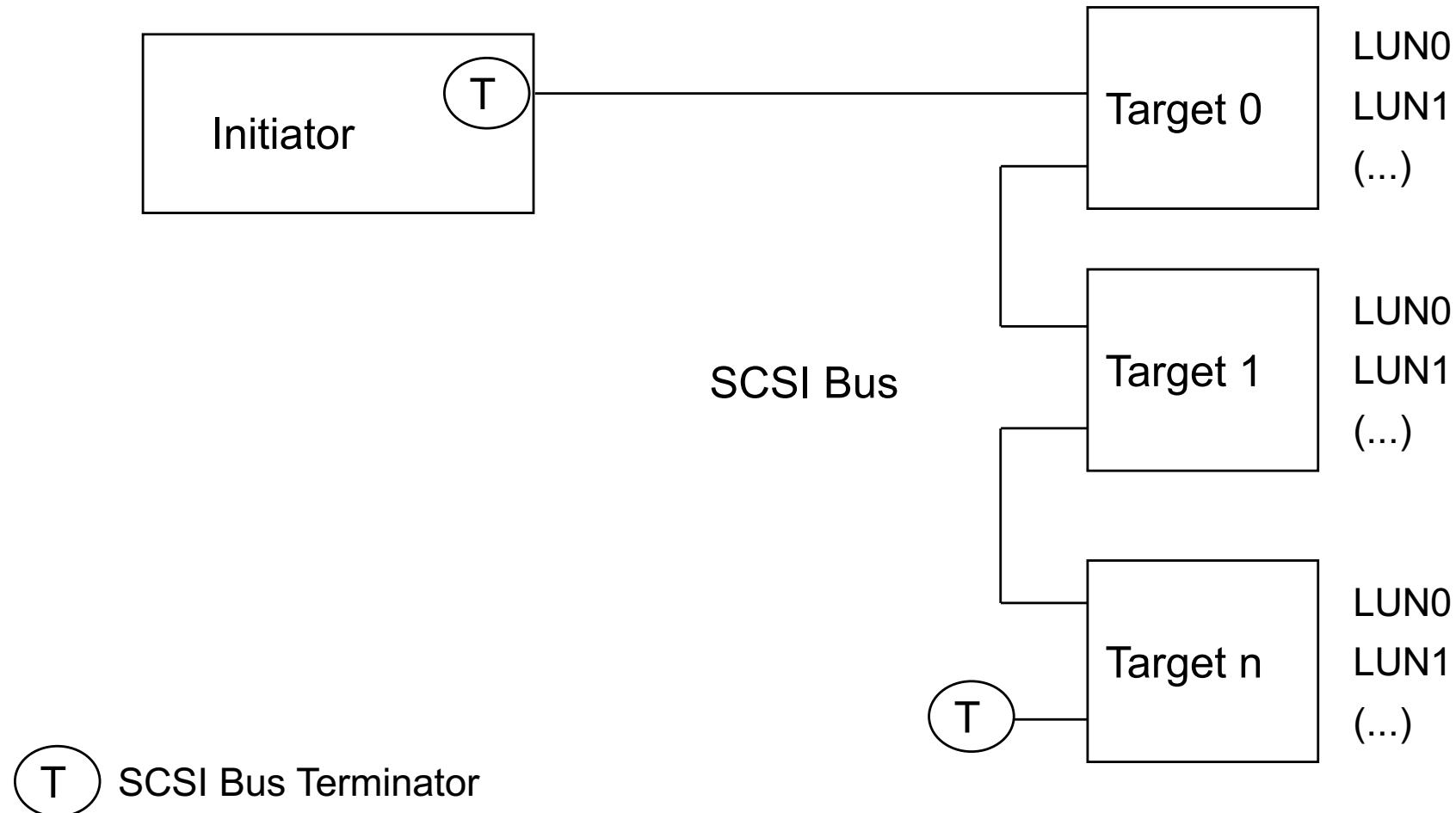
Tecnologia SCSI

Configuração simples: um *initiator* → um *target*



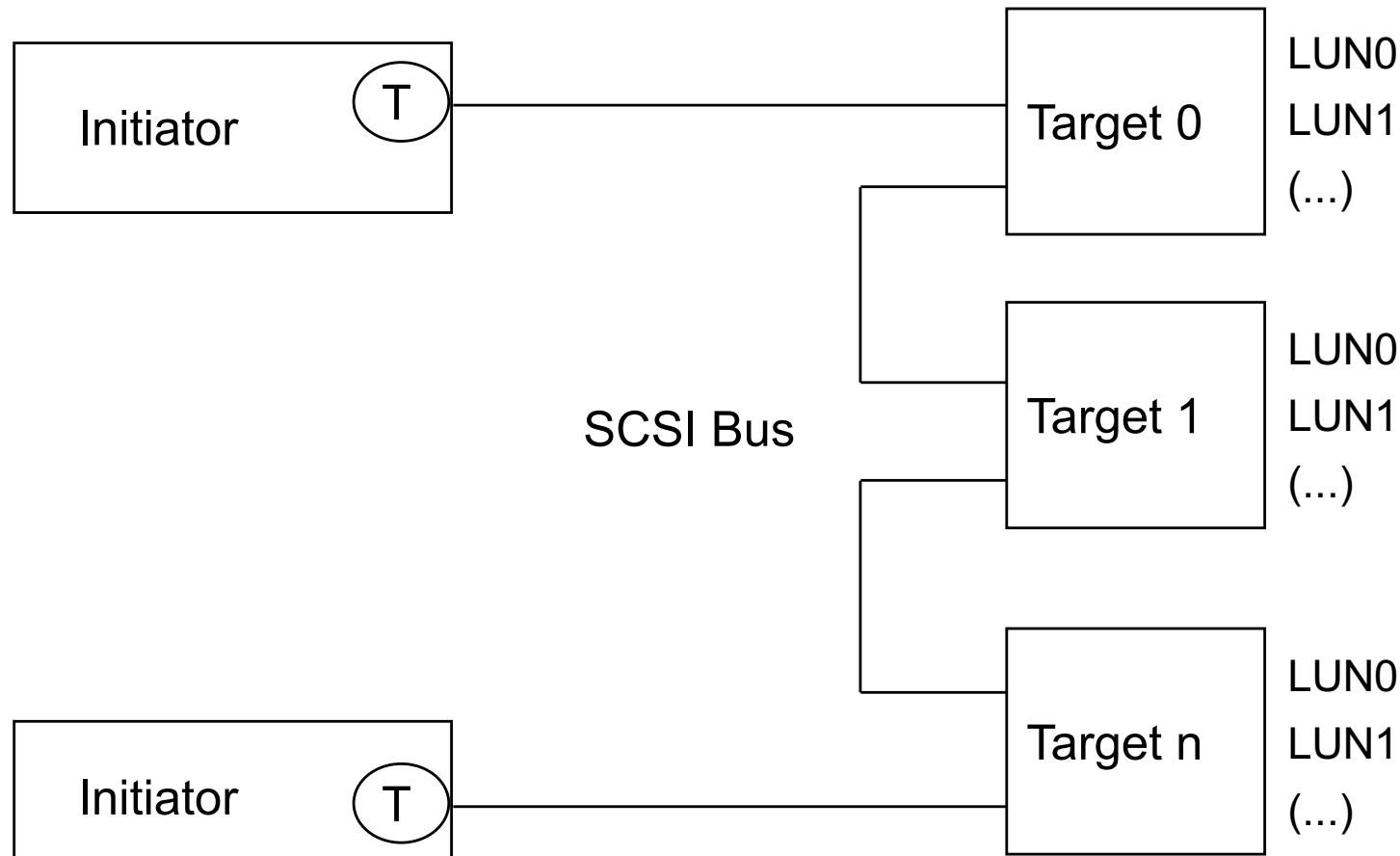
Tecnologia SCSI

Configuração: um *initiator* → vários *target*



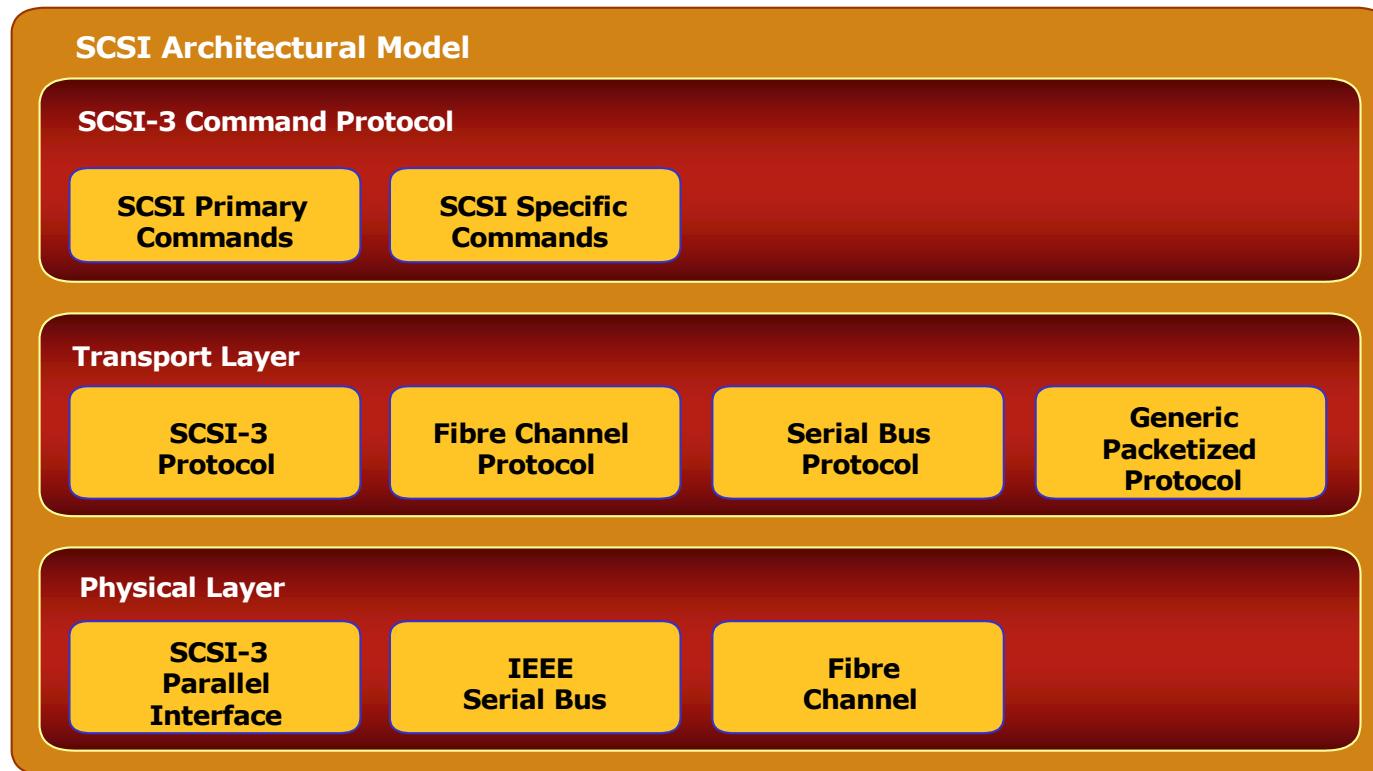
Tecnologia SCSI

Configuração: vários *initiators* → vários *target*



Tecnologia SCSI

Arquitetura

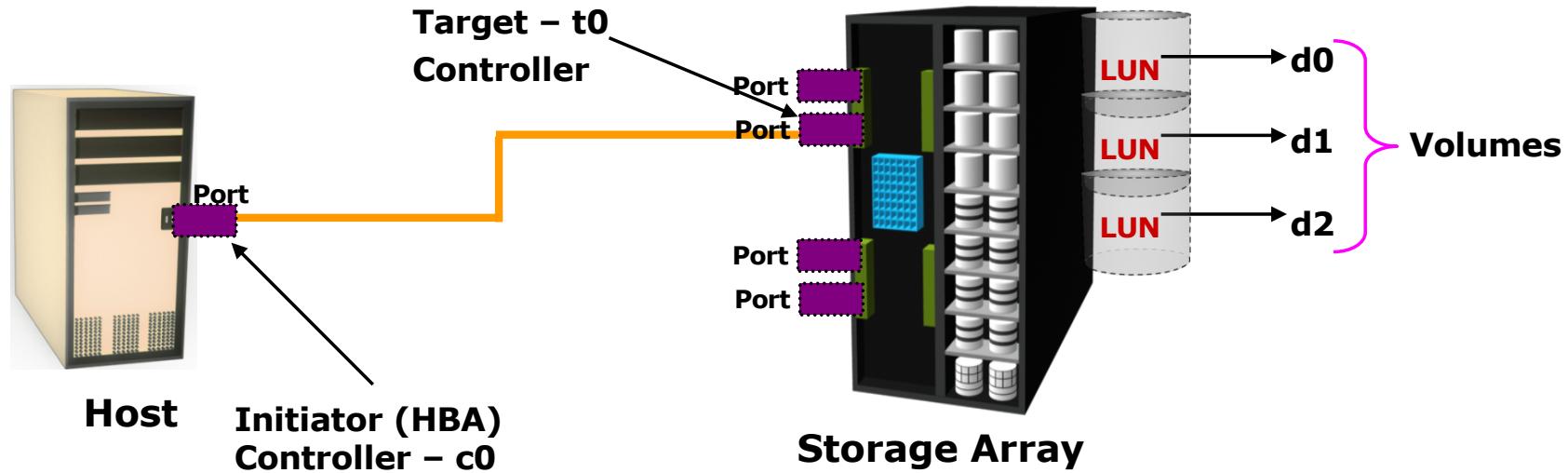


Comandos de I/O entre os dispositivos

Regras de comunicação entre os dispositivos

Detalhes da interface, adaptadores, etc..

Tecnologia SCSI - endereçamento



Host Addressing:

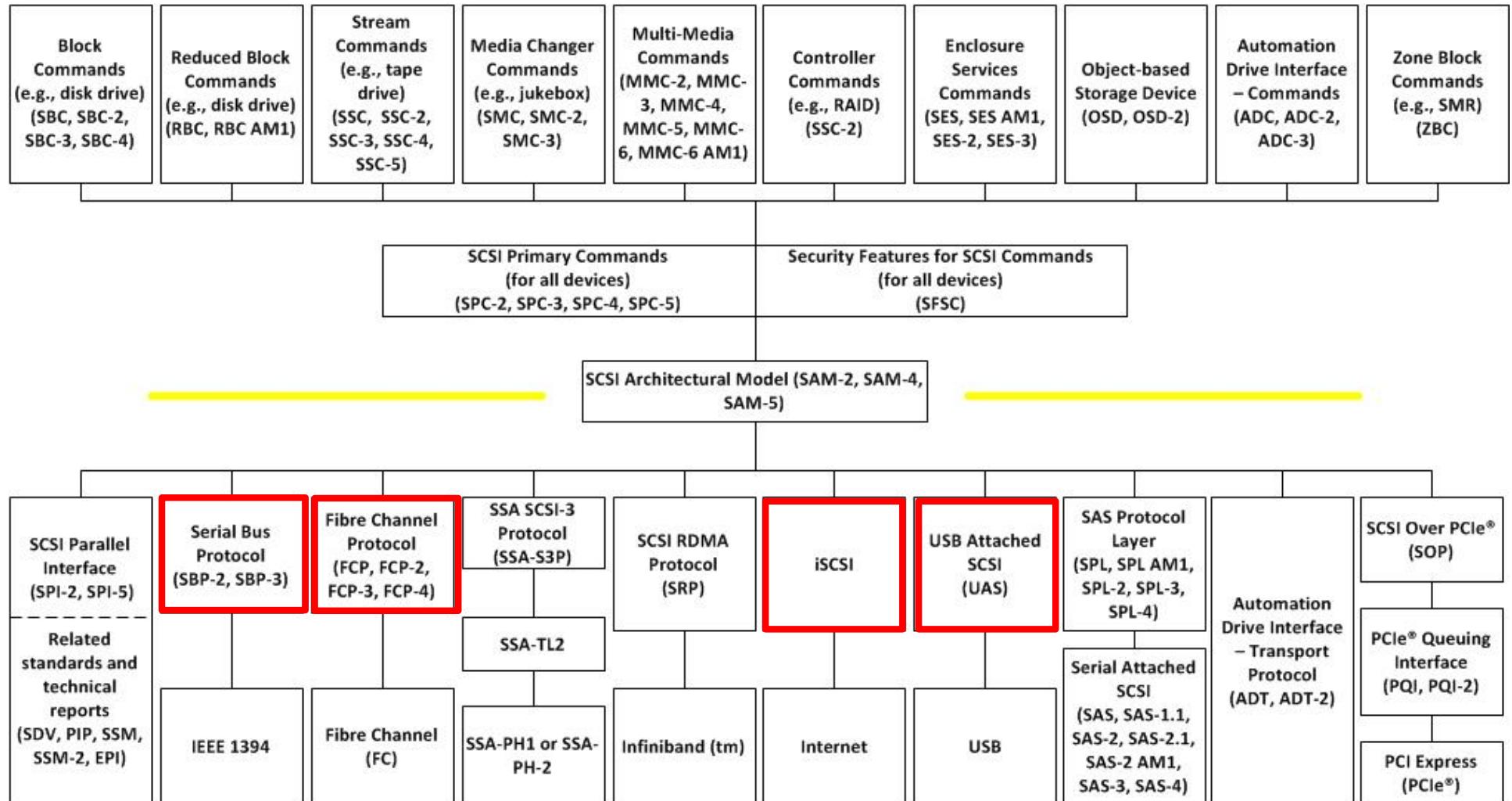
Storage Volume 1 - c0t0d0

Storage Volume 2 - c0t0d1

Storage Volume 3 - c0t0d2

Initiator ID	Target ID	LUN
c0	t0	d0

Tecnologia SCSI - standard



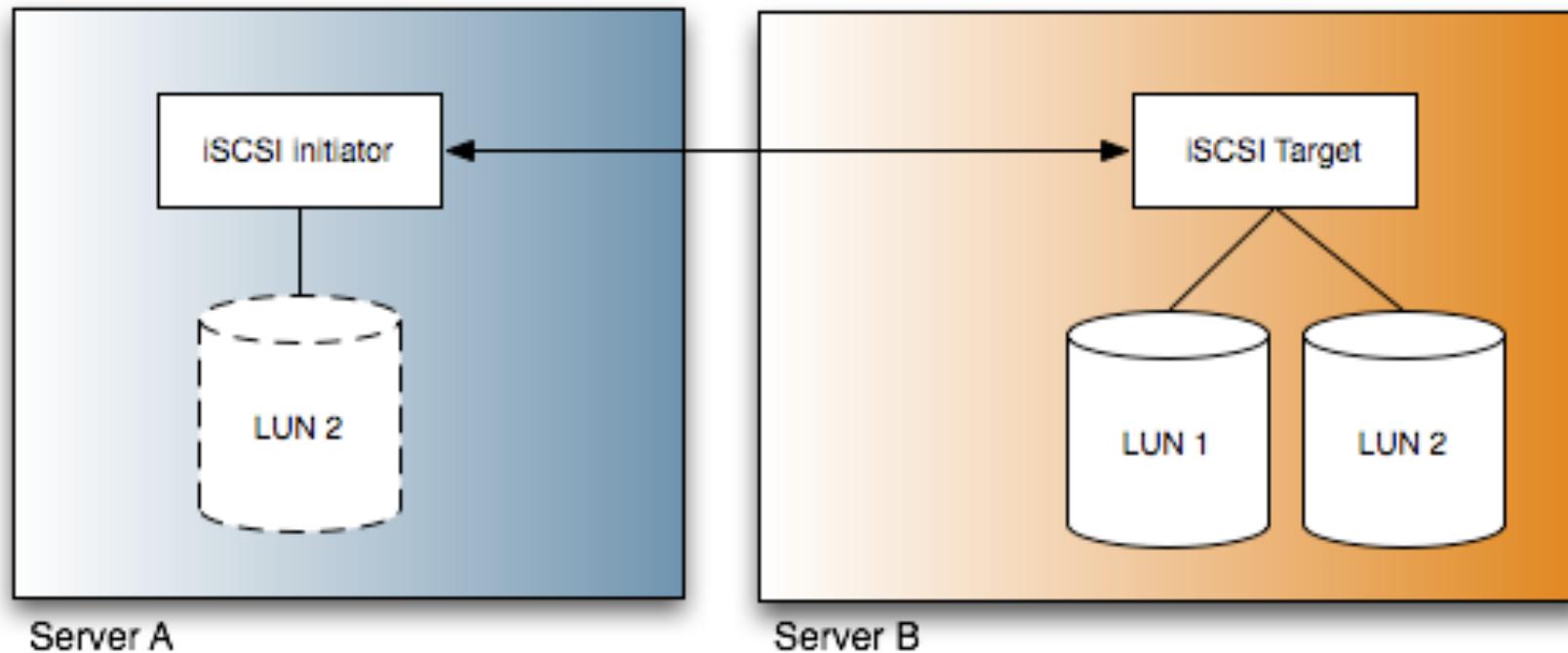
<http://www.t11.org>

Tecnologia iSCSI

- internet Small Computer System Interface
- Motivação:
 - enviar comandos SCSI por rede TCP/IP (p.e. Internet).
 - acesso/partilha de storage através de longas distâncias
- Estabelece ligações “*initiator* → *target*” numa sessão TCP
- Topologia em estrela
- Normas IETF: RFCs 3720, 3721

Tecnologia iSCSI

Acesso remoto por iSCSI



Acesso a uma LUN remota (*target*) a partir de um dispositivo iSCSI (*initiator*).

Tecnologia iSCSI

- **Connection** Ligação TCP usada para enviar mensagens de controlo, comandos SCSI, parâmetros e iSCSI PDUs. Poderá haver várias “connections” entre o *target* e o *initiator*, todas na mesma “session”.
- **Session** Define um grupo de “connections” TCP a partir de um *initiator*. As “connections” podem ser adicionadas e removidas dinamicamente. O *initiator* consegue aceder a todas as “connections” numa sessão e o respetivo *target*.

1 session → n connections

Tecnologia iSCSI

Fases das sessões/ligações iSCSI:

- **LOGIN PHASE**
 - Estabelece ligação TCP
 - Autenticação de ambos os pontos da ligação
 - Negociação de parâmetros operacionais
 - Associação “connection → session”
- **FULL-FEATURE PHASE**
 - Transferência de dados

- Tipos de sessões**
- Normal
 - Discovery

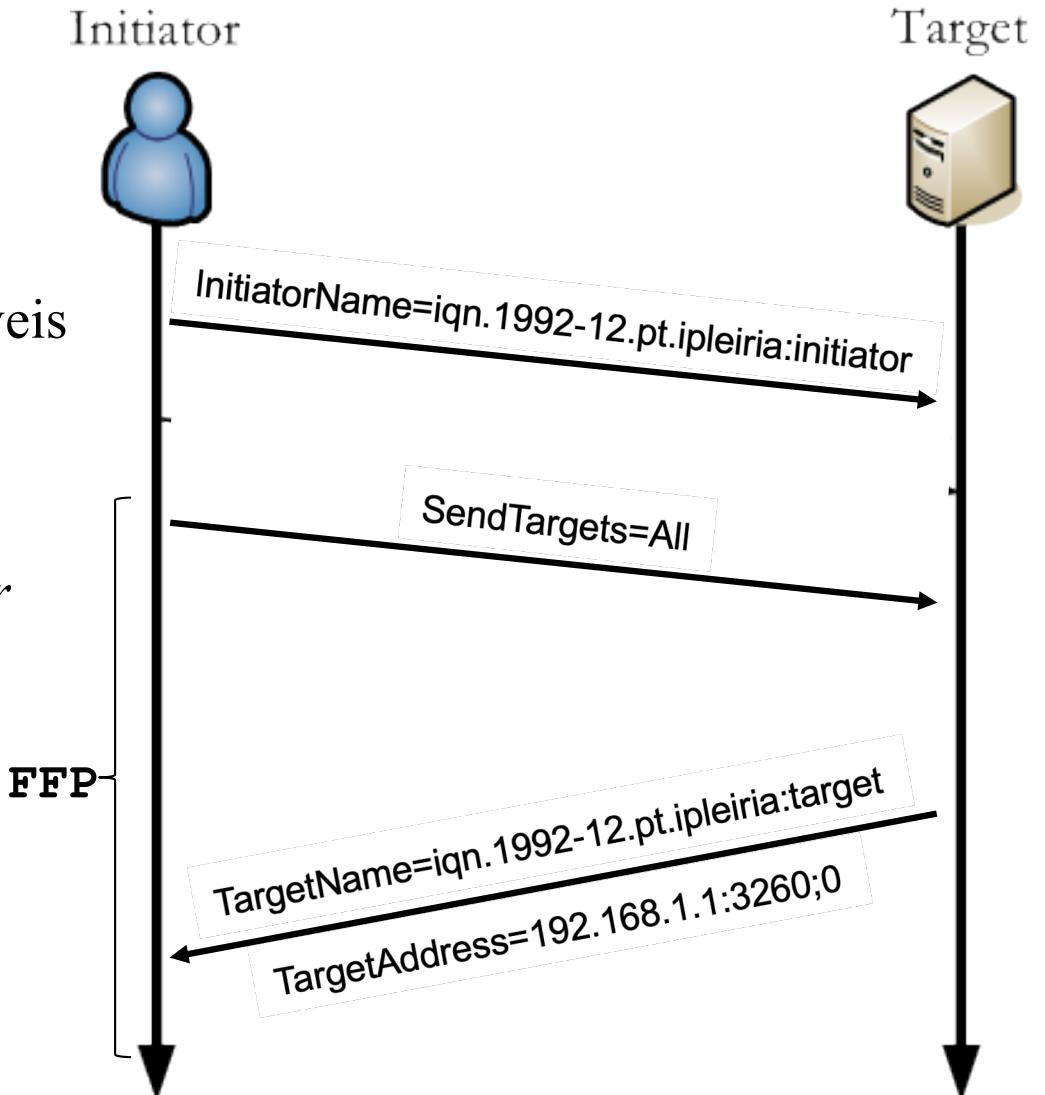
Tecnologia iSCSI

Sessão DISCOVERY

iSCSI *initiator* inicia procura de possíveis iSCSI *targets* a que se possa ligar.

Login Phase: Autenticação do *initiator* no *target* selecionado.

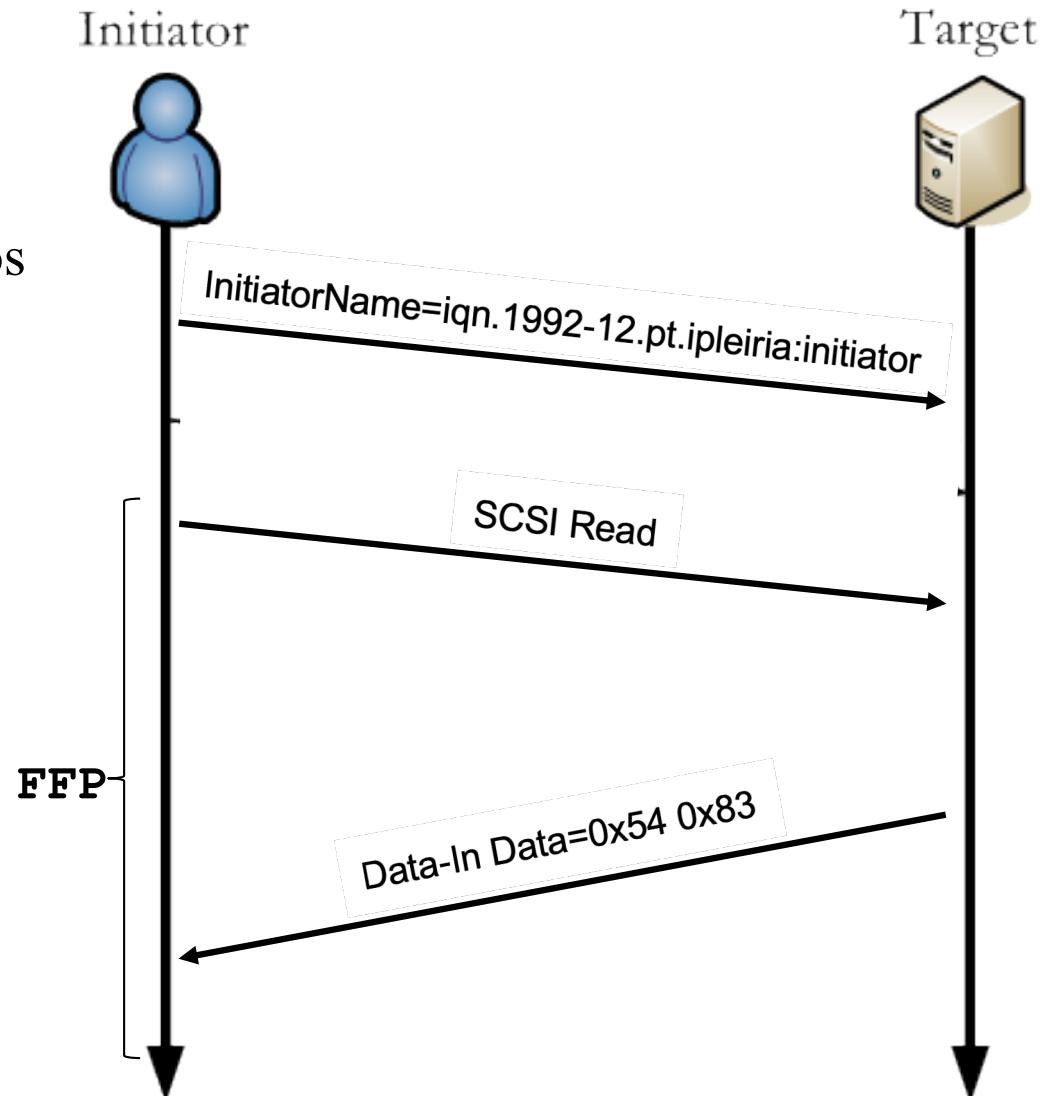
Full-Feature Phase: Troca de mensagens entre *initiator* e *target*.



Tecnologia iSCSI

Sessão NORMAL

Initiator e *target* negoceiam parâmetros de comunicação (p.e. tamanho das mensagens individuais e número de sessões simultâneas).



Tecnologia iSCSI – convenção de nomes



Dois formatos principais: **iqn** e **eui**

iqn (iSCSI qualified Name): definir para cada dispositivo um nome único com detalhes sobre o dispositivo.

Type Date Org.Unit : Location
ign.2001-04.com.example:diskarrays-sn-a8675309

Reverse DNS

Opcional

Tecnologia iSCSI – convenção de nomes



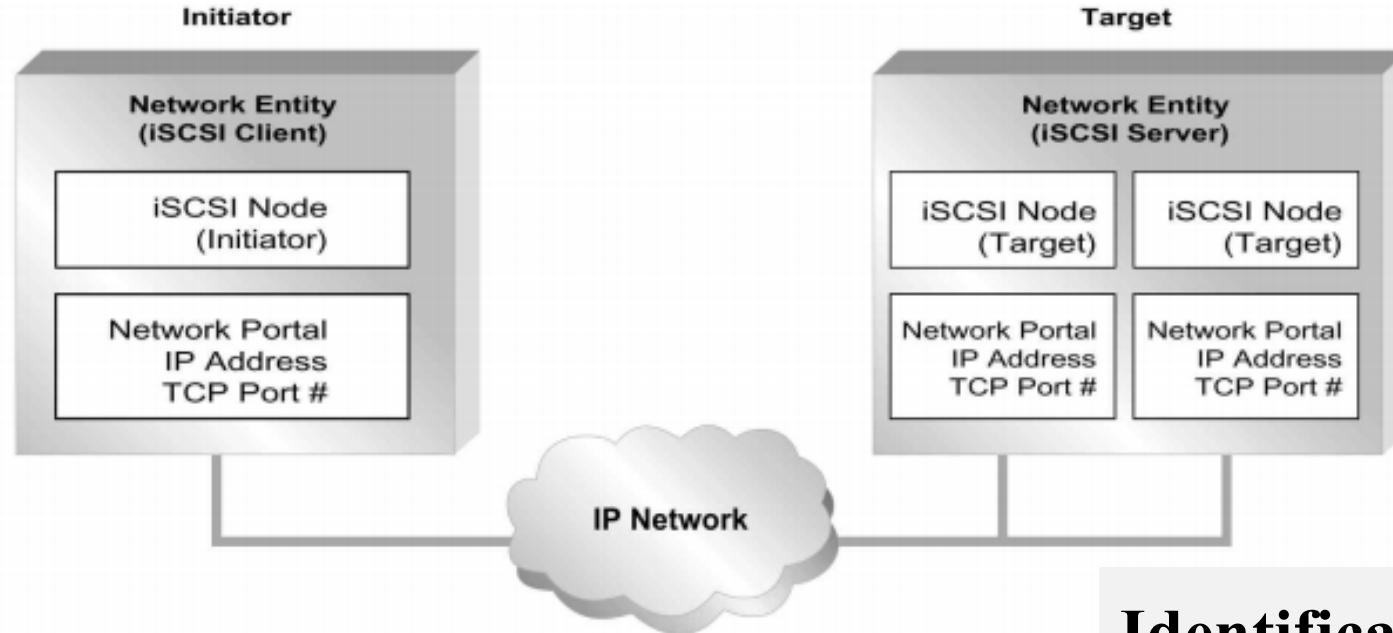
eui: utilizar a convenção IEEE EUI (Extended Unique Identifier) para a definição de IDs (hexadecimal)

Type EUI-64 identifier

eui.02004567A425678D

iSCSI alias: utilizar um nome apelativo para o dispositivo. Esta designação será utilizada durante a fase de login, entre o *initiator* e o *target*.

Tecnologia iSCSI – identificação dos pontos



iSCSI Technical White Paper; White paper; Nishan Systems

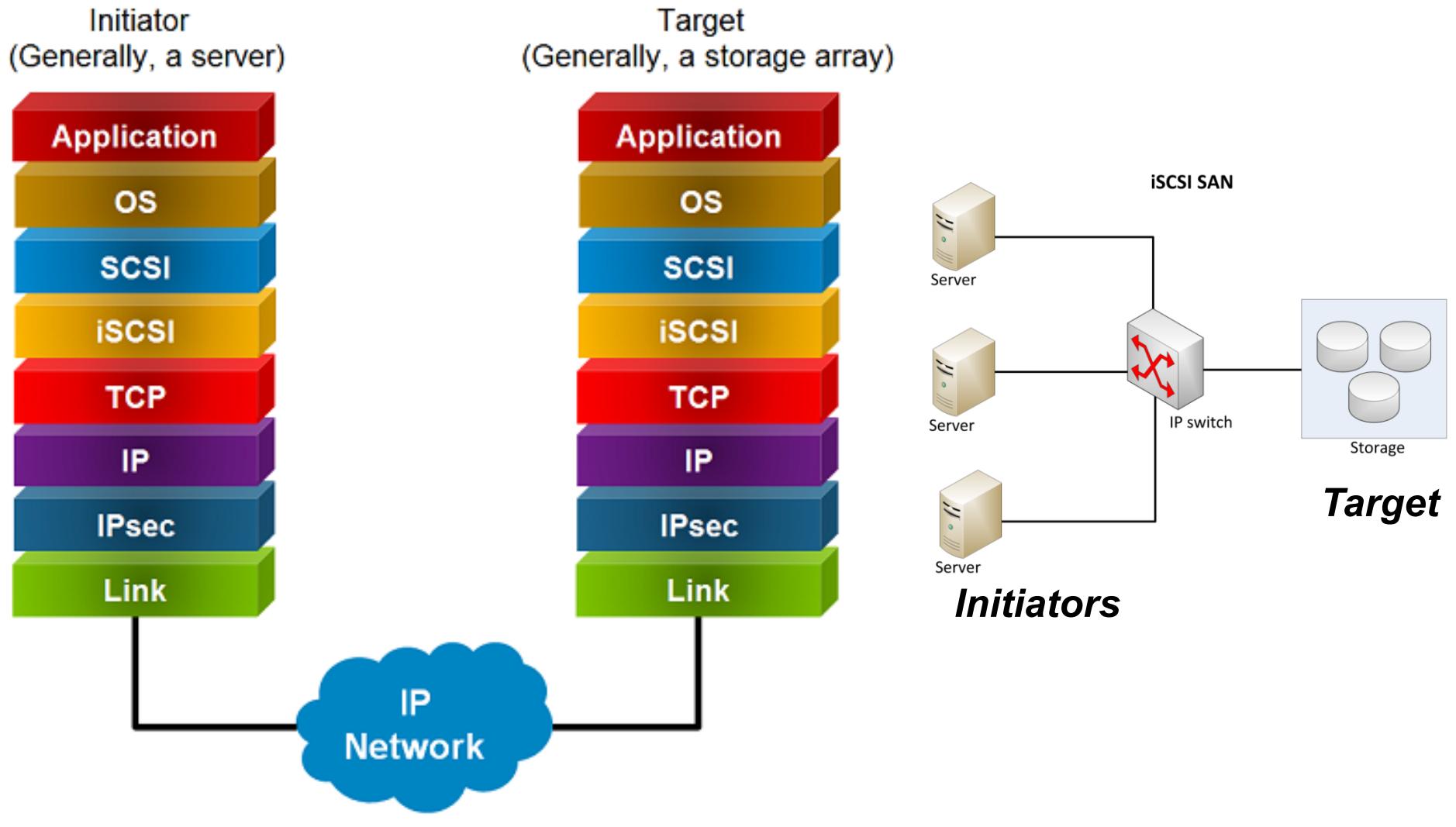
Normalmente:

TCP Port = 860 e 3260

Identificação completa

- hostname ou endereço IP
- TCP Port
- iSCSI ID
- CHAP password (opcional)

Tecnologia iSCSI

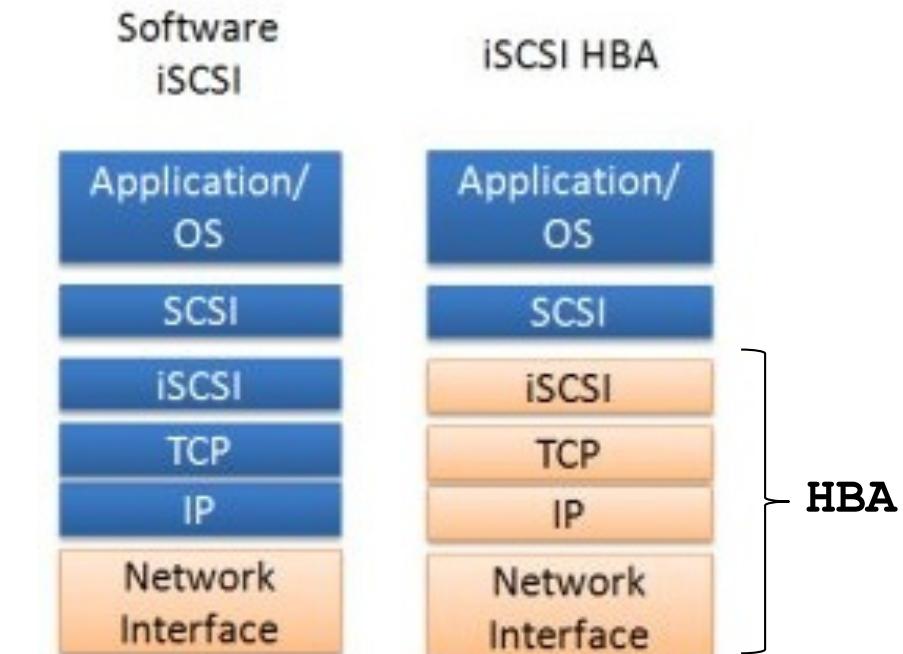


Tecnologia iSCSI - implementações

Sistemas operativos disponibilizam software para target e/ou initiator.

Targets

Host Bus Adapter (HBA) instalados em discos (ou tapes).



Implementação para Linux:

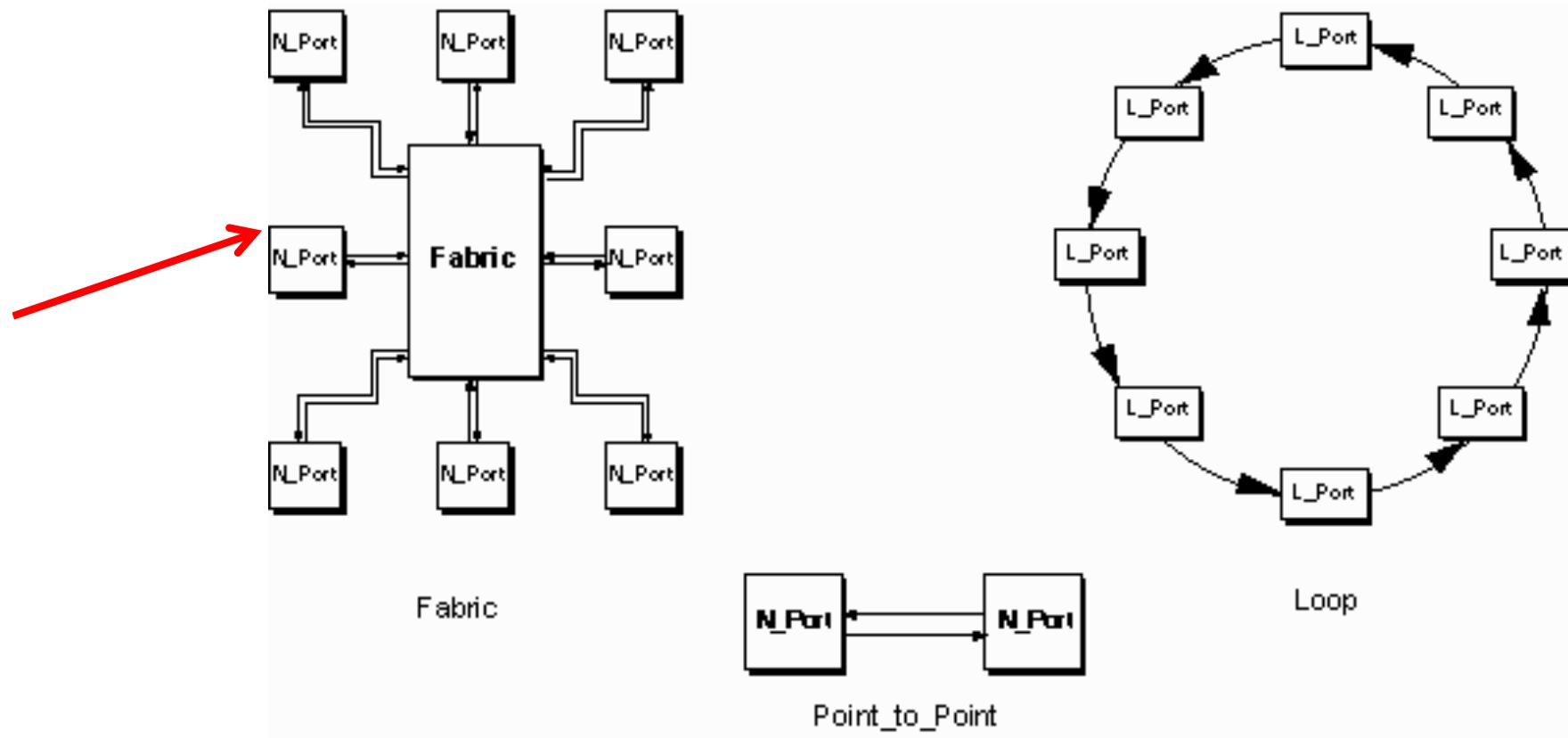
- <http://linux-iscsi.sourceforge.net>
- <http://www.open-iscsi.org>

Tecnologia Fiber-Channel (FC)

- Tecnologia de redes para acesso massivo a storage
- Substituto natural do SCSI: mais rápido e maiores distâncias
- Utiliza o Fiber-Channel Protocol (FCP) , norma ANSI-T11
- Um dos interfaces mais usados para SAN (juntamente com iSCSI)
- Originalmente para fibra (~ 10Kms). Mais recentemente, cobre.
- Utiliza FC Protocol (FCP) na camada de transporte
- Interage com outros protocolos: p.e. IP e SCSI
- Noções similares ao SCSI: *initiator*, *target* e HBA.

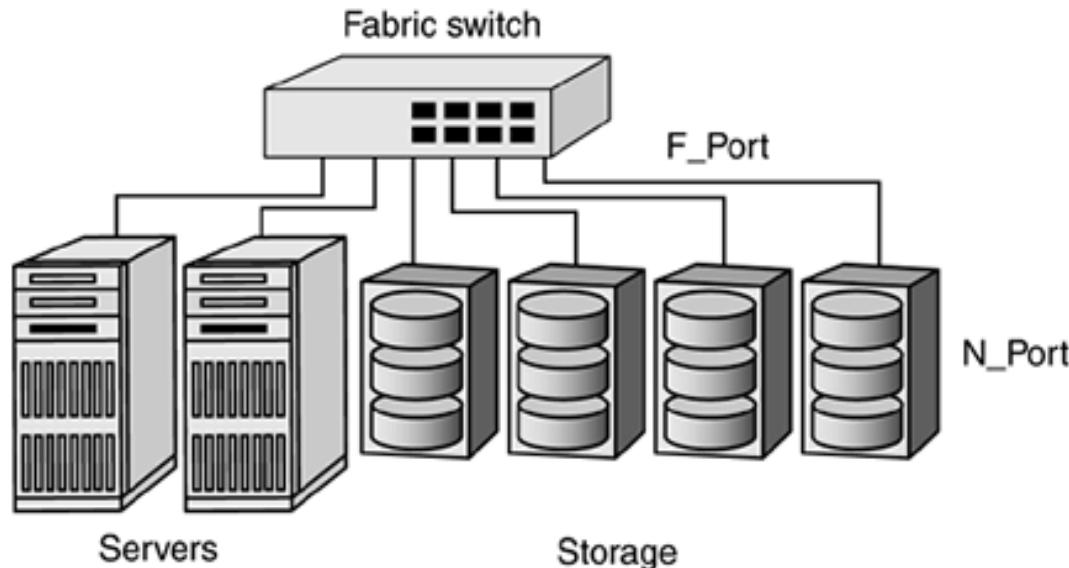
Tecnologia Fiber-Channel (FC)

Topologias disponíveis:



Tecnologia Fiber-Channel (FC)

Topologias do tipo *switch fabric*:



N_Port: porta de ligação de um nó FC ao switch

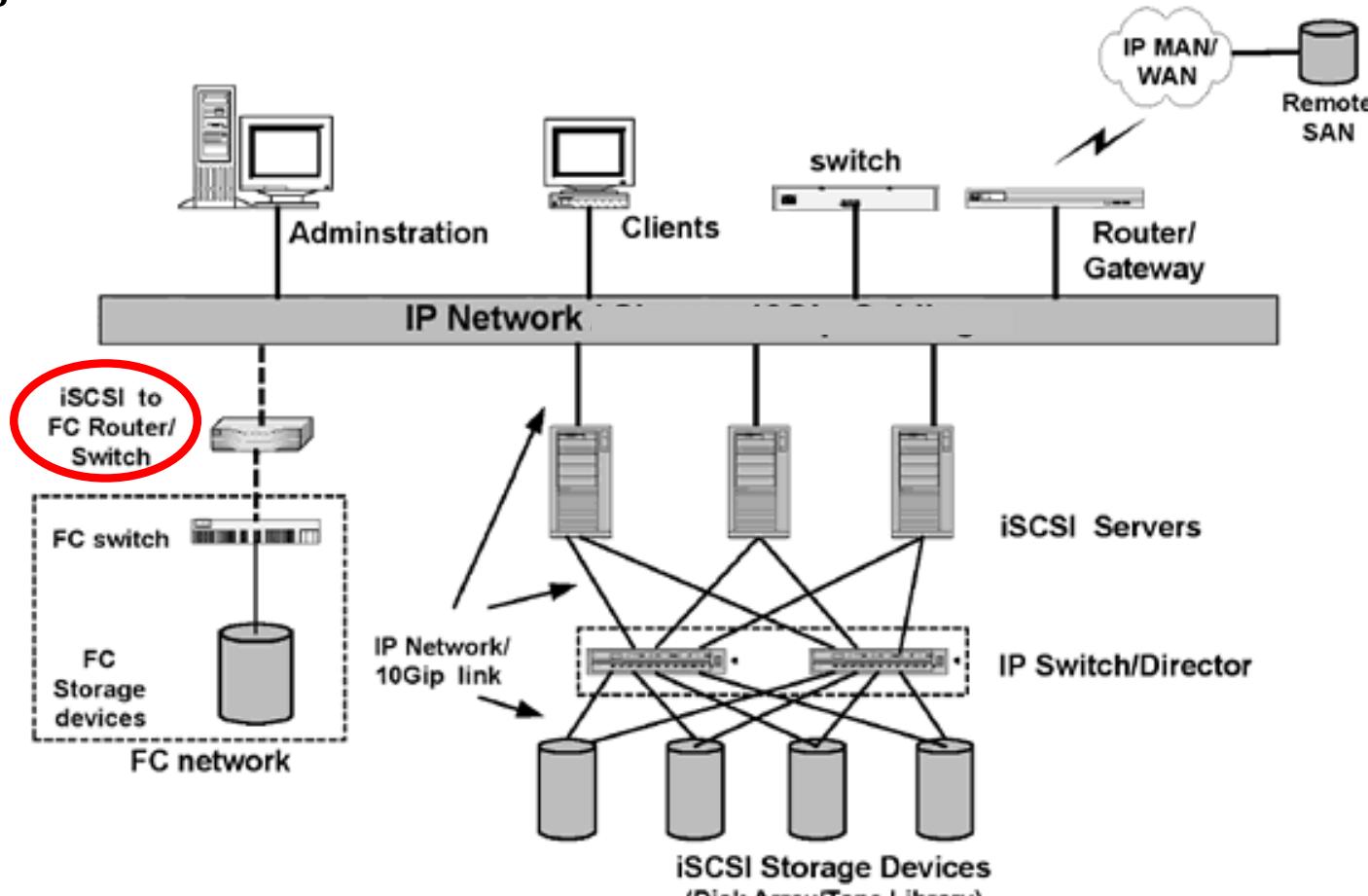
F_Port: porta do switch para ligar a um nó FC

L_Port: porta usada para ligação de um nó a um FC loop

NL_Port: porta de um nó para ligação simultânea a um loop FC e a um switch

Tecnologia Fiber-Channel (FC)

Integração FC - iSCSI



www.siemon.com/

Outras tecnologias

- ATA-over-Ethernet (AoE)
- InfiniBand (IB)
- Fibre Channel over Ethernet (FCoE)
- Fibre Channel over IP (FCIP)
- HyperSCSI - SCSI over Ethernet
- iSCSI Extensions for RDMA (iSER)
- Internet Fibre Channel Protocol (iFCP)
- Serial Storage Architecture (SSA – IBM)

Conclusões

- Necessidades de replicação de dados é cada vez maior
- Um exemplo claro de clusters de HA associada à necessidade de balanceamento de carga
- Storage distribuído e virtualizado tomou maior interesse com a cloud
- A seguir de perto: cloud providers (Google et al.) e Apache (Apache Ecosystem)

Bibliografia

- Marcus E, Stern H., “*Blueprints for high availability*”; 2003; Wiley; ISBN: 0471430269
- Luiz André Barroso, Jimmy Clidaras, Urs Holzle; “*The datacenter as a computer*”; Morgan and Claypool Editors; ISBN: 978-1627050098; 2013 [pdf]

Disaster recovery

1. Conceitos fundamentais
2. Noção de DRP
3. Sites partilhados

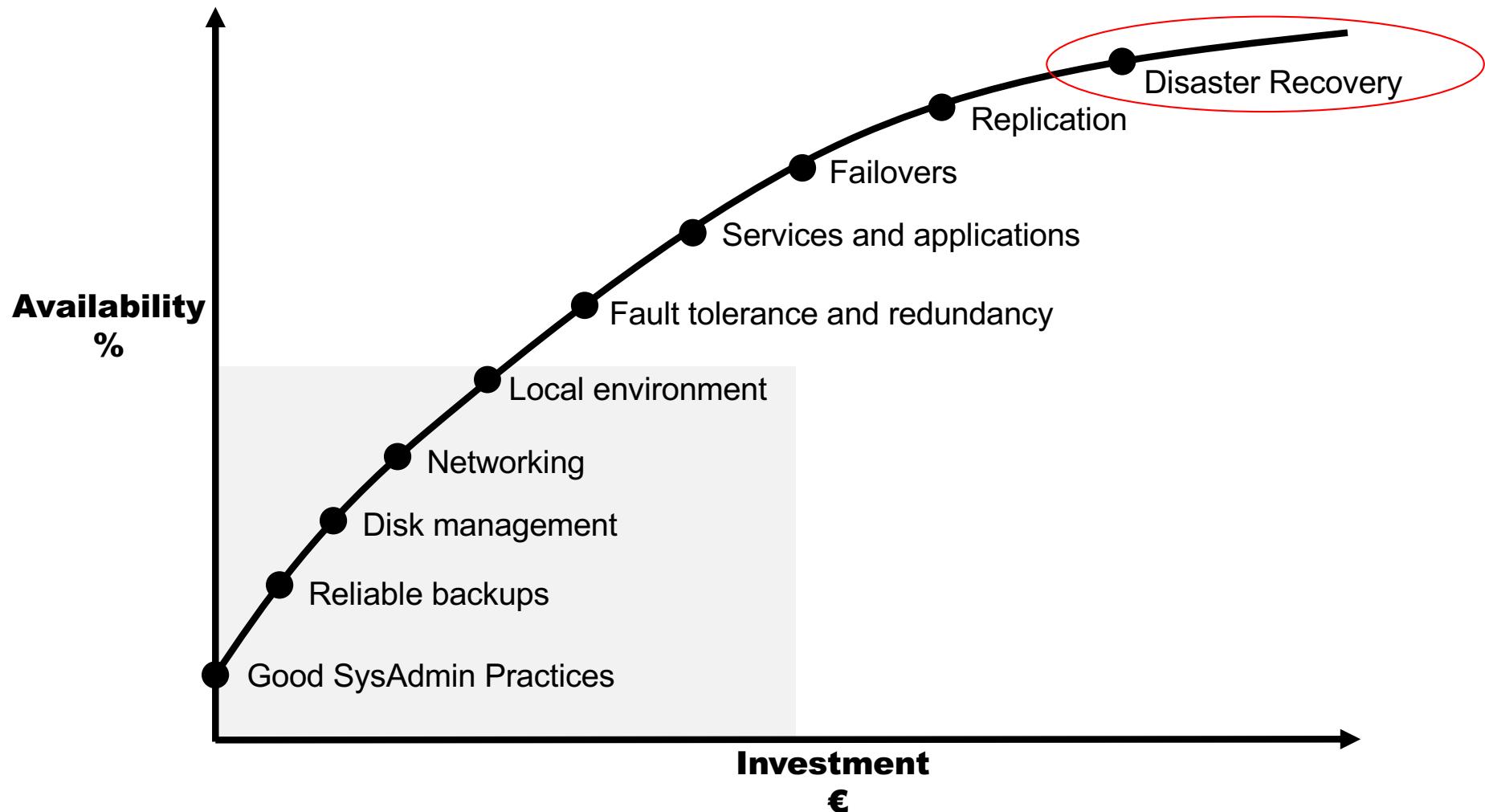
Enquadramento



www.disasterrecovery.org



Availability index

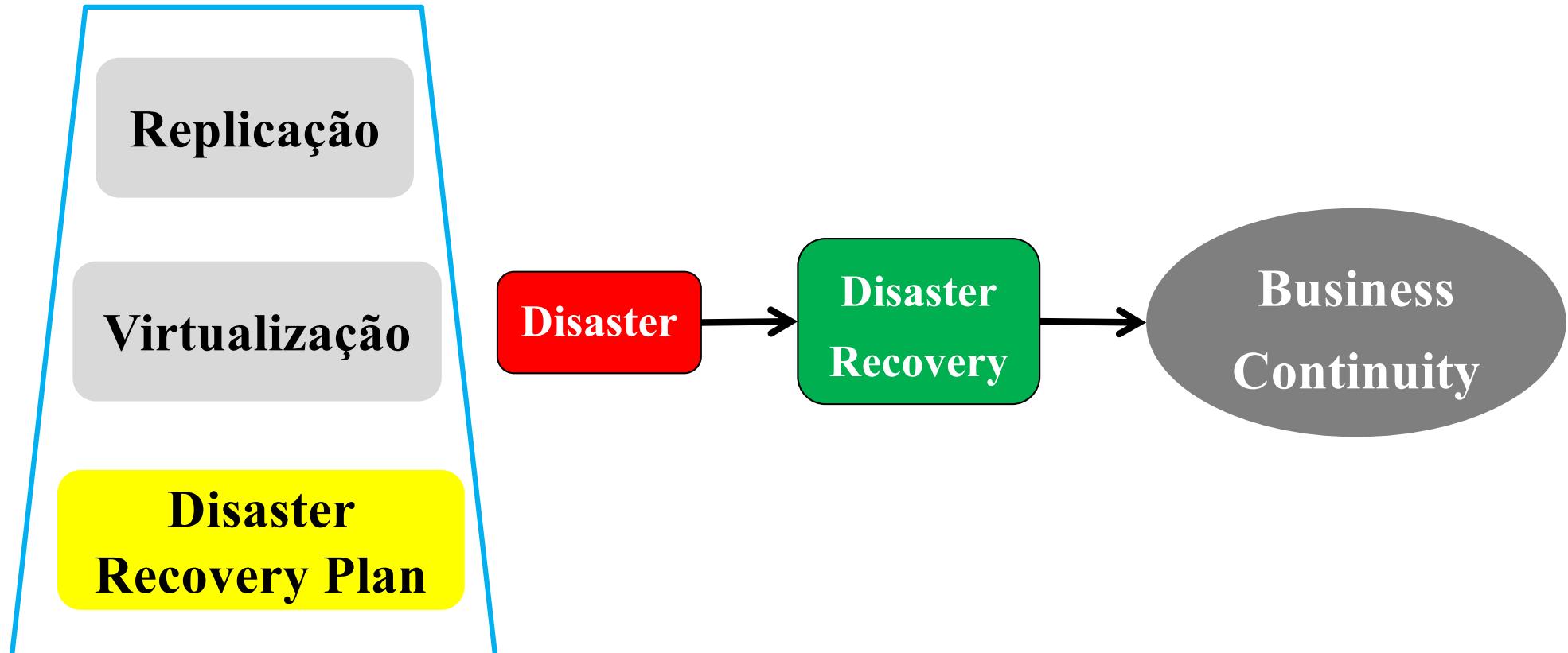


Adapted by Marcus E, Stern H., "Blueprints for high availability"; 2003; Wiley; ISBN: 0471430269;

Enquadramento

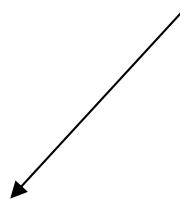


Enquadramento

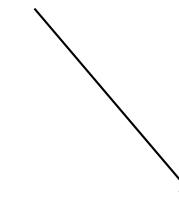


Business continuity and DR planning

Bussiness continuity ≠ Disaster Recovery



"Risks and threats to the ongoing availability of services, business functions and the organization are actively reviewed and managed at set intervals as part of the overall risk-management process."



"Is the process by which suitable plans and measures are taken to ensure that, in the event of a disaster, the business can respond appropriately with the view to recovering critical and essential operations in a little time possible."

The Official (ISC)2® Guide to the CCSPPSM CBK®, Second Edition
Adam Gordon; John Wiley & Sons, Inc, 2016 (pp.57)

Disaster recovery plan

Objetivos fundamentais de um DRP:

1. Proteger os funcionários
2. Assegurar sobrevivência da empresa, durante e após o desastre
3. Assegurar a continuidade da empresa e do negócio

Disaster recovery plan

Conteúdo de um plano de DRP

NIST - Special Publication 800-34, Contingency Planning for Information Technology Systems, ISO/IEC 24762, BS 25777

- Definir um “*contingency planning policy statement*”
- Definir um “*business impact analysis (BIA)*”
- Identificar medidas de controlo preventivas
- Desenvolver estratégias de recuperação
- Desenvolver um plano de contingência para as TI
- Testar, treinar ... testar, treinar ... testar, treinar ...
- Atualizar ... atualizar ... atualizar ... atualizar ...

Disaster recovery plan

Conteúdo de um plano de DRP

NIST - Special Publication 800-34, Contingency Planning for Information Technology Systems, ISO/IEC 24762, BS 25777

- Documentar e priorizar hw, sw e outros elementos
- Selecionar o site de DR
- Identificar pessoas chave, com posições críticas e correspondentes backups
- Criar e treinar equipas de resgate/emergência
- Implementar testes e exercícios práticos
- Atualização constante do plano

Disaster recovery plan

Business Impact Analysis (BIA)

Functional Area	Functional Name	Mail-zone	Risk Code F=Financial C=Customer R=Regulatory	Time Before Impact 0=week 2 or more 1=week 1 5=up to three days 10=day 1 20=4 hours 40=immediate	Customer Impact 0=none 1=Low 3=Med 5=High	Regulatory Impact 0=none 1=Low 3=Med 5=High	Financial Impact 0=none 1=0 to 10K 2=>10K but <100K 3=>100K but <500K 4=>500K but <1 Mil 5=>1 Mil	Rating Total Sum of I thru 4	Recovery Time Sensitivity Code	Alt. Site
Customer service	Call center	Z 45	C & F	40	5	1	3	49	AAA	Surviving sites then Smith Road
Customer service	Customer account maint.	Z 37	C	1	3	0	0	4	D	Work from home
Customer service	Customer monetary	Z 38	C & F & R	10	3	3	4	20	A	Smith Road

Exhibit 6.1 BIA Form.

Building an Enterprise-Wide Business Continuity Program; Kelley Okolita; 2009

Disaster recovery plan

Exemplos

- <http://searchdisasterrecovery.techtarget.com/>
 - <http://www.drj.com/resources/sample-plans.html>

<COMPANY NAME>		Business Continuity Plan
BC 030204... Key Suppliers and Vendors and Emergency Contact Information		
<small>(TO ACCESS GUIDELINES ON COMPLETING THIS PART OF THE BUSINESS CONTINUITY PLAN, CLICK HERE)</small>		
<p>Listed below are the organisation's key suppliers who may need to be contacted in the event of an emergency. In the event of these regular supplier not being able to provide the goods or services required in an emergency, an alternative list of suppliers has also been drawn up.</p>		
1. REGULAR SUPPLIERS		
NAME OF SUPPLIER	KEY GOODS OR SERVICES PROVIDED	NORMAL CONTACT DETAILS
2. ALTERNATIVE SUPPLIERS		
NAME OF SUPPLIER	KEY GOODS OR SERVICES PROVIDED	NORMAL CONTACT DETAILS
COMPLETED BY: NAME: _____ DATE: _____ REVIEWED BY: NAME: _____ DATE: _____		

- Documento assinado
 - Compromisso assinado
 - Vários templates disponíveis

Disaster recovery plan - preparação

- Identificar coordenador(es) do DRP e backups
- Identificar e priorizar (todas) as funções do negócio
- Identificar um site de DR
- Estimar o tempo aceitável de recuperação após falha
- Definir metodologia de backups (*onsite e offsite*)
- Definir modelo de distribuição de informação crítica (números de telefone, passwords, planos, ...)

Disaster recovery plan - preparação

- Definir equipas de recuperação
- Recolher informação específica e crítica sobre a rede
- Coligir informação confidencial
- Sinalizar fornecedores críticos
- Identificar outros serviços: p.e. apoio psicológico
- Disponibilizar treino contínuo do DRP para todos

Disaster recovery plan - preparação

Equipas de recuperação:

- Gestão de desastre
 - Comunicações
 - Recuperação de infraestrutura TI
 - Contacto com fornecedores
 - Análise de destruição
 - Interface com o negócio
 - Logística
-
- ```
graph LR; A["• Gestão de desastre
• Comunicações
• Recuperação de infraestrutura TI
• Contacto com fornecedores
• Análise de destruição
• Interface com o negócio
• Logística"] --> B["• Sistemas
• Rede
• Armazenamento
• Aplicações
• Dados"]
```

# Disaster recovery plan – escolha do site de DR

## 1. Localização física

- Acesso aos dados apenas através de uma única SAN?
- Ambos os sites partilham *facilities*?
- Próximo de serviços de saúde, bombeiros, etc...?
- Nível de *low-key* do site?
- Está bem dimensionado?
- Partilha de recursos para DR com outras companhias.

## 2. Segurança

- Regras de acesso ao equipamento (emergência declarada ou não)

## 3. Quanto tempo?

# Disaster recovery plan – modelo de distribuição

## 1. Restrito?

- Documento escrito apenas pelo(s) coordenador(es) do DRP e pelo(s) backups
- Cópia digital em vários sítios, com acesso controlado
- Coordenadores têm DRP da sua área/secção/departamento

## 2. Abrangente?

- Documento disseminado por papel e em formato digital, por todos os colaboradores

# Disaster recovery plan – conteúdo

- Contactos de telefone pessoais
- Passwords privilegiadas e regulares
- Procedimentos de emergência
- Hierarquia de contactos (1<sup>a</sup>linha, 2<sup>a</sup>linha, ...)
- Organograma da organização
- Localização física dos sites (alguns podem ser secretos)
- Informação proprietária sobre contactos de fornecedores, identificação de patentes e projetos em curso

Informação sensível que deve ser mantida em ambiente restrito.

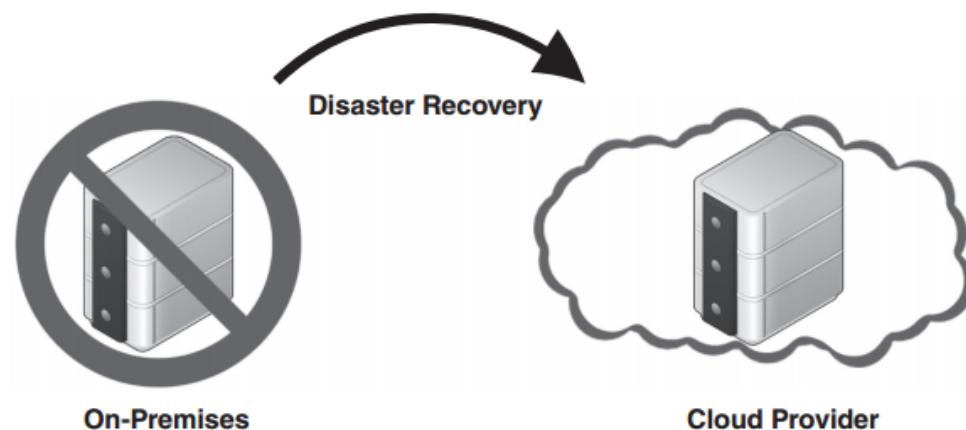
Prevenir fugas de informação através de colaboradores dispensados.

# Business continuity – cloud environment

**Domain 3**

## Characteristics of the cloud environment to consider in BCDR plan

### 1 On premises (local) and cloud as BCDR



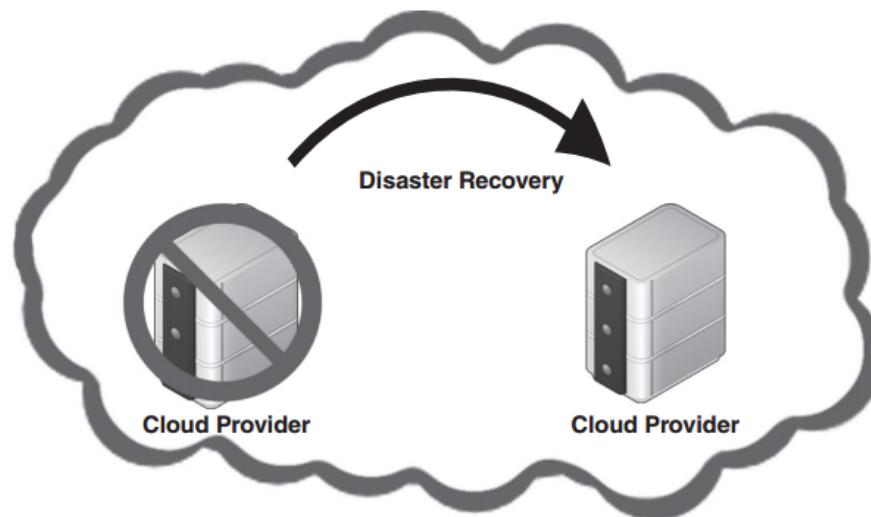
- Traditional failover strategy
- Endpoint is the cloud

# Business continuity – cloud environment

**Domain 3**

## Characteristics of the cloud environment to consider in BCDR plan

### 2 Cloud service consumer, primary provider BCDR



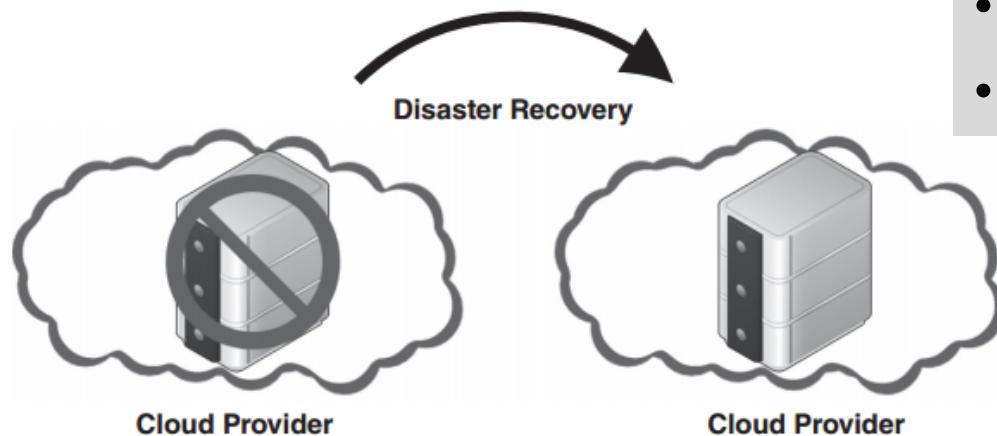
- Both sites are on a CSP
- ... in different regions

# Business continuity – cloud environment

**Domain 3**

## Characteristics of the cloud environment to consider in BCDR plan

### 3 Cloud service consumer, alternative provider BCDR



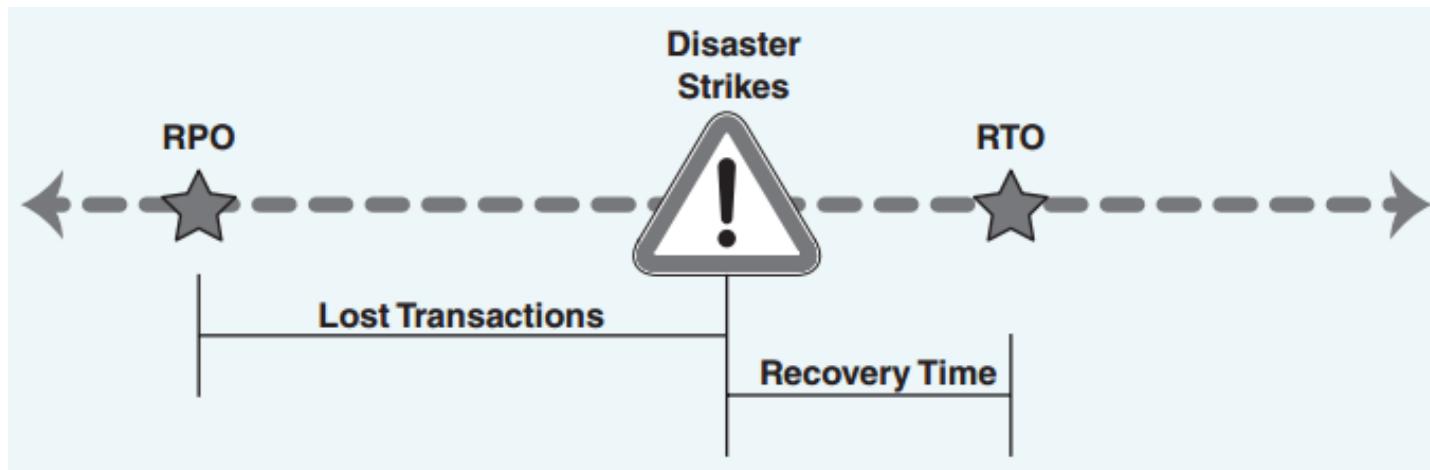
- Both sites are on different CSP
- Avoid risk of complete CSP failover

# Business continuity – business requirements

Domain 3

How much data can the company afford to lose?

How fast you need a system to be up and running after a disaster?



**RPO** = Recovery Point Objective

**RTO** = Recovery Time Objective

# Business continuity – BCDR strategy

- Is data sufficiently valuable for additional BCDR strategies?
- What is the required RTO?
- What is the required RPO?
- What “disasters” were included in the analysis?
- Does that include CSP failure?

How BCDR can differ in a cloud environment from the traditional approaches that exist in noncloud environments?

# Disaster recovery – main SLA components

1. SPoF should be all documented
2. Migration strategies to alternate providers should be possible
3. Alternate CSP should support all components in failover events
4. Controls should be enabled for data integrity
5. Users should select incremental backup settings
6. SLA should be revised at regular intervals

The Official (ISC)2® Guide to the CCSPSM CBK ®, Second Edition  
Adam Gordon; John Wiley & Sons, Inc, 2016 (pp.59)

# Disaster recovery – main SLA components

## ISO/IEC documents regarding SLA items:

- ISO/IEC DIS 19086-1, “Information Technology—Cloud Computing—Service Level Agreement (SLA) Framework—Part 1: Overview and Concepts”
- ISO/IEC NP 19086-2, “Information Technology—Cloud Computing—Service Level Agreement (SLA) Framework and Technology—Part 2: Metrics”
- ISO/IEC CD 19086-3, “Information Technology—Cloud Computing—Service Level Agreement (SLA) Framework and Technology—Part 3: Core Requirements”
- ISO/IEC AWI 19941, “Information Technology—Cloud Computing—Interoperability and Portability”
- ISO/IEC CD 19944, “Information Technology—Cloud Computing—Data and Their Flow Across Devices and Cloud Services”
- ISO/IEC FDIS 20933, “Information Technology—Distributed Application Platforms and Services (DAPS)—Access Systems”

The Official (ISC)2® Guide to the CCSPSM CBK®, Second Edition  
Adam Gordon; John Wiley & Sons, Inc, 2016 (pp.60)

# Disaster recovery plan – sites de DR partilhados

- |                                 |                                   |
|---------------------------------|-----------------------------------|
| 1. Experiência                  | ✗ Equipamento partilhado ...      |
| 2. Poupanças financeiras        | ✗ ... perda de controlo           |
| 3. Segurança remota             | ✗ Testes tornam-se mais complexos |
| 4. Atualização do DRP e do site |                                   |
| 5. Serviços extra               |                                   |

## DR site Partilhado *versus* dedicado

PME → site partilhado

Grandes instituições → site dedicado

# Disaster recovery plan – conclusões

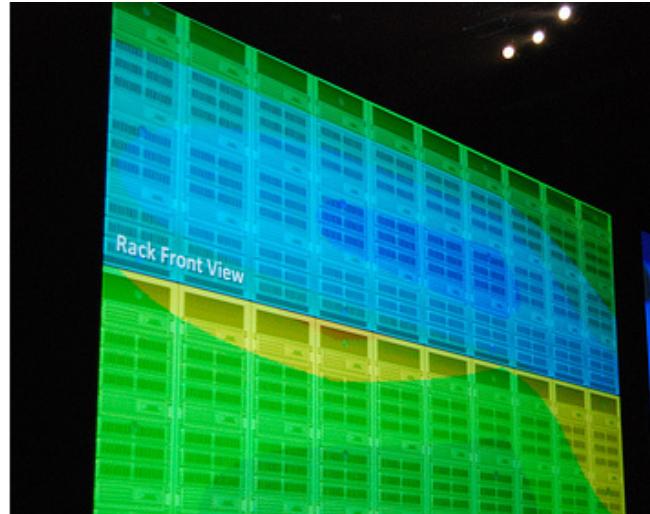
- Desenho e teste de um bom DRP implica uma redução no tempo de recuperação após desastre.
- DR pode ser (é!) complexo e sujeito a erros. Capacidade de olhar para os detalhes poderá minimizar complexidade e erros.
- Um bom DR depende de ... pessoas! Poderão colaborar mais ou menos, conforme o grau de motivação e entrosamento na companhia.

# Bibliografia

- Luiz André Barroso, Jimmy Clidaras, Urs Holzle; “The datacenter as a computer”; Morgan and Claypool Editors; ISBN: 978-1627050098; 2013 [pdf]
- Marcus E, Stern H., “*Blueprints for high availability*”; 2003; Wiley; ISBN: 0471430269

1. Noção de DCIM
2. Componentes principais monitorizados num DCIM
3. Protocolo SNMP
4. Noção de MIB
5. Principais aplicações

# Monitorização



# Monitorização

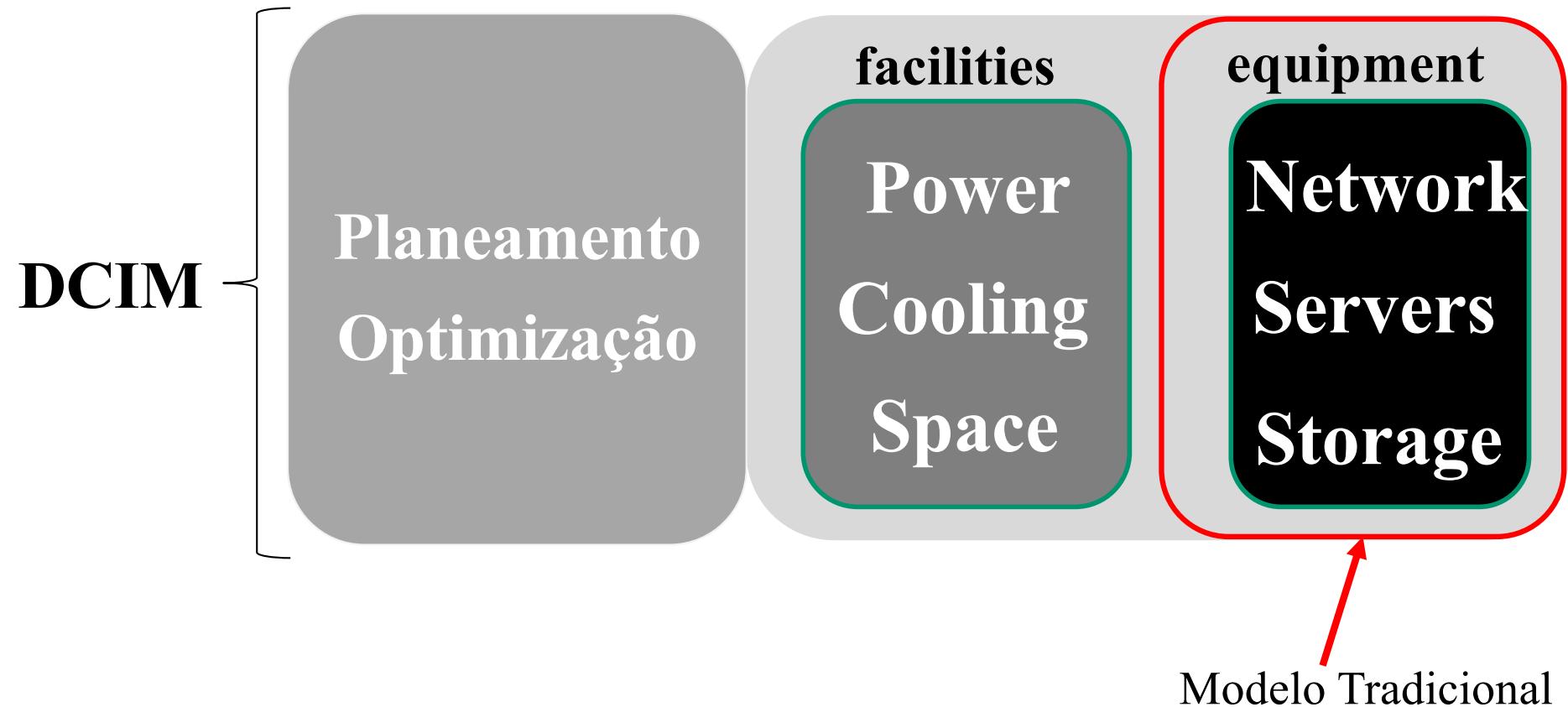


# Monitorização – modelo tradicional

- Monitorizar indicadores típicos de um sistema (espaço disco, alarmes, latência da rede, medidas de desempenho,...)
- Aplicações específicas para cada uma das áreas monitorizadas.
- Modelo focado no hardware (avarias de componentes) e com vista à deteção de downtime e medição de disponibilidade.
- Várias aplicações de monitorização com pouca integração
- Exemplos: Nagios para monitorização de computadores

# Monitorização - DCIM

## Data Center Infrastructure Monitoring



# Monitorização – objetivos

- Monitorizar todos os componentes do DC
- Adquirir uma visão integrada do DC
- Obter informação que permita planear e organizar o DC
- Medir Service Level Agreement (SLA) e Operational Level Agreement (OLA)
- Validar se Service Level Requirement (SLR) estão a ser integralmente considerados no SLA.

# Monitorização – componentes

## O que há de novo no DCIM?

- Inventário (*asset tracking and lifecycle management*)
- Gestão e planeamento da capacidade (global e por componente)
- Gestão de mudanças de equipamentos
- Gestão de virtualização e relação com equipamento físico
- Gestão de *utilities* (energia, AVAC, eficiência e estimativa de custos)
- Gestão de recursos e localização
- Monitorização *multi-layered*
- Planeamento futuro e modelação de cenários

# Monitorização – KPI e KRA nas facilities

Facility KRA

Infrastructure monitoring & health check

Scheduled & Preventive Maintenance

Incident and Problem Management

Maintaining Energy efficiency

Uptime Reporting

Facility KPIs

<http://www.greenfieldsoft.com/>

# Monitorização – KPI e KRA nas TI

## KRA: Data Center IT Staff

IT KRA

IT Monitoring

IT Hardware Maintenance

IT Asset Management

IT Vendor/Contract Management

Business Continuity

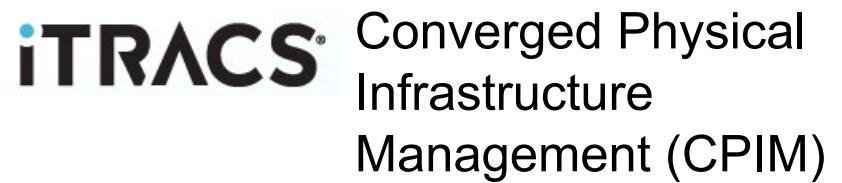
Reporting

IT KPIs

<http://www.greenfieldsoft.com/>

# Monitorização – aplicações DCIM

Figure 1. Magic Quadrant for Data Center Infrastructure Management Tools



# Monitorização – Benchmarking na cloud

**Testar serviço prestado por fornecedores de cloud:**

- Largura de banda fornecida
- Latência de rede
- Operações em disco
- Operações em memória
- Operações em CPU
- Preço

Objetivo: comparar o serviço prestado por vários IaaS

# Monitorização – Benchmarking na cloud

- Cloud Spectator – [www.cloudspectator.com](http://www.cloudspectator.com)
- Cloud Harmony – [www.cloudharmony.com](http://www.cloudharmony.com)
- Cloud Sleuth – [www.cloudsleuth.com](http://www.cloudsleuth.com)
- Server Bear – [www.serverbear.com](http://www.serverbear.com)

# Monitorização – aplicações DCIM – open source

- Aplicações de monitorização baseadas em SNMP
- Monitorização global baseada em SNMP e execução de scripts remotos.



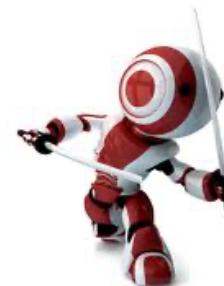
<http://www.snmp.com/>

**Nagios®**



**ZABBIX**

**Zenoss™**



Shinken

# Monitorização – aplicações DCIM – open source

## RackTables

<http://racktables.org>

The screenshot displays the RackTables application interface, which is a web-based tool for managing data center infrastructure. The top navigation bar includes links for 'Rackspace', 'Objects', 'IPv4 space', 'Files', and 'Reports'. A search bar is also present. Below the navigation, there are twelve icons representing different management functions:

- Rackspace:** Represented by a server rack icon.
- Objects:** Represented by a server icon with a cursor pointing at it.
- IPv4 space:** Represented by a vertical stack of IP address blocks.
- IPv6 space:** Represented by a vertical stack of IP address blocks.
- Files:** Represented by a folder icon.
- Reports:** Represented by a line graph icon.
- IP SLB:** Represented by a stack of server icons.
- 802.1Q:** Represented by a network switch icon connected to four clouds.
- Configuration:** Represented by wrench and screwdriver icons.
- Log records:** Represented by a scroll icon.
- Virtual Resources:** Represented by three colored cubes (blue, red, green).
- Patch cables:** Represented by a bundle of colored patch cables.

A URL bar at the bottom shows the address: [demo.racktables.org/index.php?page=depot](http://demo.racktables.org/index.php?page=depot).

# Monitorização - SNMP

1. Gestão proativa
2. Protocolo SNMP
3. Noção de MIB
4. Noção de SMI

# Enquadramento

## Gestão de rede proactiva

- Analisar a rede durante o período normal
- Identificar problemas e ...
- ... planear *downtime* (intervenções e upgrade)

## Processos

- Gestão de:
  - Falhas
  - Configuração
  - Accounting*
  - Performance*
  - Segurança



## Arquitecturas

- In-band / out-band
- centralizada / distribuída

## Protocolos

- **SNMP**
- RMON
- NetFlow
- WMI

# Enquadramento - Funções

- Monitorização da disponibilidade da infraestrutura de DC
- Automatização do processo de gestão
- Monitorização do tempo de resposta da rede
- Confronto com o contracto de nível de serviço definido
- Segurança
- Reencaminhamento do tráfego
- Reposição dos serviços de rede em caso de falha
- Gestão de utilizadores

# Gestão proactiva

- **Verificar o estado da rede em operação normal**
- **Permite:**
  - Identificar potenciais problemas
  - Optimizar a *performance*
  - Planear actualizações (software e hardware)
- **Medições de rotina e definição de relatórios periódicos:**
  - Analisar tendências
  - Planear alterações
  - Comparar com os níveis de serviços acordados

# Tráfego originado por tarefas de gestão

Para estimar o tráfego gerado é importante definir:

- protocolos de gestão envolvidos
- redes e equipamentos geridos ( $N_d$ )
- informação de gestão recolhida ( $N_c$ )
- frequência de *polling* ( $P$ )

$$\text{Tráfego} = \frac{N_d \cdot N_c}{P}$$

# Tráfego originado por tarefas de gestão

## Exemplo:

- 200 equipamentos
- 10 características/equipamento
- *Polling* de 5 segundos
- Pedidos e respostas =  $2 \times (200 \times 10) = 4000$  operações
- Cada Pedido/Resposta = 64 bytes

$$4000 \times 64 \times 8 = 2048000 \text{ bits/5 segundos} \quad \boxed{409600 \text{ bps}}$$

# Arquitecturas de gestão de rede

## SNMP - TCP/IP

- A gestão deve ser simples
- Abordagem orientada à variável
- A troca de informação de gestão pode fazer-se sobre protocolos sem confirmação (UDP)

## CMIP / CMOT - OSI

- A gestão deve ser poderosa
- Abordagem orientada a objectos
- A troca de informação de gestão deve fazer-se sobre protocolos com confirmação (e.g. TCP)

## TMN - Redes de telecomunicações (SDH, ATM, FR, ...)

- É definida apenas a arquitectura de gestão
- Os protocolos usados são os propostos pelo OSI
- A gestão é feita *out-of-band* (*overlay network*)

# SNMP

- Simple Network Management Protocol
- Standard *de facto* para gestão de redes
- Protocolo para gestão de redes TCP/IP e equipamento activos (routers, switches,...)
- Componentes → gestor e agentes
- Protocolo baseado em pedido → resposta  
Mensagens do tipo GET, SET e TRAP

# SNMP - *Simple Network Management Protocol*

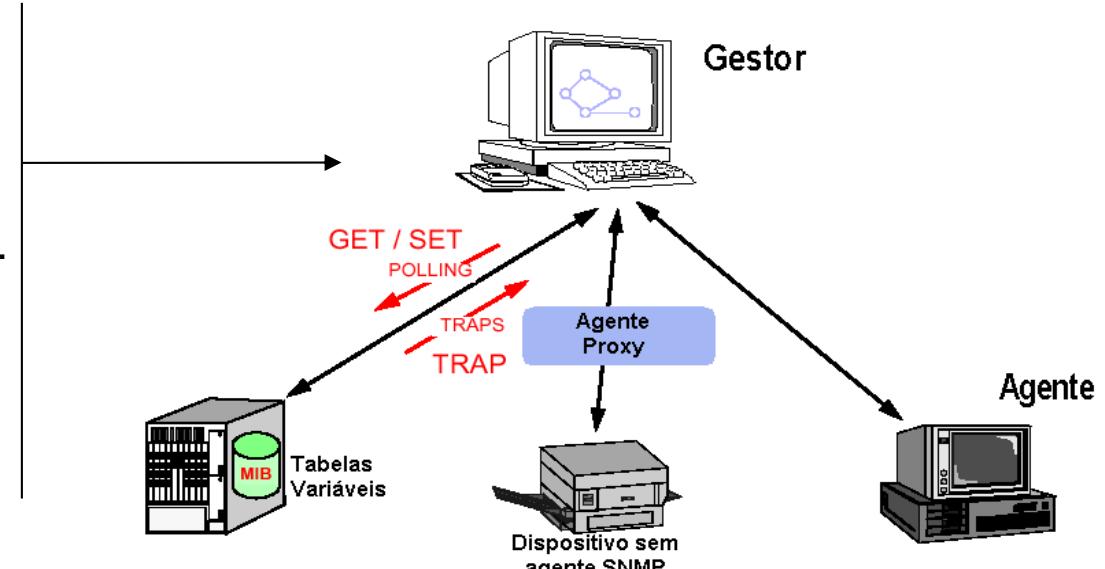
## Gestor → Agente/proxy SNMP

**Get** - Consulta de uma variável da MIB.

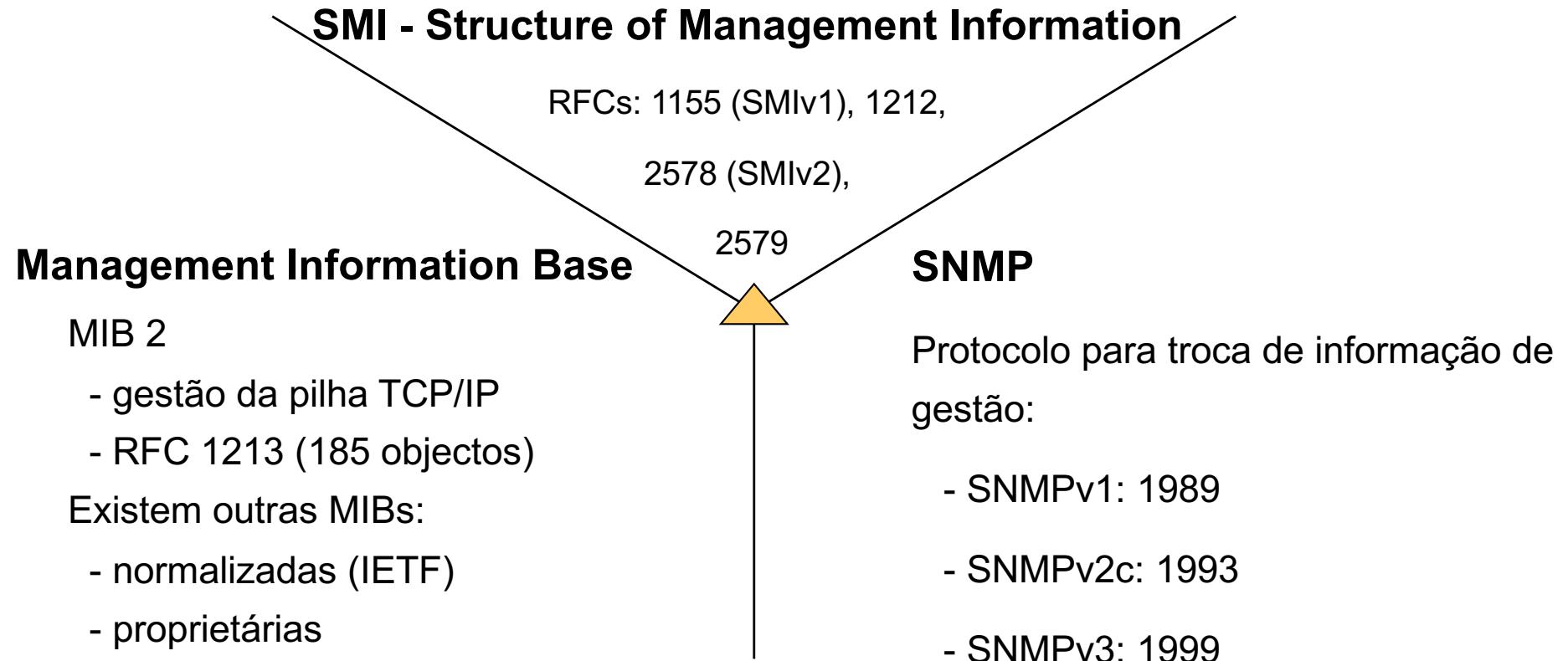
**Set** - Alteração de uma variável da MIB.

## Agente/proxy SNMP → Gestor

**Trap** - Notificação de um evento.

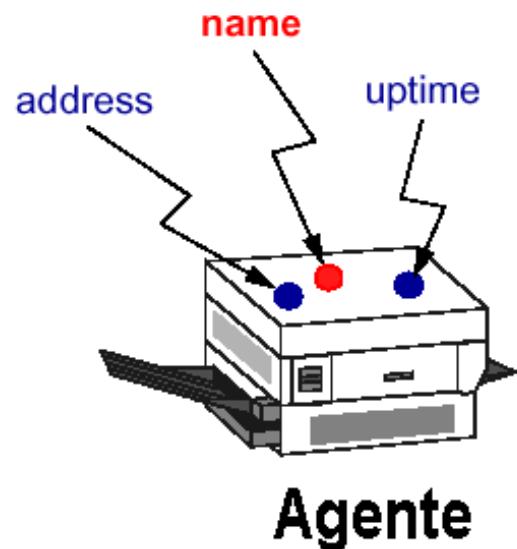


# Componentes do SNMP

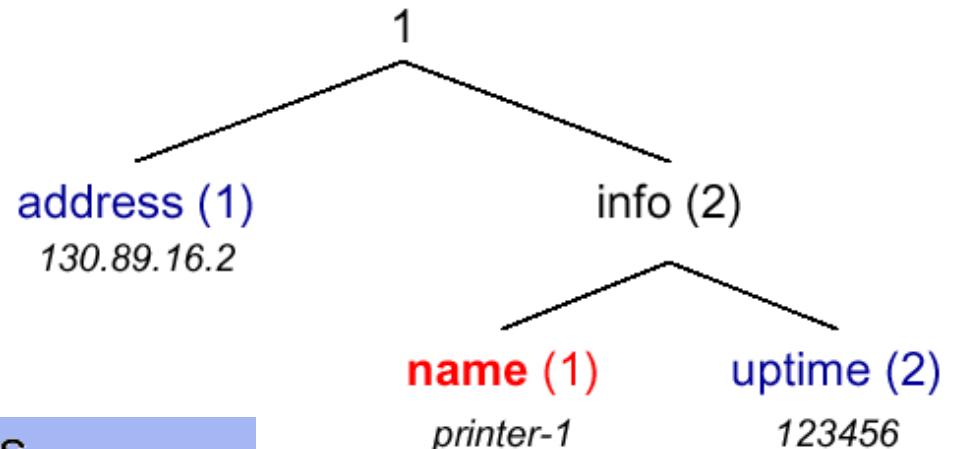


# *Structure of Management Information (SMI)*

- Informação é guardada em tipos de dados escalares
- Todas as variáveis têm identificador: OID – *Object Identifier*
- Cada variável possui um tipo de dados
- Um instância da variável possui um valor

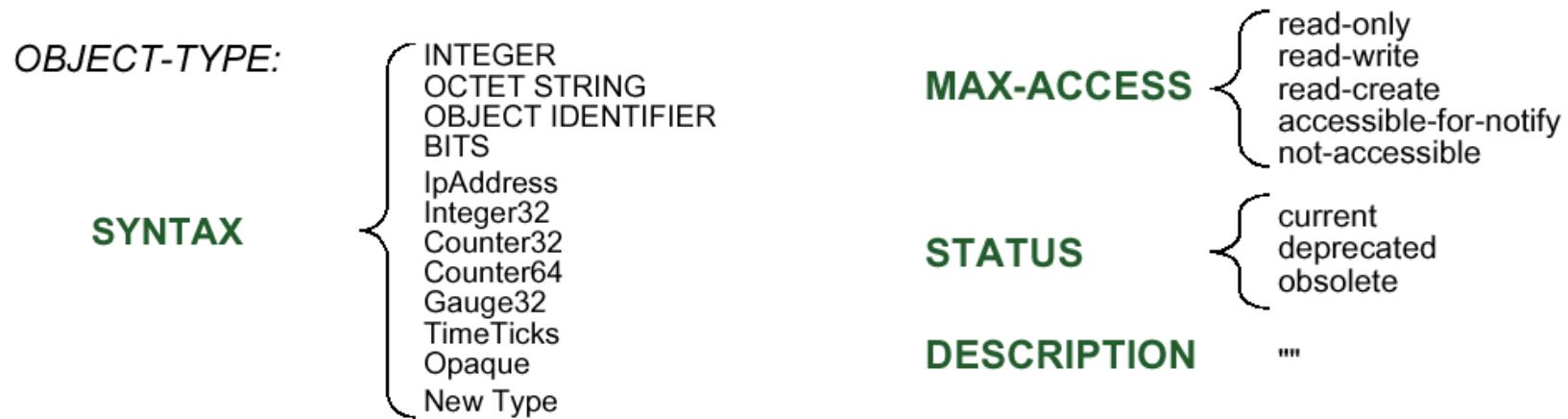


• address  
Object ID = 1.1  
Object Instance = 1.1.0  
Value of Instance = 130.89.16.2



# *Structure of Management Information (SMI)*

## Definição formal dos objectos de gestão



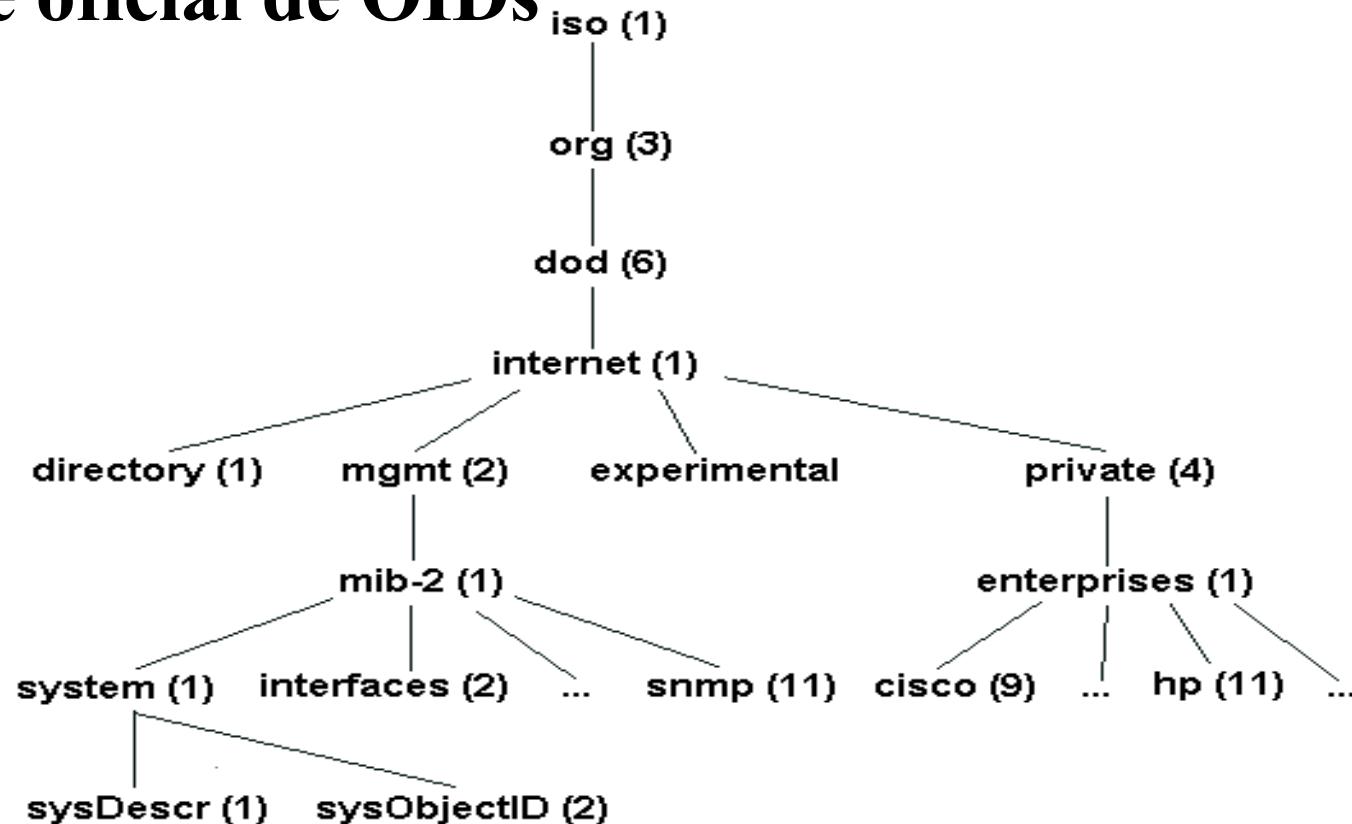
-- Definition of address

address **OBJECT-TYPE**  
**SYNTAX** ipAddress  
**MAX-ACCESS** read-write  
**STATUS** current  
**DESCRIPTION** "The Internet address of this system"  
**::= {NEW-MIB 1}**

Abstract Syntax  
Notation One (ASN.1)

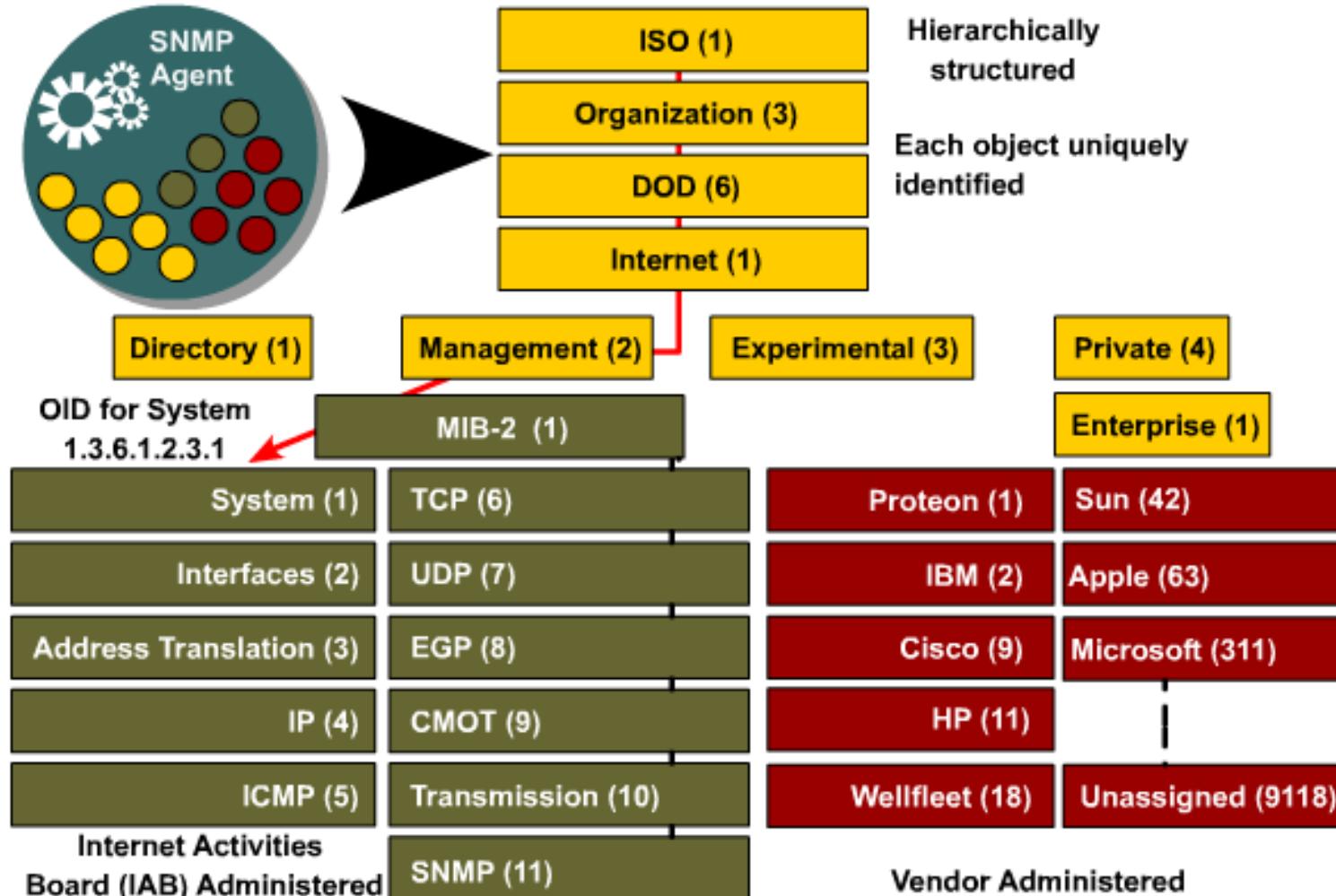
# *Structure of Management Information (SMI)*

## Árvore oficial de OIDs



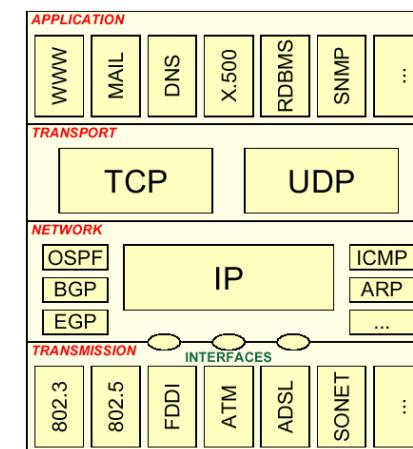
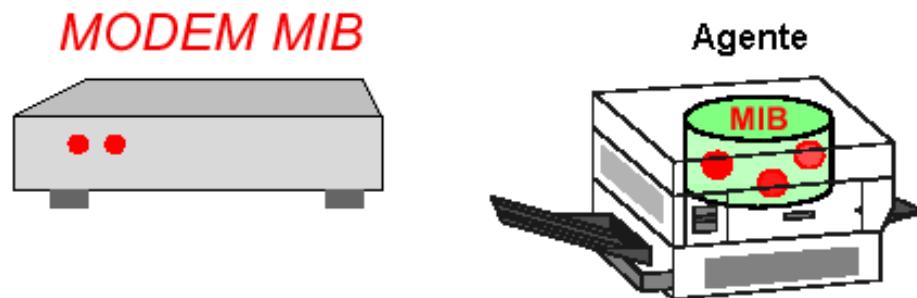
`.iso.org.dod.internet.mgmt.mib-2.system.sysDescr ≡ .1.3.6.1.2.1.1.1`

# *Structure of Management Information (SMI)*



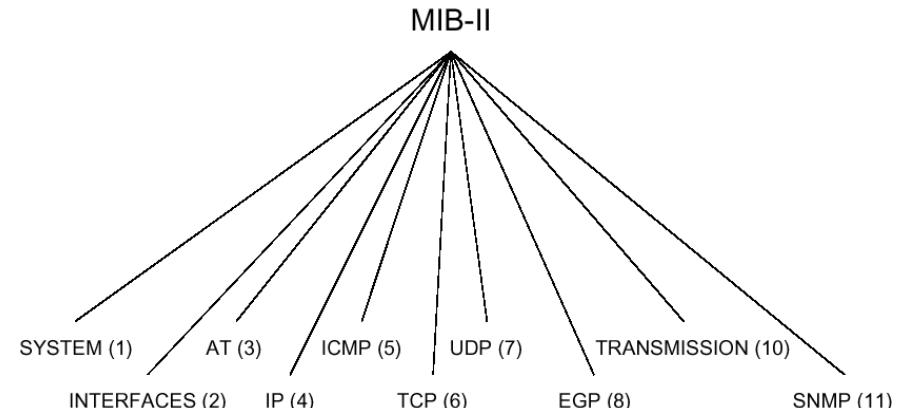
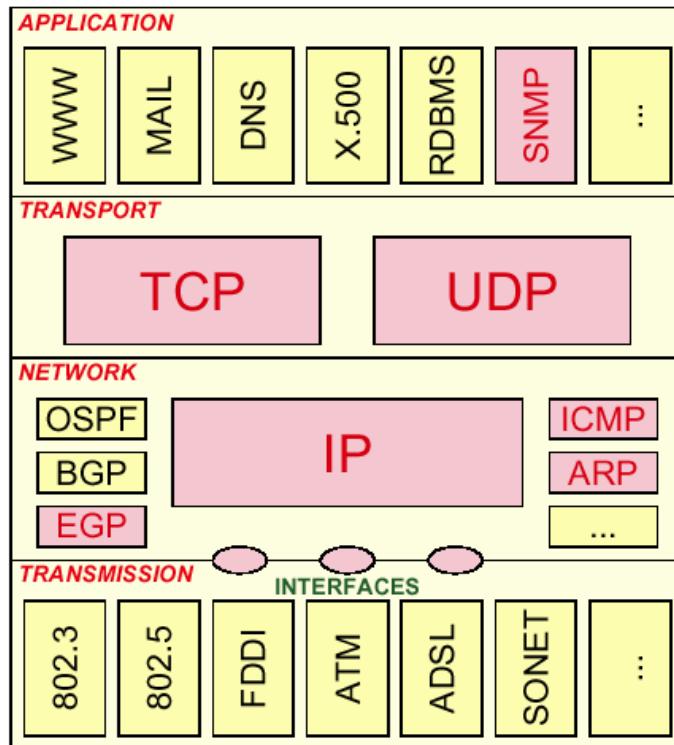
# *Management Information Base (MIB)*

- Repositório de objectos de gestão que representam recursos a gerir (observar ou controlar)
- A composição da MIB tem que ser conhecida pelo fabricante do objecto gerido e pelo Gestor do equipamento
- As MIBs podem evoluir (flexibilidade) e ser definidas por várias equipas independentes (modularidade)



# *Management Information Base (MIB)*

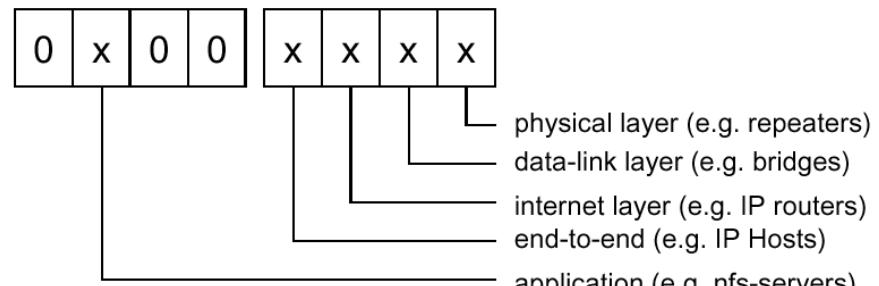
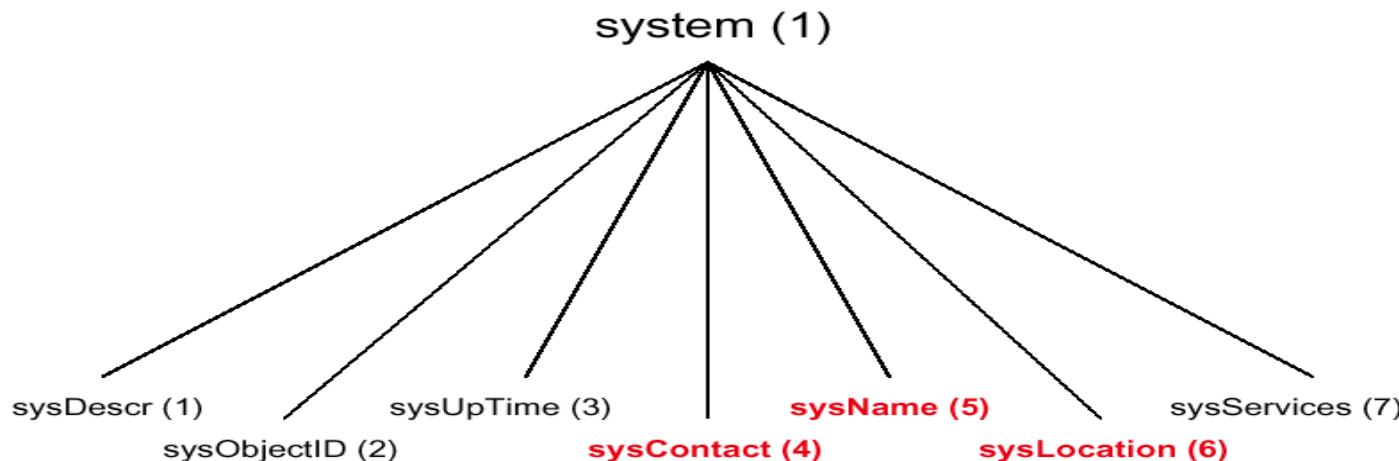
## Gestão da pilha protocolar TCP/IP - MIB II (RFC 1213)



# *Management Information Base (MIB)*

- Gestão da pilha protocolar TCP/IP - MIB II (RFC 1213)

## Grupo *System*(1)

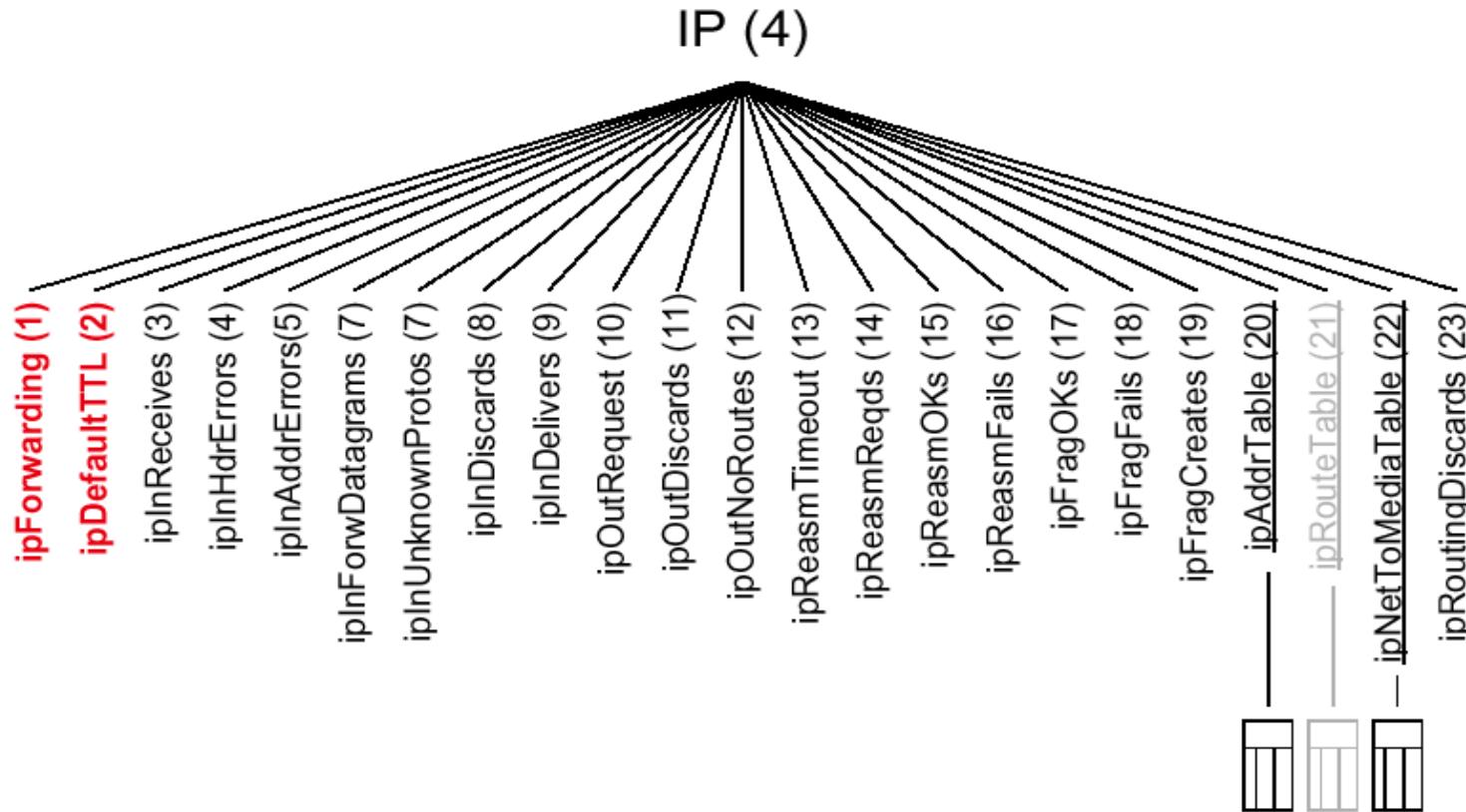


|              |                                                         |
|--------------|---------------------------------------------------------|
| sysDescr:    | <b>"Cisco Gateway"</b>                                  |
| sysObjectID: | <b>1.3.6.1.4.1.9.1.1</b>                                |
| sysUpTime:   | <b>37153422</b> ( <i>4 days, 7 h, 12 min, 14.22 s</i> ) |
| sysContact:  | <b>"helpdesk@cs.utwente.nl"</b>                         |
| sysName:     | <b>"utic01.cs.utwente.nl"</b>                           |
| sysLocation: | <b>"near logica meeting room"</b>                       |
| sysServices: | <b>6</b> ( <i>bridge and router functions</i> )         |

# *Management Information Base (MIB)*

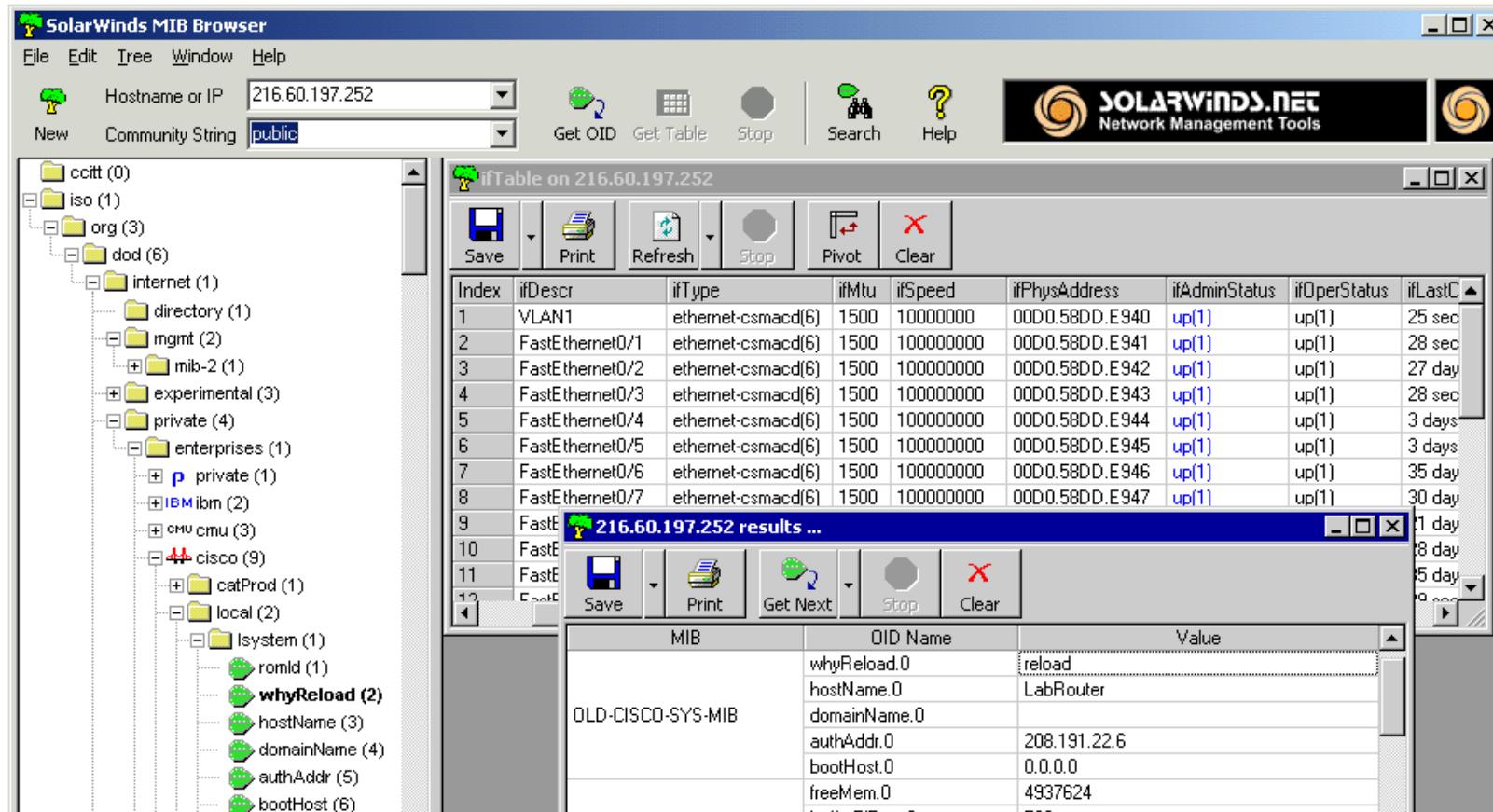
- Gestão da pilha protocolar TCP/IP - MIB II (RFC 1213)

## Grupo *IP(4)*

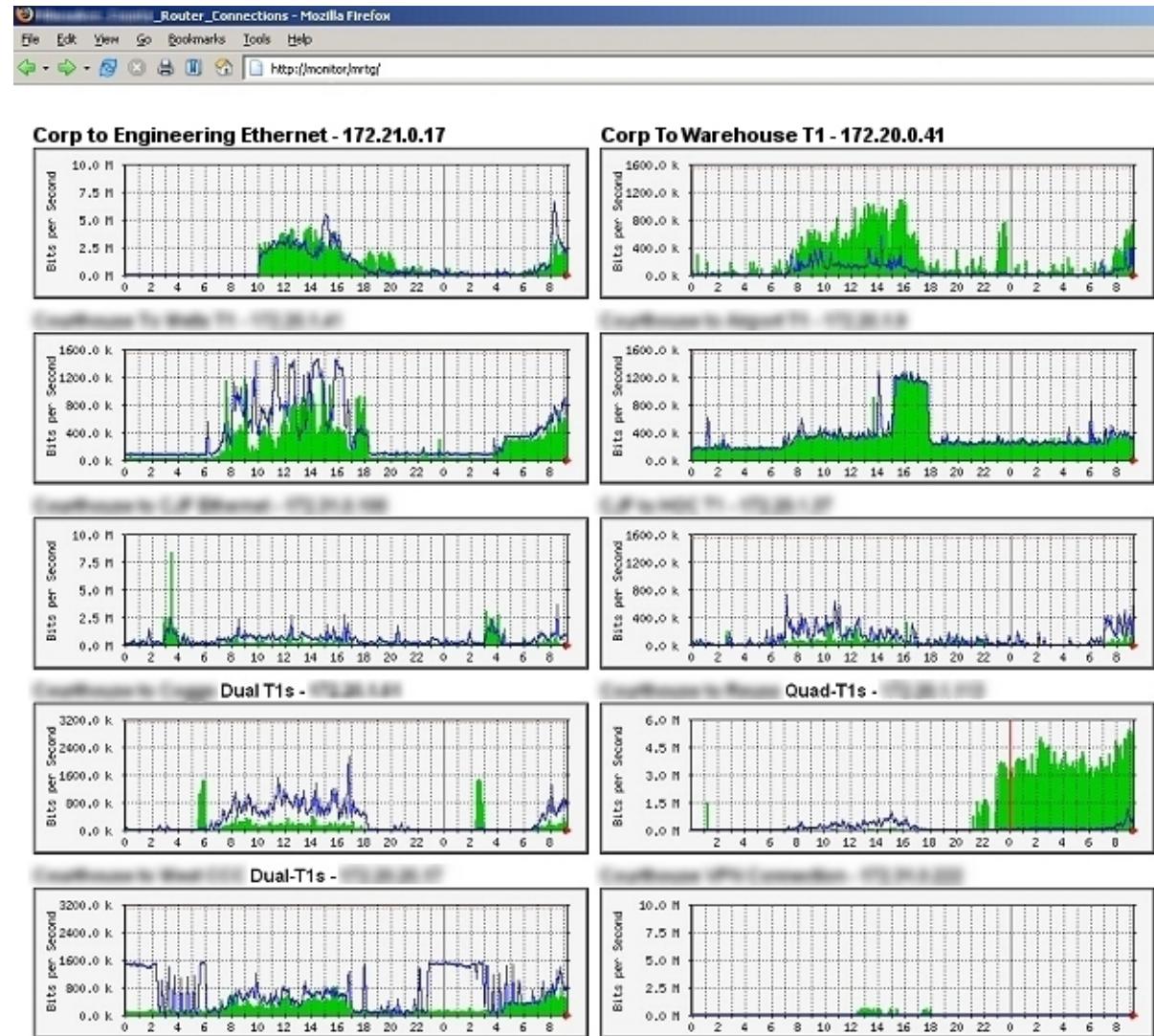


# Management Information Base (MIB)

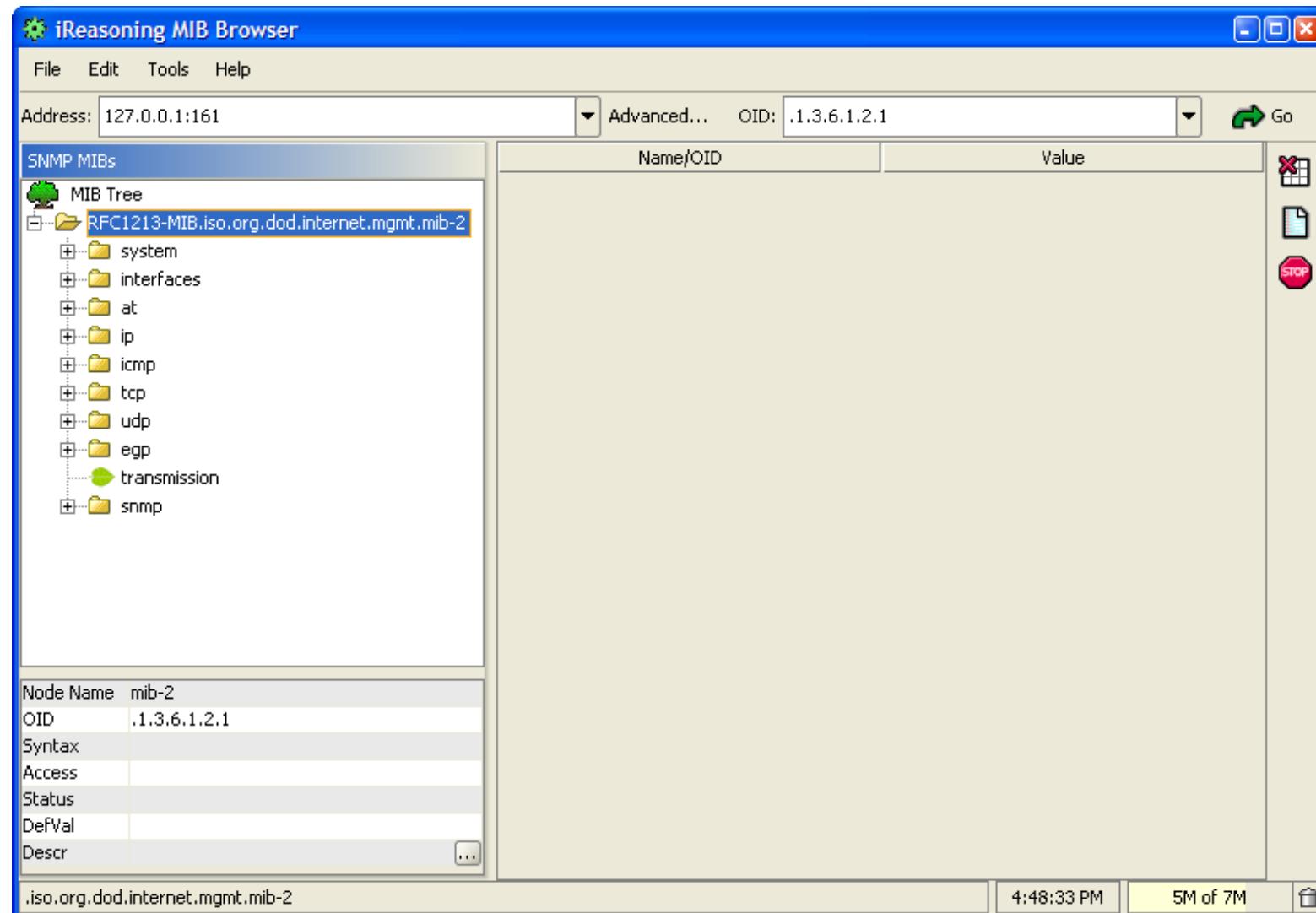
## Visualização num MIB Browser



# SNMP Tools - MRTG



# MIB browser - iReasoning



# snmpd

## Instalar

```
sudo apt-get install snmpd
sudo apt-get install snmp
```

## Configurar /etc/snmp/snmpd.conf

```
rocommunity public
syslocation "Local"
syscontact contacto@mail.net
SNMPDOPTS=' -Lsd -Lf /dev/null -u snmp -I -smux -p
 /var/run/snmpd.pid -c /etc/snmp/snmpd.conf'
```

## Iniciar

```
sudo service snmpd restart
```

**Testar:** snmpwalk -v 1 -c public -O e localhost

# nagios3

## Instalar

```
sudo apt-get install nagios3 nagios-nrpe-plugin
sudo apt-get install nagios-nrpe-server
```

## Configurar

/etc/nagios

/etc/nagios-plugins:

### Configuração no Ubuntu:

<https://help.ubuntu.com/lts/serverguide/nagios.html>

## Iniciar

```
sudo /etc/init.d/nagios3 restart
```

```
sudo /etc/init.d/nagios-nrpe-server restart
```

# nagios3

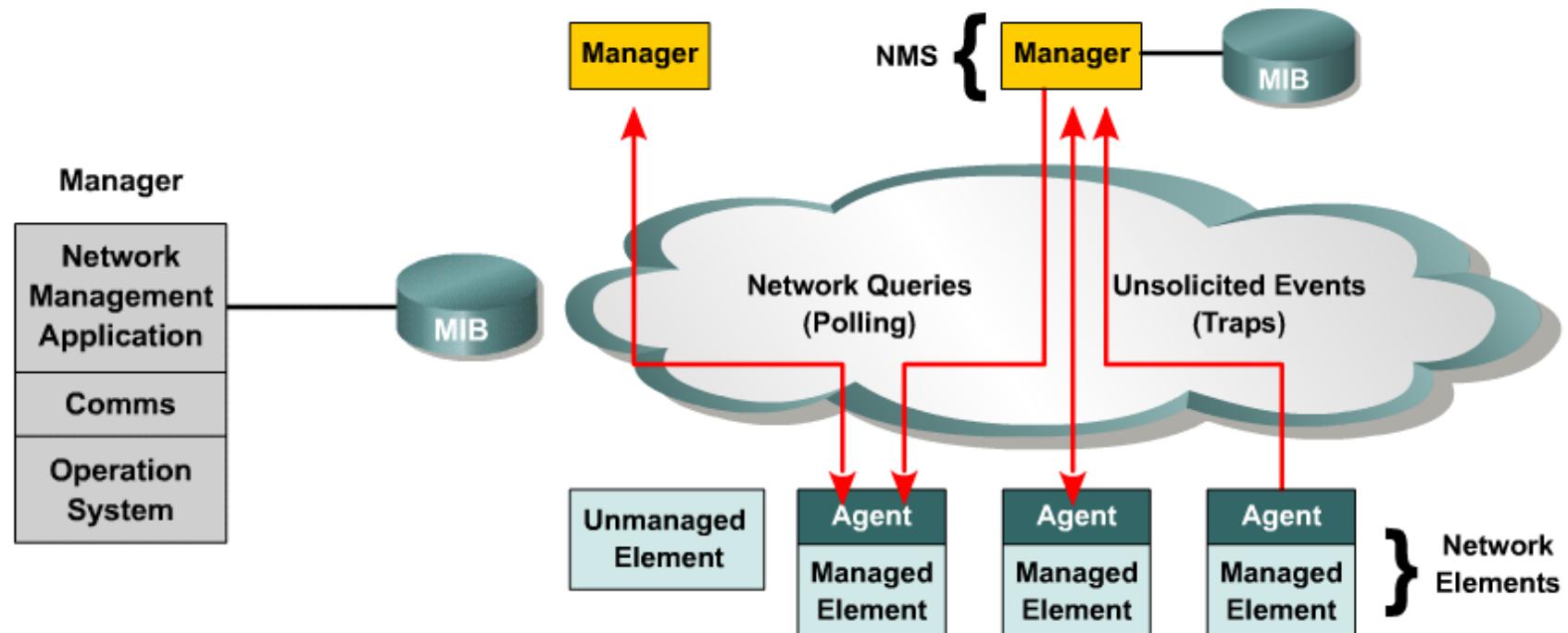
Acesso remoto: <http://server/nagios3>

The screenshot shows the Nagios 3 web interface running in Microsoft Internet Explorer. The left sidebar contains navigation links for General, Monitoring, Service Problems, Reporting, and Configuration. The main content area displays the 'Current Network Status' with last update information and a log-in message for 'binger'. It features three summary boxes: 'Host Status Totals' (Up: 15, Down: 2, Unreachable: 0, Pending: 0), 'Service Status Totals' (OK: 29, Warning: 1, Unknown: 1, Critical: 4, Pending: 0), and 'Service Status Details For All Hosts'. The 'Service Status Details For All Hosts' table lists various hosts and their services with their current status, last check time, duration, attempt count, and status information. Two specific entries are circled in red: 'Terminalserver Sessions' and 'if-traffic'. The 'Terminalserver Sessions' entry shows a warning status with a yellow background, while 'if-traffic' shows a critical status with a red background.

| Host           | Service                 | Status               | Last Check          | Duration            | Attempt         | Status Information                                                |                                                                                            |
|----------------|-------------------------|----------------------|---------------------|---------------------|-----------------|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| bart           | Diskusage C:            | OK                   | 2004-07-06 11:10:19 | 20d 0h 7m 26s       | 1/3             | C:\ - total: 3.91 Gb - used: 2.62 Gb (67%) - free 1.28 Gb (33%)   |                                                                                            |
|                | Diskusage D:            | WARNING              | 2004-07-06 11:14:13 | 20d 0h 7m 20s       | 3/3             | D:\ - total: 29.99 Gb - used: 26.78 Gb (89%) - free 3.20 Gb (11%) |                                                                                            |
|                | HTTP                    | OK                   | 2004-07-06 11:21:41 | 14d 1h 37m 47s      | 1/3             | HTTP ok. HTTP/1.1 200 OK - 0.027 second response time             |                                                                                            |
|                | MS-Exchange             | OK                   | 2004-07-06 11:20:58 | 20d 0h 8m 6s        | 1/3             | All services are running                                          |                                                                                            |
|                | SMTP                    | OK                   | 2004-07-06 11:21:33 | 22d 1h 53m 13s      | 1/3             | SMTP OK - 0 second response time                                  |                                                                                            |
| cixten         | Diskusage C:            | Nagiosstat goes here | 2004-07-06 11:19:45 | 0d 22h 2m 24s       | 1/3             | C:\ - total: 39.06 Gb - used: 8.01 Gb (21%) - free 31.05 Gb (79%) |                                                                                            |
|                | Terminalserver Sessions | OK                   | 2004-07-06 11:18:01 | 0d 22h 29m 13s      | 1/3             | 11                                                                |                                                                                            |
|                | ftp.sunet.se            | PING                 | OK                  | 2004-07-06 11:21:30 | 0d 0h 31m 24s   | 1/10                                                              | PING OK - Packet loss = 0%, RTA = 36.37 ms                                                 |
|                | haubits                 | PING                 | OK                  | 2004-07-06 11:21:21 | 193d 8h 33m 3s  | 1/10                                                              | PING OK - Packet loss = 0%, RTA = 1.36 ms                                                  |
|                | itknsqwl                | PING                 | OK                  | 2004-07-06 11:21:21 | 56d 22h 30m 57s | 1/10                                                              | PING OK - Packet loss = 0%, RTA = 6.10 ms                                                  |
| lisper         | if-traffic              | OK                   | 2004-07-06 11:21:20 | 63d 1h 45m 23s      | 1/10            | OK: rate[IN]=250 kbit/s OK: rate[OUT]=286 kbit/s                  |                                                                                            |
|                | if-traffic              | PING                 | Critical            | 2004-04-20 12:39:00 | 77d 20h 45m 1s  | 10/10                                                             | PING CRITICAL - Packet loss = 100%                                                         |
|                | if-traffic              | PING                 | UNKNOWN             | 2004-04-20 12:39:00 | 77d 20h 45m 1s  | 10/10                                                             | check_shmp_counter: ERROR during get-request: No response from remote host 162.119.68.186' |
|                | jasper                  | Diskusage C:         | OK                  | 2004-07-06 11:15:46 | 77d 1h 13m 47s  | 1/3                                                               | C:\ - total: 4.00 Gb - used: 2.99 Gb (75%) - free 1.01 Gb (25%)                            |
|                |                         | Diskusage E:         | OK                  | 2004-07-06 11:20:41 | 140d 1h 3m 7s   | 1/3                                                               | E:\ - total: 4.00 Gb - used: 1.46 Gb (36%) - free 2.54 Gb (64%)                            |
| MS-Exchange    |                         | OK                   | 2004-07-06 11:21:41 | 61d 22h 57m 53s     | 1/3             | All services are running                                          |                                                                                            |
| NotesConnector |                         | OK                   | 2004-07-06 11:21:41 | 61d 22h 57m 57s     | 1/3             | All services are running                                          |                                                                                            |
| SMTP           |                         | OK                   | 2004-07-06 11:21:43 | 61d 22h 58m 4s      | 1/3             | SMTP OK - 0 second response time                                  |                                                                                            |
| lenin          | SMTP                    | OK                   | 2004-07-06 11:21:51 | 20d 2h 18m 14s      | 1/3             | SMTP OK - 0 second response time                                  |                                                                                            |
| marx           | HTTP                    | OK                   | 2004-07-06 11:21:46 | 23d 2h 15m 17s      | 1/3             | HTTP ok. HTTP/1.1 200 OK - 0.016 second response time             |                                                                                            |
|                | SMTP                    | OK                   | 2004-07-06 11:21:51 | 22d 19h 2m 16s      | 1/3             | SMTP OK - 0 second response time                                  |                                                                                            |

# Sistemas integrados de gestão

- NMS - *Network Management Station*
  - Estação de trabalho através da qual se oferece acesso (*frontend*) às funções de gestão de toda a rede informática.



# Bibliografia

- António Miguel Figueira; “Introdução ao Cloud Computing”; FCA;  
ISBN: 978-972-722-802-7; 2015 (Cap 12)
- <http://www.net-snmp.org/>
- <https://www.nagios.org>