

SISTEMAS E REDES MULTISERVIÇO

**Capítulo 5 – Arquiteturas de Data
Center, Monitorização e avaliação de
desempenho**

Resumo do Capítulo



- **Arquiteturas de Data Center**
 - Caracterização
 - Servidores
 - Storage
 - SAN
 - HCI
- **Avaliação e Disponibilidade de Redes**
- **Monitorização**

Data Center



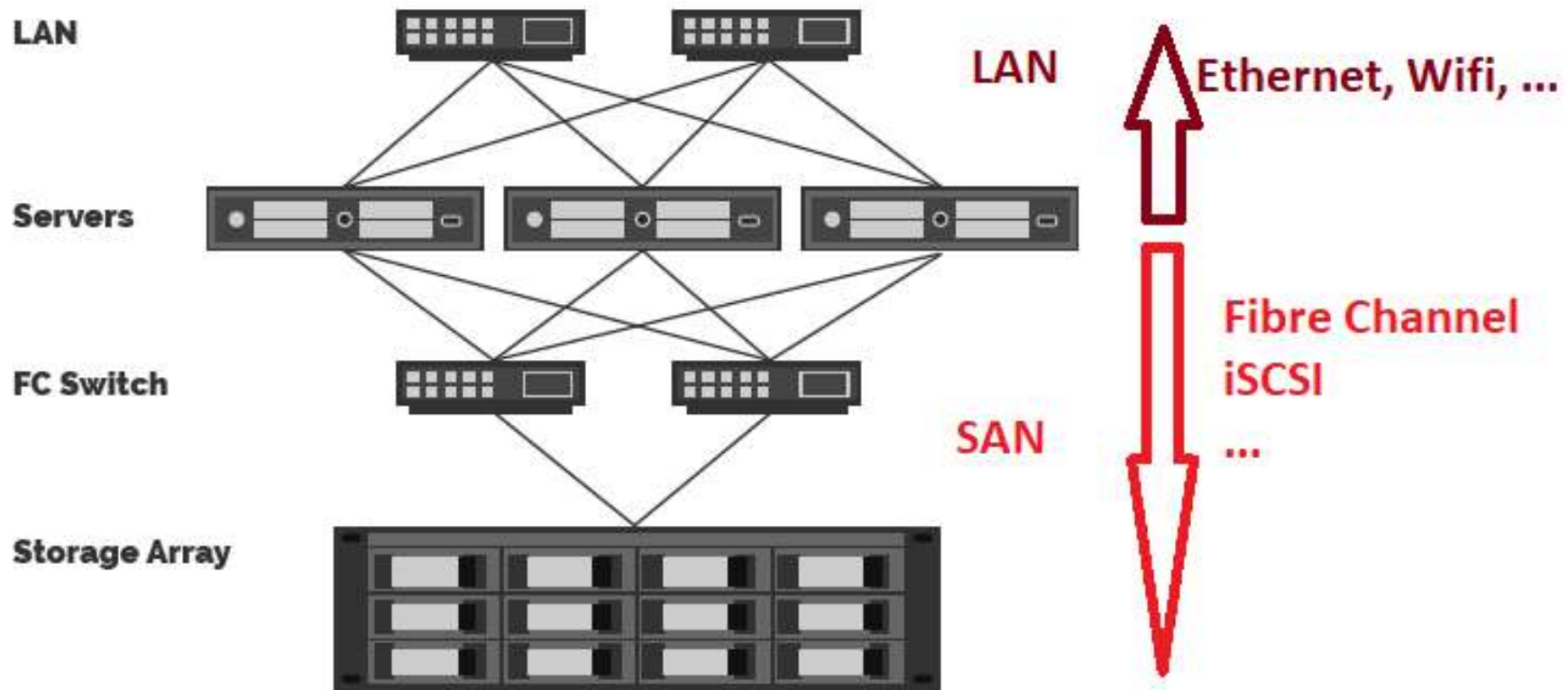
- Recurso constituído por computadores e armazenamento em rede para gerir, processar, armazenar e disseminar grandes quantidades de dados.
- Constituído por
 - Capacidade de processamento e memória para criar servidores
 - Capacidade de armazenamento (Storage)
 - Infraestruturas – edifício, energia, climatização, rede de dados, bastidores, cabos, etc
 - Software de gestão

Evolução no Data Center



- **Anos 90**
 - Um servidor físico para cada aplicação com storage dedicada
 - Muito espaço físico e consumo de energia!
 - Capacidades dos servidores subaproveitadas
- **Anos 00**
 - Partilha de recursos de computação (por Virtualização) e storage
 - redução da necessidade de hardware
 - SAN – Storage Area Network – para ligação dos servidores ao storage partilhado
- **Tendência atual**
 - Rapidez, disponibilidade, capacidade e economia
 - Hiperconvergência – trocar a SAN por sistemas integrados de computação e storage
 - Software Defined Data Center

Arquitetura Típica



Servidores



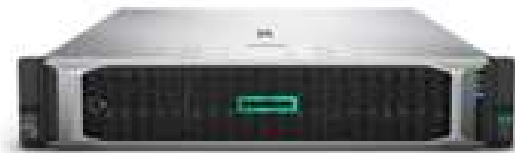
- **Servidores** – Computadores com elevadas capacidade de processamento e memória adequados para:
 - Alojamento de aplicações
 - Gerir Ficheiros
 - Processar dados
- Podem ser
 - Rack
 - Blades
 - Mainframes

Servidores



Servidores em Rack

- **Vantagens:**
 - Montado em bastidores
 - Fácil acomodação
 - Equipamentos standard (independência de fabricantes)
- **Dificuldades:**
 - Cablagem independente para energia, rede e ligação ao storage



Servidores



Servidores em Blades

- **Vantagens**

- Componente modular que encaixa num chassis
- A alimentação de energia e ligação à rede e ao storage é comum a todos os servidores no mesmo chassis
- Maior capacidade do que os servidores em Rack com menor espaço ocupado

- **Dificuldades**

- Chassis proprietário – todos servidores (blades) do mesmo fabricante
- Mais caro do que em rack



Servidores



- **Servidores Mainframe**
 - Equipamentos dedicados de alta performance
 - Extremamente poderosos
 - Exemplo: IBM com 12 milhões de transações encriptadas por dia
- **Dificuldades**
 - Muito caros
 - Podem ocupar muito espaço



Dimensionamento de servidores



- Devem ser adequados a garantir a prestação do serviço sem falhas ou atrasos.
 - **Hardware:**
 - CPU – quantidade, tipo e velocidade;
 - Memória - Cache, RAM, Flash;
 - Storage - SSD, HDD; RAID; ...
 - **Software:**
 - Sistema Operativo;
 - Software aplicativo de suporte ao serviço.

Dimensionamento de servidores



- No **dimensionamento** deve ser considerado o tipo de serviço e a carga expetável, nomeadamente tipificando o consumo por cada cliente ligado e o máximo de clientes ligados previstos.

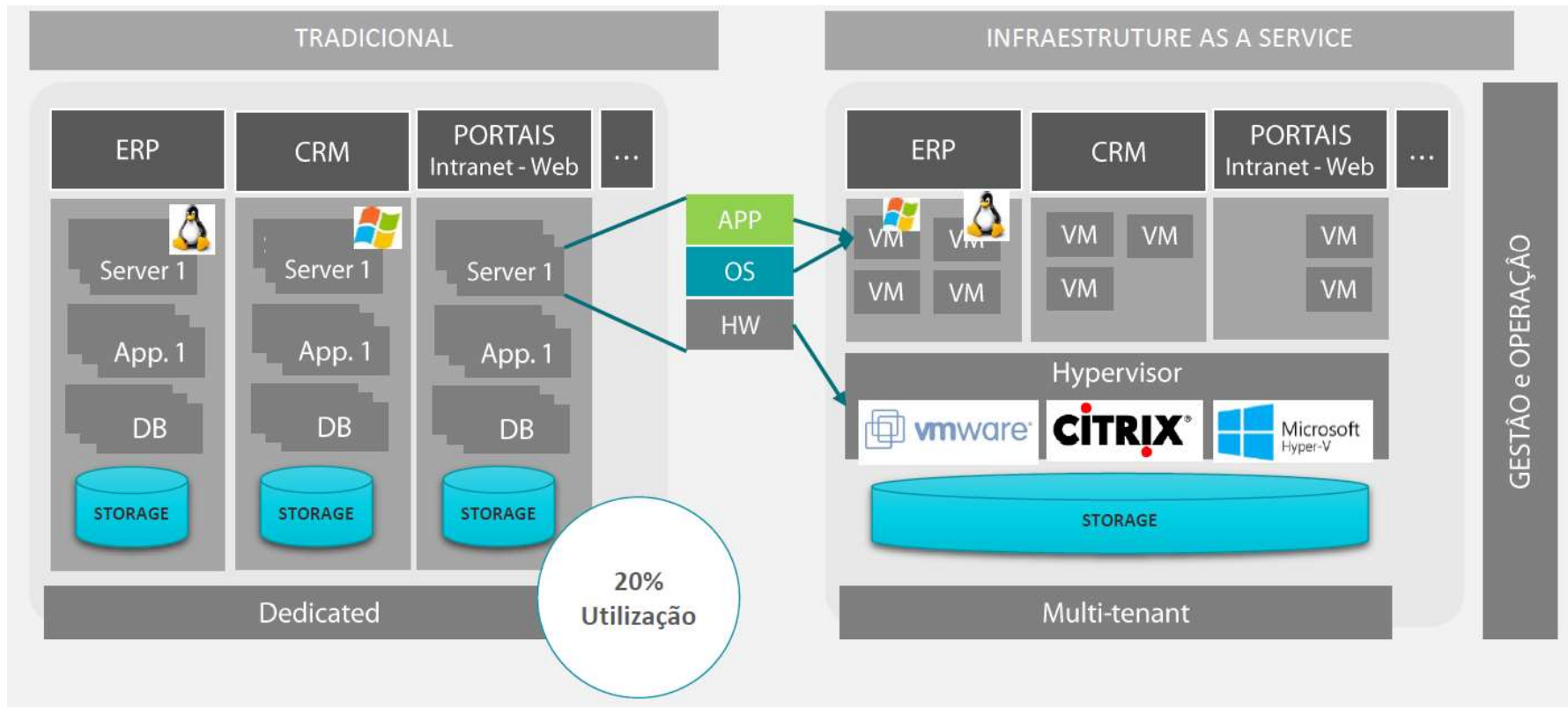
Atualmente, não existe um servidor físico para cada aplicação. Com a **Virtualização**, são criados e geridos servidores em máquinas virtuais em recursos partilhados de computação e storage.

VIRTUALIZAÇÃO



- Tecnologia que permite criar uma plataforma de hardware através de um componente de software
 - O software cria uma **máquina virtual** que emula um computador onde é possível instalar um sistema operativo.
 - Maior facilidade na gestão de máquinas para alterações, backups, mobilidade, etc...
 - Tecnologia fundamental para o Cloud Computing (MAS NÃO É A MESMA COISA!) pois permite partilhar uma plataforma informática em pedaços independentes que podem ser geridos por diferentes entidades

VIRTUALIZAÇÃO



VIRTUALIZAÇÃO



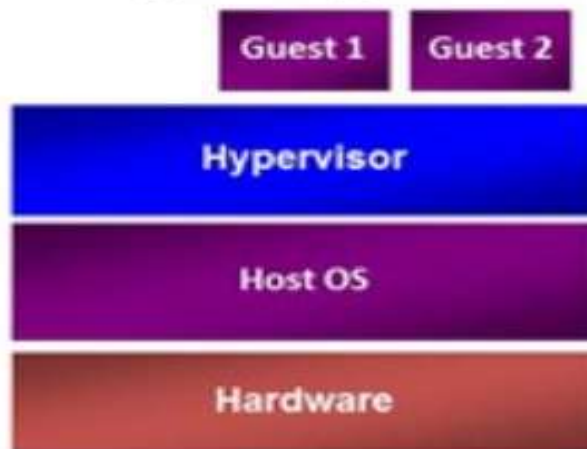
- Componentes de virtualização
 - Hardware físico de suporte (host ou **hospedeiro**)
 - Limita a capacidade computacional das máquinas virtuais que suporta;
 - Responsável pelas interfaces reais de ligação à rede;
 - **Hypervisor**
 - Camada de software que atua entre o hardware e o Sistema Operativo que emula as máquinas virtuais com recurso à partilha dos recursos do hospedeiro;
 - Faz a gestão dos recursos do host e a sua atribuição às Máquinas Virtuais;
 - Pode gerir os recursos de várias máquinas físicas (exemplo: *storage virtualization*);
 - **Máquinas Virtuais**
 - Sistemas independentes que atuam como um computador

VIRTUALIZAÇÃO



Hypervisor Design: Two approaches

Type 2 Hypervisor



Examples:

Virtual PC & Virtual Server
VMware Workstation
KVM

Type 1 Hypervisor



Examples:

Hyper-V
Xen
VMware ESX

VIRTUALIZAÇÃO



- **Vantagens da virtualização de máquinas**
 - Melhor aproveitamento dos recursos
 - Maior rapidez na criação de computadores ou servidores
 - Possibilidade de tratar um computador ou servidor como um ficheiro que se pode transportar facilmente
 - Mais facilidade para criar backups e arquiteturas de Disaster Recovery
 - Poupança de energia – fundamental!

Storage – Tipos de disco



- Avaliados pela capacidade, latência (tempo que demora a iniciar uma tarefa) número de operações de leitura/escrita (IOPS) e velocidade de transferência dos dados
- Durante muitos anos, **discos mecânicos (HDD)**
 - A velocidade é limitada pela rotação do disco – um bom disco atinge 200 a 400 IOPS
 - A latência também é afetada pela natureza mecânica do acesso aos dados – na ordem dos milissegundos
 - Discos SAS (**Serial Attached SCSI**) e SATA (*Serial Advanced Technology Attachment*)



Storage – Tipos de disco



- Tipos de disco para Storage

- Recentemente, discos **Solid State Drive (SSD)**

- Não há componentes mecânicos - informação guardada em memória não volátil (chips de memória)
 - Menor latência (na ordem dos microssegundos)
 - Mais IOPS (pode atingir mais de 100.000 IOPS)
 - Menor consumo energético
 - Menos propenso a avarias
 - Mais caro mas em processo de redução!
 - Por enquanto, discos de menores capacidades

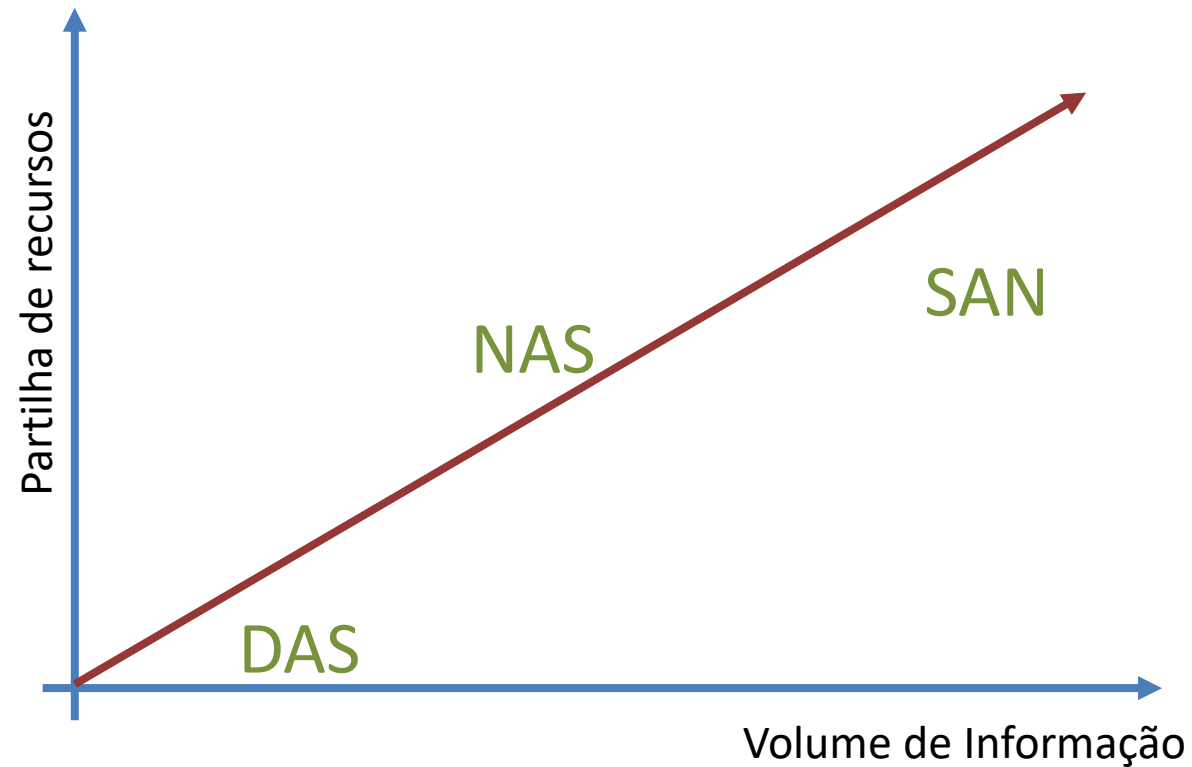


Storage



- Como gerir o armazenamento de dados (storage)?

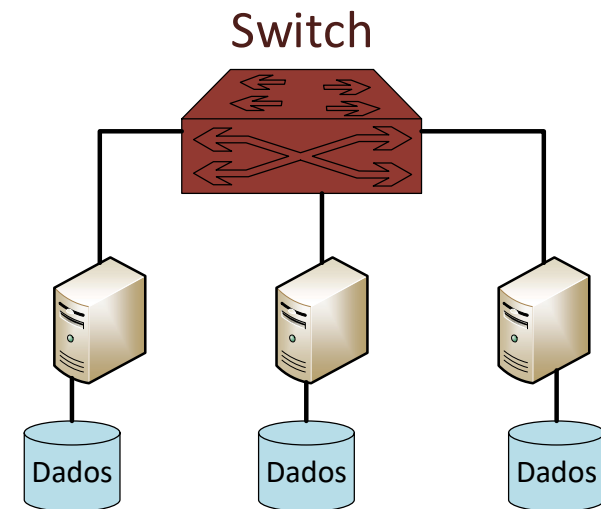
- DAS
- NAS
- SAN



Storage



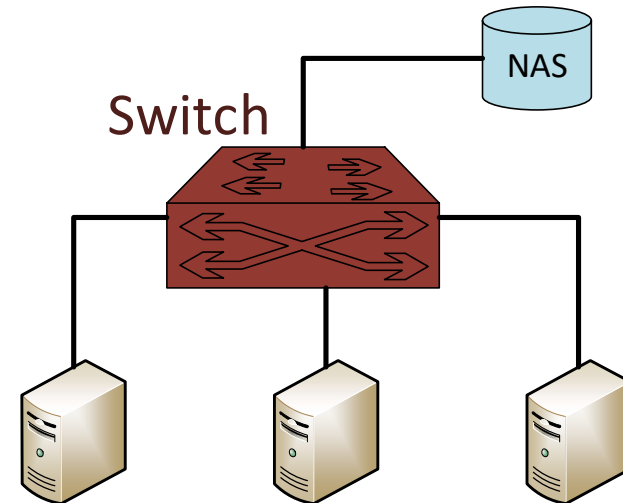
- **DAS – Direct Attached Storage**
 - A unidade de armazenamento está ligada diretamente ao sistema (p.e. servidor) que a usa sem passar pela rede;
 - Método tradicional usado quando a capacidade de disco de um servidor era ultrapassada;
 - Solução para baixas necessidades de volume em que não é necessário partilhar o storage;
 - O armazenamento só é utilizado pelo servidor a que está ligado



Storage

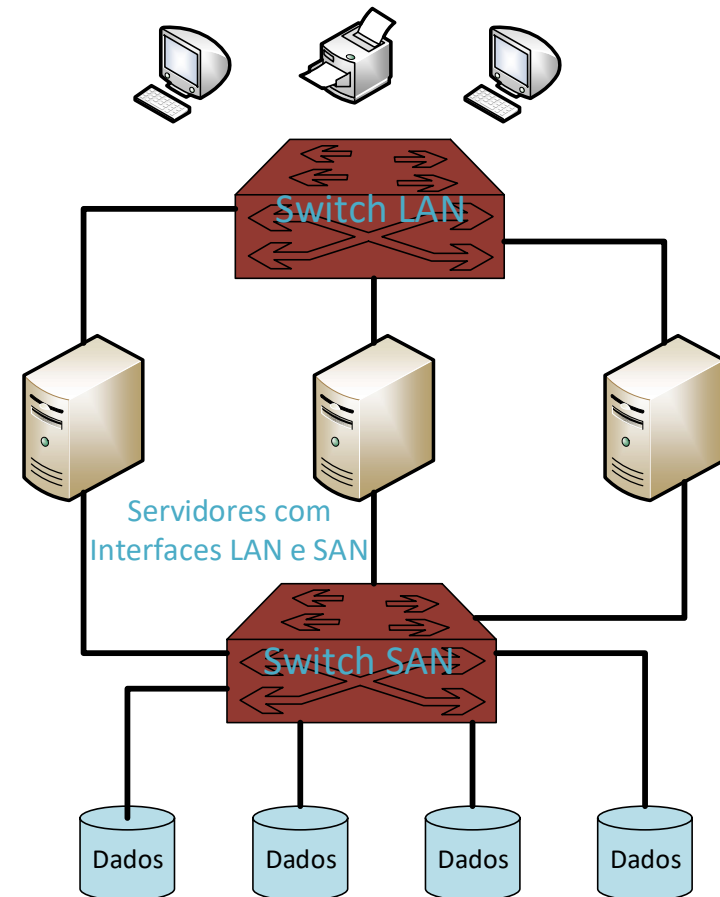


- **NAS – Network Attached Storage**
 - A unidade de armazenamento está ligada à LAN;
 - É ligada via TCP/IP, como qualquer dispositivo de rede, e tipicamente configurada por Web Browser;
 - A informação é acedida por File Share (p.e. NFS – Network File System) e pode funcionar p.e. como servidor multimédia;
 - Método mais comum em pequenas empresas;
 - Qualquer sistema da rede pode aceder à informação inclusive ao mesmo tempo.



SAN –Storage Area Networks

- **SAN – Storage Area Network**
 - Tecnologia, baseada em Switchs, que interliga múltiplos Servidores Físicos, Máquinas Virtuais e sistemas de armazenamento de dados (storage), tipicamente em DataCenters;
 - Existe uma rede própria para ligar servidores e storage, que não tem as mesmas regras da LAN; - evita que o congestionamento da LAN afete os servidores;
 - Exige investimento financeiro e capacidade de a gerir;
 - Há diferentes tecnologias.



SAN – Storage Area Network



- Tecnologias de rede Dominantes

- Fibre Channel

- Tecnologia mais antiga nas SANs
 - Funcionamento distinto da Ethernet/IP
 - Protocolos específicos para transporte de SCSI
 - Interface física com Host Bus Adapter (HBA)
 - Maiores débitos mas maior complexidade e custo
 - Exige equipamentos próprios (switchs, interfaces de rede dos servidores e unidades de storage)
 - Débitos múltiplos de 4Gb (típico 8, 16 ou 32Gbps; máx atual 128Gbps, roadmap para 512Gb)

SAN – Storage Area Network



- Tecnologias Dominantes

- iSCSI - Small Computer Systems Interface (SCSI) over IP



- Tecnologia SAN desenvolvida para ligar as interfaces SCSI (maioria do storage) em Ethernet/IP
 - Protocolo SCSI encapsulado em TCP/IP
 - A conectividade é fornecida através de adaptadores de barramento de host iSCSI (HBAs);
 - Já tem débitos semelhantes à FC mas com menores custos
 - Débitos típicos de 1Gb e 10Gb; máximo 100Gbps, roadmap para 400Gb

SAN – Storage Area Network

- Tecnologias Dominantes
 - Fibre Channel over Ethernet (FCoE)
 - Evolução das redes Fibre Channel para encapsular os pacotes FC em tramas Ethernet para poderem ser trabalhados por Switchs e Routers mais baratos;
 - Exige adaptadores de rede convergentes (CNA) que passam tramas Ethernet ou FCoE
 - Está a ter bastante sucesso por adicionar as vantagens do FC com os custos de equipamentos Ethernet

Evolução - HCI



- **Hyperconverged infrastructure (HCI)**
 - O SSD está a alterar a arquitetura do Data Center. É mais rápido ter o storage acedido diretamente do que através de uma SAN...
 - As várias componentes (processamento, storage, ligação à rede) ficam assembladas no mesmo rack (**nó**)!
 - Escalabilidade acrescentando mais nós.
 - A solução HCI inclui o bastidor, as cablagens pré-feitas, os nós e, muito importante, o software de gestão que inclui o Hypervisor e a capacidade de gerir por software todo o hardware de forma integral e partilhado (**Software Defined DataCenter**).

Evolução - HCI



- **Software Defined DataCenter**
 - O software faz a abstração do hardware;
 - Permite a criação e configuração de recursos de forma automática (automação)
 - p.e. Configuração automática de uma estação padrão
 - Simplifica os processos para o utilizador

Resumo do Capítulo



- Arquiteturas de Data Center
- Avaliação e Disponibilidade de Redes
 - Avaliação de desempenho
 - Business Continuity Plan (BCP)
 - Disaster Recovery (DR)
 - Alta Disponibilidade
 - Redundâncias
 - Balanceamento de Carga
- Monitorização

Avaliação de Desempenho

- As redes e sistemas de computadores podem ser avaliadas por:
 - Débito das ligações
 - Taxa de perda de pacotes
 - Atraso e variação do atraso
 - Tempo de resposta aos pedidos das aplicações → implicações no dimensionamento de servidores
 - Disponibilidade (tempo de *uptime* vs tempo de *downtime*)

AVALIAÇÃO DE DESEMPENHO

- **Disponibilidade** – medida de avaliação de redes ou sistemas que leva em conta o tempo que os serviços estiveram disponíveis.

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

- **TEMPO É DINHEIRO!**

Avaliação de Desempenho

- Para obter maior Disponibilidade -> maior investimento em hardware e software!
- Tipicamente as organizações procuram um compromisso entre a taxa de disponibilidade e o custo das soluções.
- Dois parâmetros relacionados:
 - MTBF – Tempo médio entre falhas
 - MTTR – Tempo médio da reparação a falhas
- **Disponibilidade = $MTBF / (MTBF + MTTR)$**

Disponibilidade de Serviços

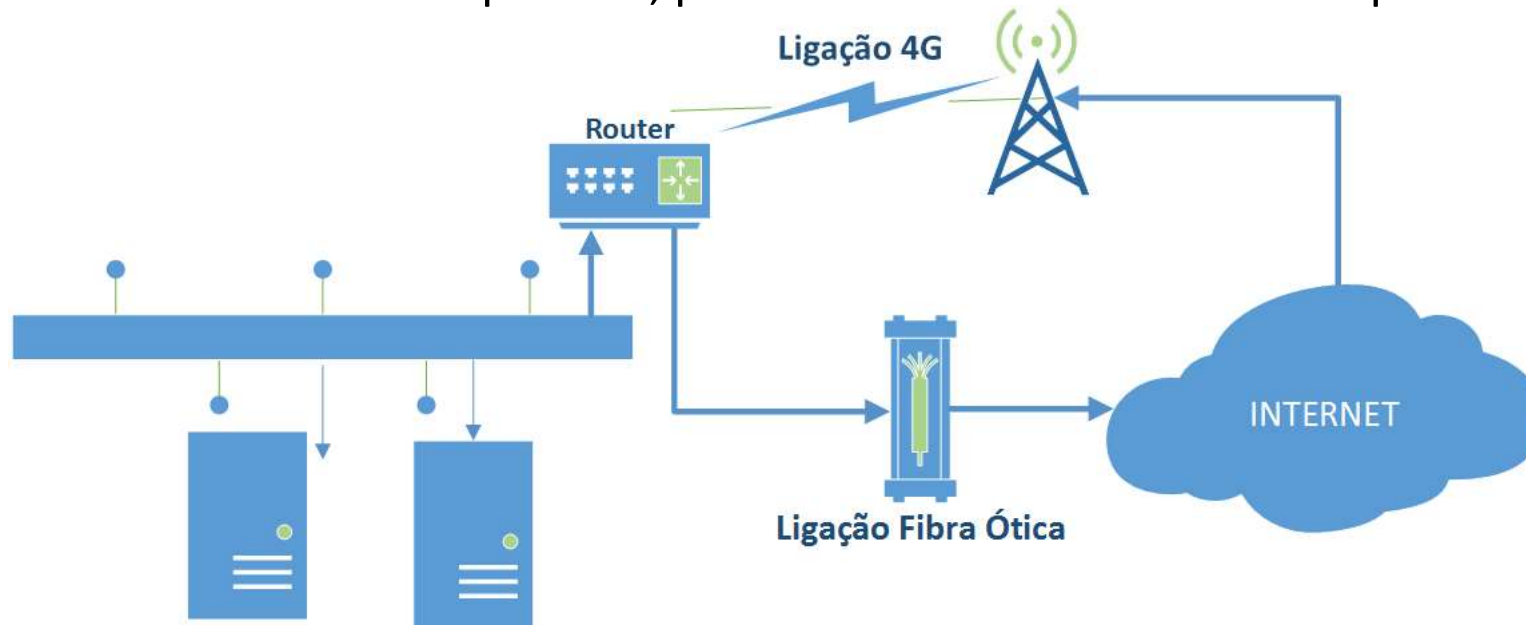
- Quando um serviço é crítico, exigindo uma elevada disponibilidade, recorre-se a sistemas de **Alta Disponibilidade**:
 - Soluções redundantes que incluem sistemas alternativos que asseguram o funcionamento do serviço quando o sistema principal falha.
 - Envolve Hardware, Software, Energia e Segurança (mesmo a física).

Disponibilidade de Serviços

- Alta Disponibilidade envolve:
 - Manter a Energia disponível
 - UPS – podem ser *on-line* (a energia está constantemente a alimentá-las e são elas que produzem a energia interna e a suportam em caso de falha) e as *off-line* (apenas atuam quando a energia falha);
 - Traçados de energia elétrica redundantes e por caminhos distintos;
 - Geradores alternativos – p.e. geradores a gasóleo.

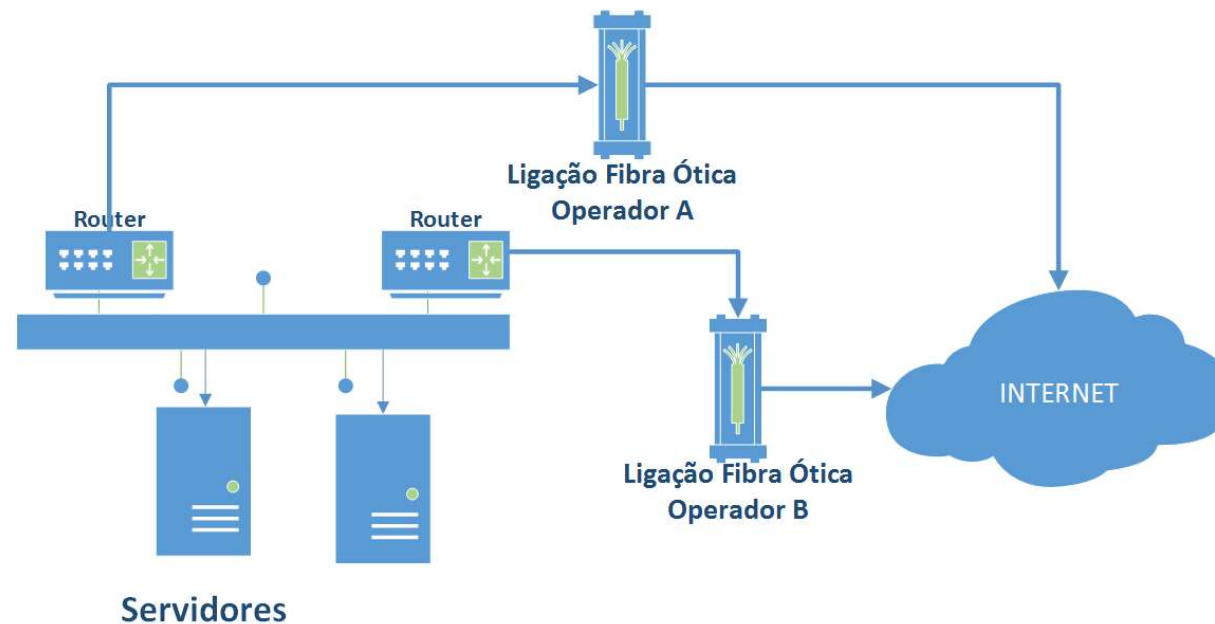
Disponibilidade de Serviços

- Alta Disponibilidade envolve:
 - Manter as Redes LAN e WAN disponíveis
 - LAN com caminhos redundantes;
 - Ligação à Internet duplicada por outro operador e/ou tecnologia (p.e. Fibra e 4G);
 - No mesmo operador, pode haver redundância de IP's públicos.



Disponibilidade de Serviços

- Alta Disponibilidade envolve:
 - Manter as Redes LAN e WAN disponíveis
 - Sistemas mais redundantes com duplicação de Routers, caminhos alternativos e operadores:
 - No mesmo operador, pode haver redundância de IP's públicos.



Disponibilidade de Serviços

- Alta Disponibilidade envolve:
 - Garantir disponibilidade nos Servidores
 - Duplicação dos equipamentos, em diferentes locais e ligados por acessos redundantes;
 - Peças redundantes (motherboard, fonte de alimentação, discos, etc.);
 - Garantir a disponibilidade da Informação
 - Backups, Backups, Backups e mais Backups – de preferência fora do edifício onde está o equipamento principal, p.e. em Cloud;
 - Celebrar **Service Level Agreement (SLA)** com fornecedores
 - Contrato que defina claramente o tempo de resposta às várias possíveis falhas!

Balanceamento de carga

- Quando um serviço é apenas assegurado por um servidor, este torna-se um “*Single point of failure*”:
 - Se falha, todo o serviço falha!
 - Solução: dimensionar servidores múltiplos e fazer **Balanceamento de carga** – repartir o serviço prestado por um conjunto de servidores para maximizar o desempenho e garantir redundância em caso de falha.
 - Serviço fundamental em prestadores de serviços de Data Centers.

Balanceamento de carga

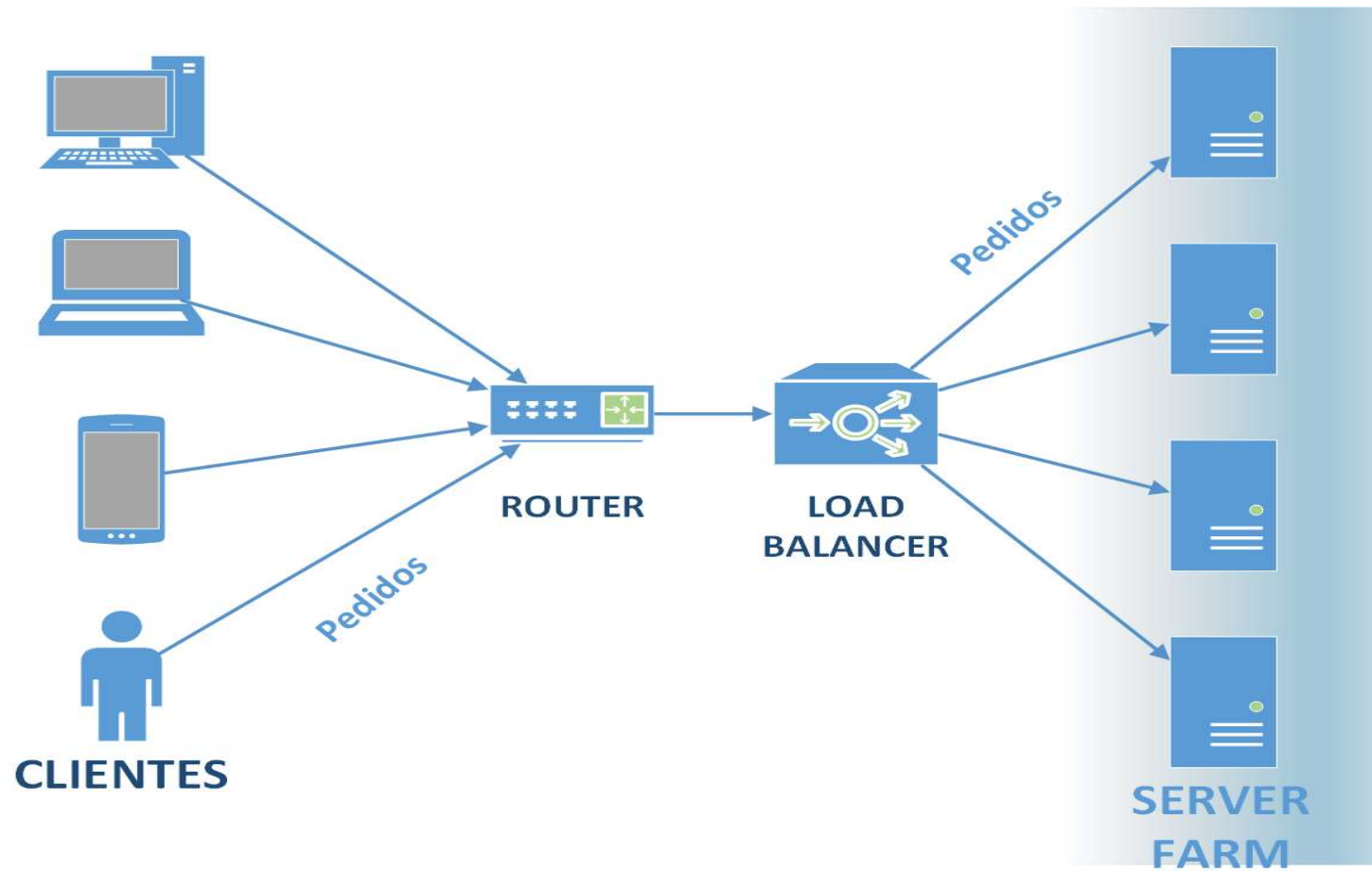


- A implementação pode ser feita:
 - **Soluções comerciais proprietárias:**
 - Exemplo: Windows Load Balancing Service (WLBS), Network Load Balancing (NLB) ou Component Load Balancing (CLB) da Microsoft.
 - **Construir uma *farm* (ou *cluster*) de servidores** – dois ou mais servidores que atuam como se fossem um só com a intervenção de um balanceador de carga que distribui o trabalho.
 - Cada servidor tem de ser capaz de aceder ao(s) disco(s) do(s) outro(s);

Balanceamento de carga



Construir uma *farm* (ou *cluster*) de servidores



Balanceamento de carga

- No sistema de *farm*, o **balanceamento de carga** divide o trabalho entre os servidores da forma mais uniforme possível para otimizar o desempenho e evitar congestionamentos.
 - **Método básico**: selecionar de forma aleatória, sequencial ou outra, o servidor a tratar cada pedido; O servidor encaminha cada pedido alternadamente para um dos servidores.

Balanceamento de carga



- **Métodos Estáticos:** o balanceador não conhece o estado atual dos servidores, apenas a sua capacidade, e atribui os pedidos aos servidores com base nessa informação;
 - Aplicável em pequenos DataCenters;
 - Exemplos: Round-Robin, Threshold Algorithm, etc.
- **Métodos Dinâmicos:** o balanceador registra o número de ligações já encaminhadas e ainda ativas para cada servidor e escolhe o que tiver menos carga no momento.
 - Mais complexo mas mais eficiente em grandes DataCenters.
 - Exemplo: Least-Connect

Balanceamento de carga



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

Disponibilidade de Serviços

- Planos necessários para definir e garantir a Disponibilidade:
 - **Business Continuity Plan (BCP)**
 - Documento que define qual a informação crítica de uma organização, ou seja, aquela que não pode faltar para não interromper a atividade da organização!
 - **Disaster Recovery (DR)**
 - Plano de recuperação após um evento que gerou a destruição completa da informação e equipamentos principais (p.e. incêndios, inundações, terremotos, ataques terroristas, etc);

Disponibilidade de Serviços

- **Business Continuity Plan (BCP)**
 - Documento que define qual a informação crítica de uma organização, ou seja, aquela que não pode faltar para não interromper a atividade da organização!
 - É um processo proativo que visa minorar os riscos de perda de informação;
 - Envolve:
 - Sistemas
 - Processos

Disponibilidade de Serviços

- **Business Continuity Plan (BCP)**
 - O que deve fazer parte do BCP:
 - Definir a informação crítica para a empresa;
 - Como essa informação existe e se mantém;
 - Quem são as pessoas responsáveis pela sua manutenção;
 - Qual o processo de manutenção e recuperação em caso de perda;
 - Quais os custos destes processos.
 - É um documento sucinto e preciso, em constante evolução e melhoria.

Disponibilidade de serviços

Disaster Recovery



- **Plano de Disaster Recovery (DR)** – Define como se faz a recuperação após um evento que gerou a destruição completa da informação e equipamentos principais (p.e. incêndios, inundações, terremotos, ataques terroristas, ataques informáticos, etc);
- É um processo reativo que é suportado no BCP.
- **Métricas:**
 - **RTO – Recovery Time Objective** - Tempo que demora desde a ocorrência do desastre até os serviços estarem disponíveis;
 - **RPO – Recovery Point Objective** - Define a quantidade de informação que se assume perdida num desastre; define o intervalo de backup da informação; no limite, a informação que se perde é a produzida entre o último Backup e o momento do Desastre.

Disponibilidade de serviços

Disaster Recovery



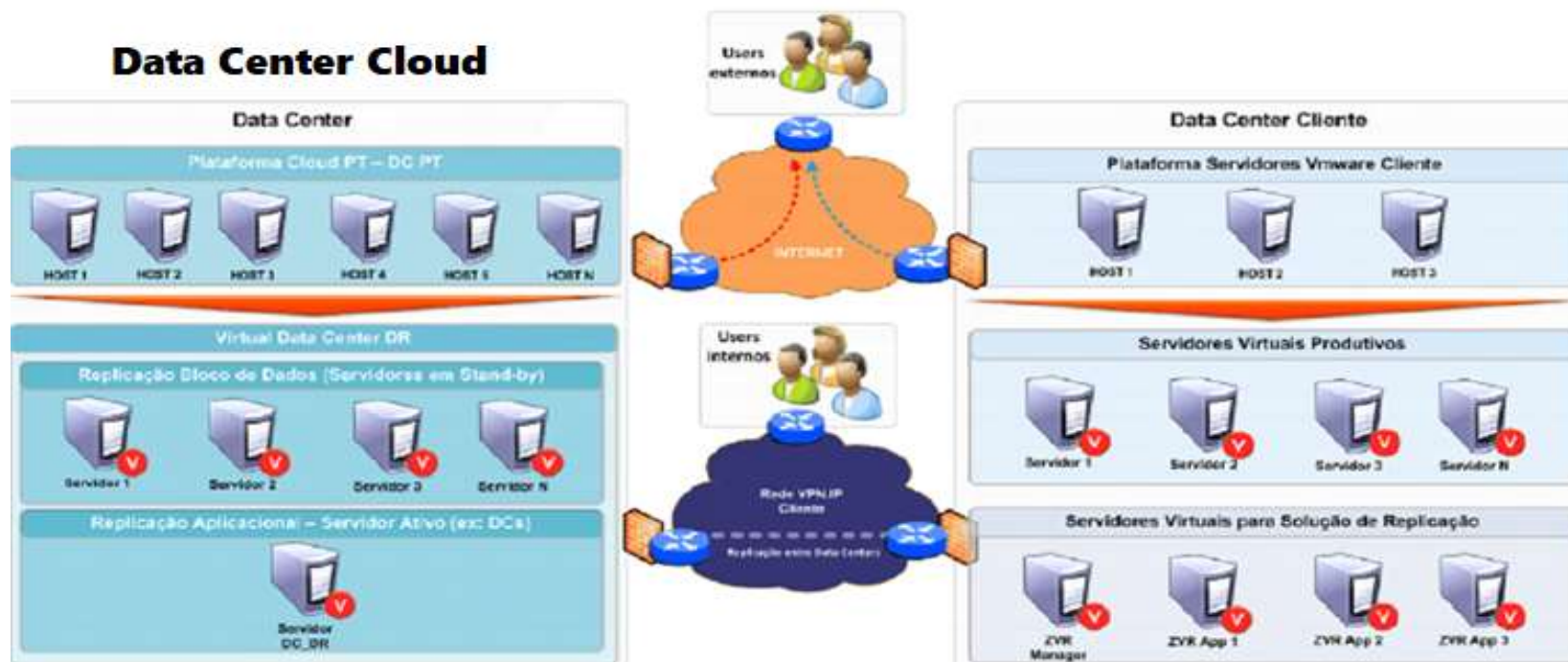
- Como implementar Disaster Recovery (DR)
 - Hoje em dia os servidores de organizações estão virtualizados, são software...
 - É relativamente simples copiar, mover...
 - Várias opções:
 - Manter **cópias atualizadas dos servidores** em local fora da empresa
 - **Duplicar Hardware e servidores** na LAN num ponto afastado do DataCenter Principal
 - Criar um **virtual Data Center na Cloud** que replica o Data Center Principal
 - Exemplo de aplicações de duplicação permanente de Servidores:
 - Zerto: <https://www.zerto.com/>
 - Veeam: <https://www.veeam.com/>

Exemplo de DR



DR suportado em Cloud:

- Imagens dos servidores virtuais no Data Center Cloud
- Ligações de Backend (via VPN na rede do operador) ao Data Center com débito garantido em ambiente seguro;
- Tempos curtos para RPO - atualização das imagens dos servidores;
- Endereços IP públicos replicados pelo Data Center (diminui o RTO).



Resumo do Capítulo



- Arquiteturas de Data Center
- Avaliação e Disponibilidade de Redes
- Monitorização
 - Monitorização de Redes e Sistemas
 - Arquitetura SNMP
 - Arquitetura WMI
 - Ferramentas de monitorização

MONITORIZAÇÃO

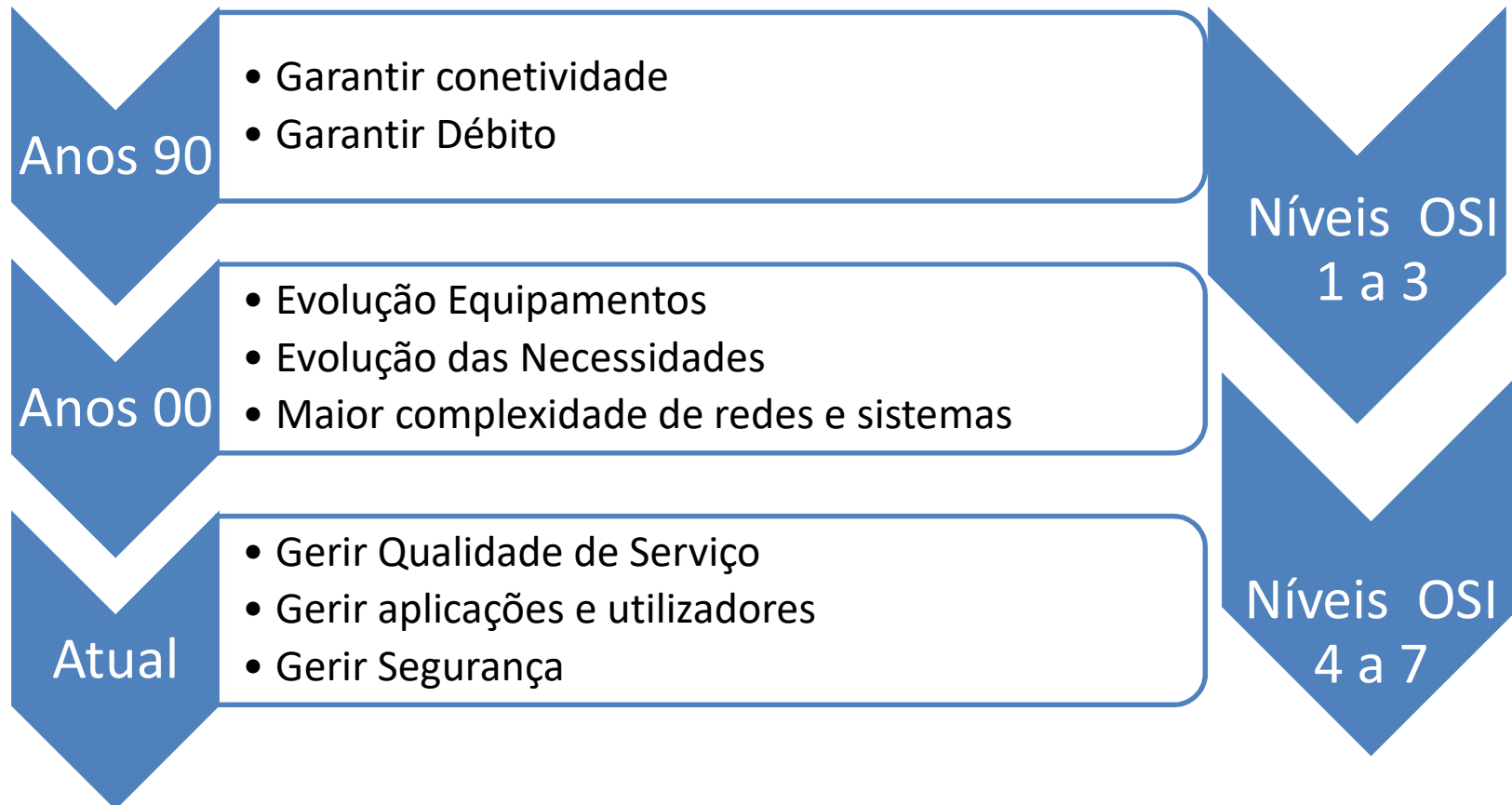


- A **MONITORIZAÇÃO** é fundamental para uma eficaz gestão das redes e sistemas informáticos.
- A sua motivação deriva da necessidade que o gestor de rede tem de conhecer, avaliar, medir e prever o desempenho de todos os elementos.
- O **CONHECIMENTO** da rede, das suas vulnerabilidades e ameaças é uma ferramenta que antecipa problemas e permite fornecer aos utilizadores uma experiência melhorada dos serviços que necessita.

MONITORIZAÇÃO



- As necessidades de gestão de redes têm evoluído:



MONITORIZAÇÃO



- Algumas **atividades de monitorização** numa rede de computadores:
 - Conetividade dos equipamentos;
 - Desempenho de serviços;
 - Medição de parâmetros;
 - Análise de tráfego e protocolos;
 - Detecção de intrusões;
 - Suporte técnico aos utilizadores;
 - ...

MONITORIZAÇÃO



- A **MONITORIZAÇÃO DE REDE** inclui um conjunto de tarefas e **funcionalidades** muito úteis na gestão de redes:
 - Detecção de avarias – através de envio de alertas ou notificações ao gestor;
 - Gestão pró-ativa – deteção e correção de anomalias
 - Documentação ou inventário da rede;
 - Acesso a ferramentas gráficas acerca do estado das redes, equipamentos, serviços e tráfego;
 - Medições e avaliação de desempenho tendo em conta níveis de serviço exigidos.

ARQUITETURA SNMP



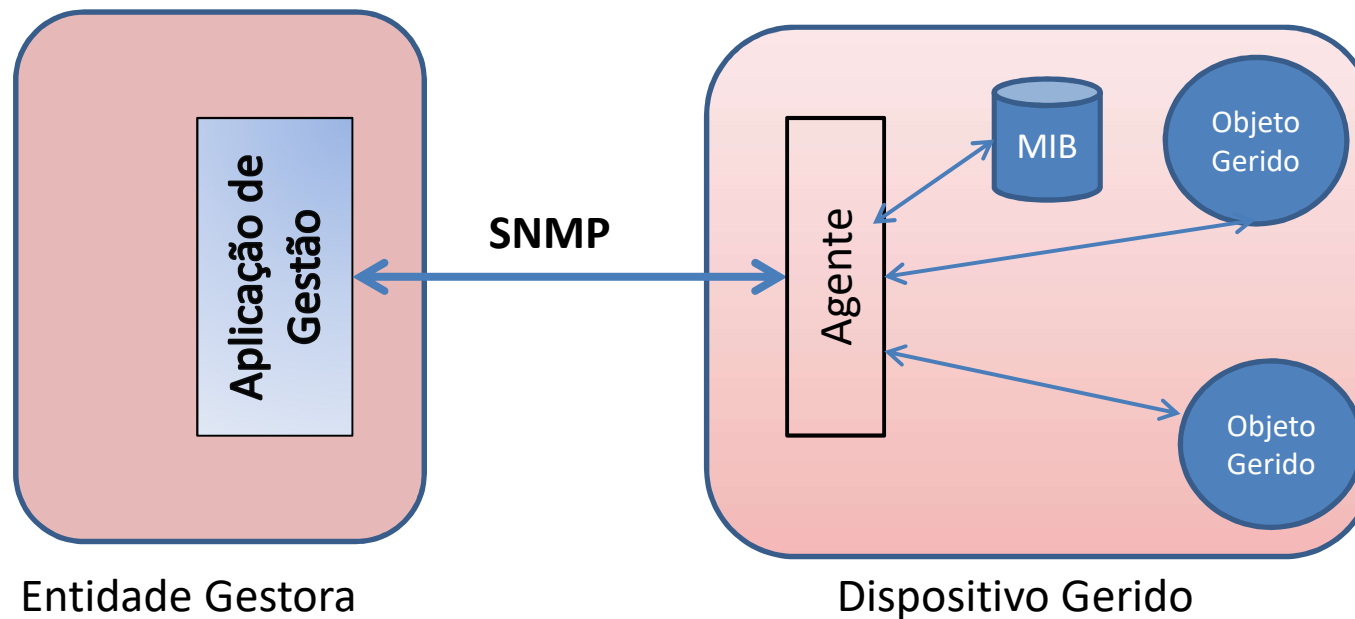
- A arquitetura mais utilizada é a **SNMP – Simple Network Management Protocol**
 - Normalizada pelo IETF em 1990 e está agora na versão SNMPv3;
Ver: <https://searchnetworking.techtarget.com/feature/The-fundamentals-of-availability-monitoring-tools>
 - Componentes:
 - Uma ou mais entidades de gestão coordenados – MIB RMON;
 - Agentes de Gestão;
 - MIB
 - Arquitetura modular
 - Linguagem SMI – define como a informação está estruturada nas MIB
 - Definição do tipo de informação a armazenar
 - Protocolo SNMP para a comunicação
 - Funcionalidades de segurança da informação

ARQUITETURA DA GESTÃO DE REDES



- Componentes da gestão de redes:
 - **Entidade gestora** (*managing entity*) – aplicação que centraliza a informação e alertas sobre a atividade da rede e permite a gestão dos dispositivos;
 - **Dispositivo gerido** (*managed devices*) – qualquer equipamento a ser gerido. Tem um ou mais **objetos geridos** (interfaces, software, etc). Em cada dispositivo corre um denominado processo **agente** que se encarrega de comunicar com a entidade gestora. O agente recorre a uma base de dados (**MIB – management information base**) que definem o tipo de objetos geridos e sua informação.
 - **Protocolo de Gestão** – forma de comunicação entre a entidade gestora e os agentes.

ARQUITETURA DA GESTÃO DE REDES



Exemplos:

Aplicação de Gestão: NAGIOS, MRTG, Spiceworks, etc.

Objeto Gerido: Placa de Rede, CPU, Memória, etc.

PROTOCOLO SNMP



- Regula a comunicação entre a entidade gestora e os agentes localizados nos objetos/dispositivos geridos;
- Permite combinar monitorização ativa com passiva
- Sete tipos de **mensagens** (PDU, utilizam porto 161)
 - GetRequest, GetNextRequest, GetBulkRequest – da entidade gestora para os agentes a pedir informação;
 - SetRequest - da entidade gestora para os agentes a alterar informação;
 - InformRequest – troca de informação entre gestores
 - Trap – alerta enviado pelo agente
 - ResponsePDU – resposta do agente aos GET e SET.

MIB



- *MIB – Management Information Base*
 - Os módulos MIB reúnem a informação dos objetos a monitorizar numa rede;
 - É um Ficheiro ASCII com a descrição formal dos objetos num dispositivo. A entidade gestora tem de compilar este ficheiro para o poder interpretar.
 - Cada objeto inclui um identificador (OID) em formato hierárquico
 - Para identificar os objetos recorre a uma linguagem específica para a estrutura dos dados (*SMI - Structure of Management Information*)

WMI



- **WMI - Windows Management Instrumentation**
 - Em sistemas Windows, o WMI é a estrutura tipicamente usada para monitorização
 - Permite obter dados de equipamentos Windows (PC's, Servidores, etc) com mais informação do que via SNMP.
 - Através do WMI é possível gerir computadores localmente ou remotamente (desde que tenha as permissões necessárias) recolhendo dados e alterando o estado dos objetos e das entidades físicas correspondentes, sejam elas hardware ou software (serviços, contas de utilizadores...).

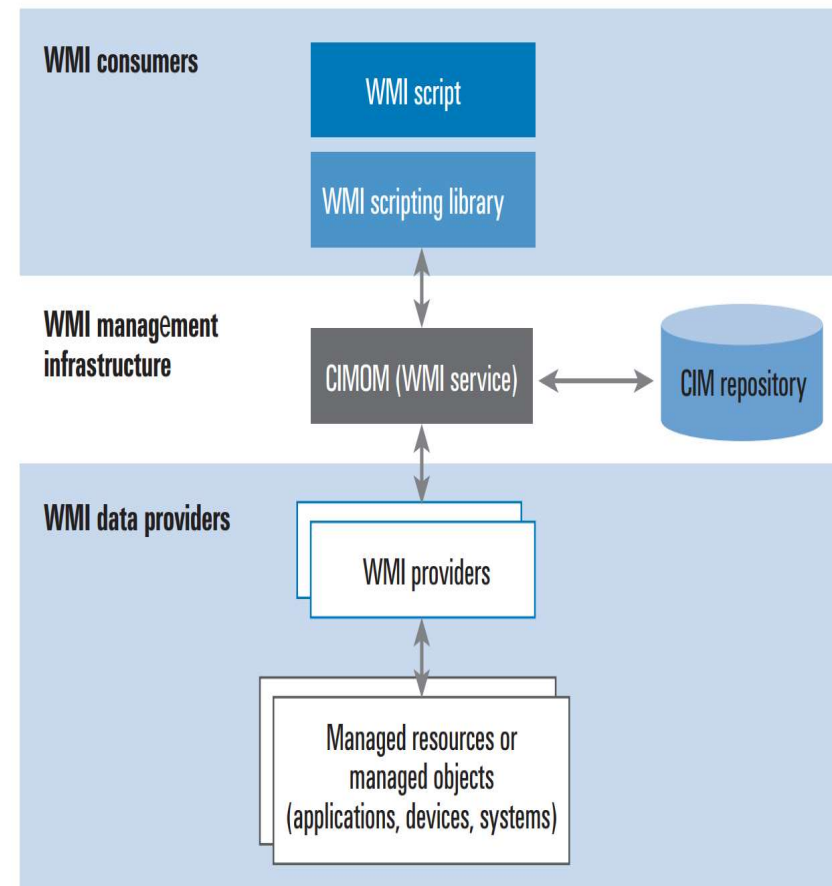
ARQUITETURA WMI



- **Arquitetura WMI:**

- **Consumers:** sistema que recebe e trata a informação – p.e. softwares de monitorização

- O acesso à informação de monitorização é feito através de scripts em qualquer linguagem que permita o controlo de objetos Microsoft ActiveX (p.e. C, C++, Python, VB Scripts, etc.)



ARQUITETURA WMI



- **Arquitetura WMI:**
 - **Data Providers:** sistema que lê a informação dos recursos geridos.
 - A informação está organizada na linguagem WQL (Windows Query Language) que segue uma estrutura semelhante a uma estrutura SQL:

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

ARQUITETURA WMI



- **Arquitetura WMI:**
 - **WMI Infrastructure**
 - Componente do SO Windows que controla e define a comunicação entre os consumers e os providers
 - É aqui que estão definidas as classes, por exemplo.

Impacto sobre a infraestrutura de rede



- A ativação de sistemas de monitorização têm **impactos nas infraestruturas de rede** que não devem ser descurados:
 - Consumo de largura de banda, nomeadamente em scans à rede;
 - Ativação de funcionalidades nos dispositivos que implicam abrir portas que podem ser usadas por terceiros para aceder à informação dos utilizadores e dos sistemas.
 - Ter o cuidado de configurar os firewalls para permitir a comunicação dos protocolos de monitorização.

SISTEMAS DE MONITORIZAÇÃO



- Devem permitir não apenas verificar conectividade mas também desempenhos e disponibilidade de serviços.
 - **Análise de soluções existentes**
 - **Produtos comerciais** – abrangentes nas funcionalidades, com custos significativos e adaptadas a meios homogêneos.
- Exemplos: HP BTO (Business Technology Optimization) , CiscoWorks, IBM Tivoli e outras

SISTEMAS DE MONITORIZAÇÃO



- **Oferta Open Source:**

- Conjunto de ferramentas disponibilizadas gratuitamente independentes de fabricantes.

Exemplos mais comuns:

- **MRTG** – mede desempenho e tráfego na rede

- **NAGIOS** – plataforma de inventariação e gestão

- **Spiceworks** ou **PRTG** – exemplos de plataformas de inventariação e monitorização *opensource* com interface web



CAPÍTULO 5



DÚVIDAS?