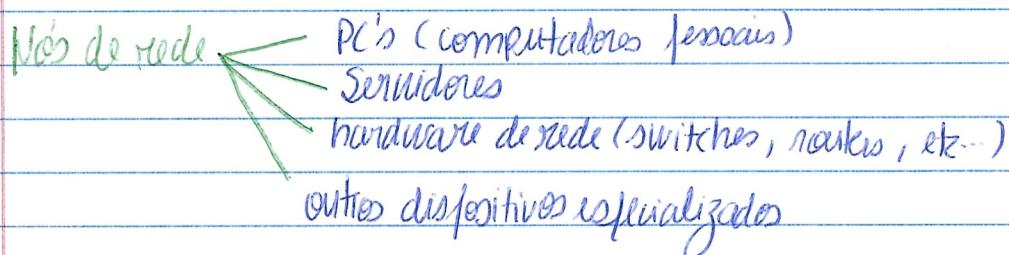


5COMRED - aulas 4 e 5

Computer Networks

→ Redes de computadores consistem num conjunto de computadores que partilham recursos entre si.

→ Esses recursos podem estar localizados nos próprios computadores ou fornecidos por mais (muitos) de redes.



Identificação na rede: cada nó tem um endereço de rede único.
Pode ter também um hostname.

• Organização de redes de computadores por proximidade geográfica

* LAN (local area network)

- abrange uma área limitada, como um edifício (Ex: ethernet).

* WAN (wide area network)

- abrange grandes áreas geográficas, como países ou o mundo.

• usa frequentemente conexões de alta velocidade ponto-a-ponto (ligações ópticas)

* SAN (storage area network): Para armazenamento de dados.

* MAN (metropolitam area network): Abrange uma cidade.

internet VS Internet

```
graph TD; A[Internet] --- B[Internet]
```

conjunto
interligado
de redes

rede global que
conecta dispositivos
no mundo inteiro

Evolução da Internet

Ideia original

- cada nó na Internet teria um endereço IP único
- Qualquer dispositivo poderia comunicar diretamente com qualquer outro.

Limitações

- Sem sigilo ou autenticação
 - ↳ Todas as mensagens eram visíveis para roteadores e hosts na mesma LAN.
- Possibilidade de falsificação (via possível forçar o campo de origem no cabeçalho dos pacotes)

Principais falhas

- visibilidade de endereços IP
- acesso restrito e conhecimento global
- questões de segurança

Modelo TCP / IP

4 camadas:

* Application layer

Função: Interface entre o utilizador (software) e a rede. É responsável por processar os dados a serem enviados ou recebidos. (HTTP, FTP, SMTP, DNS)...

* Transport layer

Função: Gerencia a comunicação p2p, garantindo que os dados sejam enviados e recebidos corretamente. (TCP (transmission control protocol), UDP (user datagram protocol))

* Internet (network) layer

Função: lida com o encaminhamento e rotreamento dos pacotes de dados entre diferentes redes. (IP (internet protocol), ICMP (internet control message protocol)).

* Link (physical) layer

Função: garante a comunicação entre dispositivos na mesma rede local, transmitindo dados fisicamente. (Ethernet, ARP (address resolution protocol)).

Ethernet Networks



Tecnologia de LAN mais amplamente utilizada para redes com fio.

- Apesar de ter evoluído, manteve:

- formato dos pacotes;
- esquema de endereçamento;

- compatibilidade retroativa (os novos mais recentes podem interagir com equipamentos antigos).

Endereço MAC (Media access control)

- cada adaptador ethernet tem um endereço único de 48 bits (xx:xx:xx:xx:xx:xx)



Primeros 24 bits → OUI (identificador único do fabricante)

Últimos 24 bits → número atribuído pelo fabricante para atribuir exclusividade

(cada fabricante recebe um intervalo fixo para evitar duplicações).

Hubs vs switches

Hubs

→ Dispositivos simples que conectam múltiplos hosts numa rede local.

Funzionam como repetidores, enviando todos os dados recebidos para todas as portas conectadas.

- não distinguem qual host deve receber os dados;

- o tráfego é enviado para todas as portas, o que pode causar congestionamento

- menor eficiência.

- operam na camada de enlace física do modelo OSI.

Switches

→ Dispositivos mais avançados que conectam múltiplos hosts, mas com capacidade de gerenciar e direcionar o tráfego de forma eficiente.

- Aprendem quais hosts estão conectados a cada porta, utilizando tabelas de endereços MAC.

- Enviam os dados apenas para a porta específica onde o host do destino está conectado.

- Reduzem o tráfego desnecessário na rede.
- Operam na camada de enlace (ou na de rede), no modelo OSI.

Switches → mais eficientes, inteligentes e evolutivos.

Resumo :

- Segmentos de rede locais (LAN's) são conectados usando hubs e switches.
- Hubs estão conectados a switches, que integram os diferentes segmentos de rede e permitem maior desempenho.

Switches em redes ethernet

→ operam na camada de enlace (Data Link Layer) do modelo OSI.

- Usados para conectar dispositivos (hosts) dentro de uma Rede Local (LAN).
- Não têm capacidade nativa para encaminhar pacotes entre redes diferentes (isso é função de routers).
- Utilizam endereços MAC (Media access control) para decidir para qual porta enviar os quadros de rede.
- Não recebem nem processam endereços IP, que pertencem à camada de rede.

Conexão de múltiplas LAN's :

Routers : operação na camada de rede

- Função : conectar redes distintas, como duas LAN's.
- Routers utilizam endereços IP para encaminhar pacotes de dados entre redes.

Características dos Routers :

1. Interconexão de redes diferentes :

- LAN1 e LAN2 podem ser diferentes em termos de tecnologia. O router age como um "tradutor" em termos de tecnologias.

2. Encaminhamento baseado em IP :

- Enquanto que switches lidam com endereços MAC na camada de enlace, routers analisam o endereço IP de cada pacote para determinar o próximo destino.

3. WAN (Wide Area Network):

- A conexão entre routers é feita por meio de uma WAN, que pode usar tecnologias como fibras ópticas, links dedicados ou conexões DSL.



LAN1 e LAN2 estão conectadas a routers que se comunicam por meio de uma WAN.



Cada LAN pode ter múltiplos hosts, e o router é o ponto de saída para os pacotes que precisam alcançar outra rede.

Estrutura lógica da Internet

• Interligação Ad Hoc de redes

• Sem uma topologia particular: a internet não possui um layout físico fixo ou uma estrutura única. Em vez disso, é uma coleção de várias redes (privadas, públicas, cooperativas, etc...) interconectadas de forma ad hoc. Cada rede pode estar ligada a outras de formas diferentes, tornando a internet altamente descentralizada e flexível.

• Capacidades de routers e links muito diferentes;

• Roteamento de pacotes de dados

• Envio de pacotes da origem ao destino por meio de ~~entre~~ redes: os dados são transmitidos sob a forma de pacotes. Esses pacotes viajam por várias redes até atingirem o destino.

• O router forma uma ponte de uma rede para outra: os routers são dispositivos responsáveis por encaminhar pacotes de uma rede para outra. Cada router forma uma "ponte" que conecta diferentes redes.

• Pacotes diferentes podem seguir diferentes rotas: cada pacote pode seguir uma trajetória diferente da origem até o destino. Isso deve-se a fatores como a carga de rede, falhas de links ou algoritmos de otimização de roteamento.

Internet Protocol



Refere-se a um conjunto de regras padronizadas que determinam como os hosts (dispositivos finais, como computadores ou servidores) e roteadores (dispositivos de rede que encaminham pacotes de dados) colaboram para transferir dados através de redes.

Como os bits podem ser transferidos entre LANs e WANs incompatíveis?

- As LANs e WANs podem usar diferentes tecnologias, protocolos e tipos de redes, o que pode causar algumas dificuldades na comunicação entre elas.

Solução: O software de protocolo é executado em cada host e roteador, permitindo que esses dispositivos comuniquem de forma transparente, mesmo quando operam em redes diferentes.

O que é um protocolo?

→ conjunto de regras padronizadas que define como a troca de dados deve ocorrer entre dispositivos de uma rede. Essas regras cobrem tudo, desde a formatação e o envio de pacotes de dados até termos em erros são corrigidos durante a transmissão.

• A interoperabilidade entre LANs e WANs é alcançada pela abstração dos detalhes técnicos de cada tipo de rede.

Tem duas funções principais:

1) Fazem um esquema de endereços:

- define um formato uniforme para os endereços dos hosts.
- cada host (e roteador) recebe um endereço único que o identifica de forma exclusiva na rede.

2) Fazem um mecanismo de entrega:

- define uma unidade de transferência padrão, o pacote.

- O pacote é composto por:

- cabecalho: contém informações como o tamanho do pacote, endereços de origem e destino.
- carga útil: contém os dados enviados do host de origem.

Global IP Internet

↳ Baseada na família de protocolos TCP/IP.

1. IP (Internet Protocol) : fornece um esquema de nomes e entrega não confidencial de pacotes de host para host.

2. UDP (User datagram Protocol) : usa o IP para entrega não confidencial de datagramas de processo para processo.

3. TCP (Transmission control Protocol) : usa o IP para entrega confidencial de fluxos de bytes de processo para processo, com garantias de ordem e retransmissões.

→ O acesso à rede é feito através de funções de entrada/saída Unix e a interface de sockets para comunicação entre processos.

A programmer's view of the Internet:

1. Hosts mapeados para endereços IP : Ex: 128.2.203.179 (127.0.0.1 é sempre localhost).

2. DNS (sistemas de nomes de domínio) : Converte nomes de domínio (ex: www.iseb.ipp.pt) em endereços IP (ex: 52.156.202.75).

3. Comunicação entre processos : Processos em hosts diferentes podem comunicar usando protocolos como TCP (orientado à conexão) ou UDP (sem conexão).

IP address

↳ endereço IP é uma identificação única para cada dispositivo na internet. O protocolo de Internet Versão 4 (IPv4) utiliza endereços de 32 bits, que são representados da seguinte forma:

→ O endereço é dividido em 4 bytes, sendo cada byte um número decimal entre 0 e 255.

→ Esses quatro números são divididos por um ponto.

Exemplo

128.2.203.179

IPv4 VS IPv6

Versões diferentes do protocolo de Internet

IPv6: utiliza endereços de 128 bits. Representados por oito grupos de 16 bits, separados por dois pontos e expressos em notação hexadecimal.

) exemplo

0000.3278.0a04.0005.0000.0000.0000.0034

pode ser
condensado → 0:3278:a04:5::34

Endereço IP:

- É preciso conhecer o endereço IP para enviar dados de forma correta entre dispositivos.

Tipos:

- Endereços privados: usados em redes internas e não são acessíveis diretamente da internet.
- Endereços públicos: são únicos e utilizados para identificar dispositivos na Internet.

Atribuição de endereços IP:

- Estáticos: endereços atribuídos permanentemente a um dispositivo.
- Dinâmicos: endereços atribuídos temporariamente (geralmente pelo DHCP - protocolo de Configuração Dinâmica do host).

→ Cada endereço IPv4 não identifica apenas um nó (dispositivo), mas também a rede à qual o nó pertence.

* Bits mais significativos (à esquerda) são usados para identificar a rede.

* Bits restantes são usados para identificar o nó dentro dessa rede.

Se quando tiveres um endereço de nó IPv4 e a máscara de rede é que conseguimos determinar o endereço de rede à qual o nó pertence!

Network Mask

↳ A máscara de rede define quantos bits são usados para identificar a rede e quantos são usados para identificar o host dentro dessa rede.

Numa rede com uma máscara de 24 bits, os primeiros 24 bits do endereço identificam a rede e os 8 bits restantes identificam os hosts dentro dessa rede.

IP: 192.168.1.0

máscara de subrede: 255.255.255.0



então os primeiros 24 bits identificam a rede e o último octeto (com valor 0) será utilizado para os endereços dos hosts dentro dessa rede.

Para calcular o número de nós válidos numa rede:

1. Máscara de rede define N bits para a rede.
2. Os $32 - N$ bits restantes são para os endereços do host.
3. O número total de endereços possíveis é $2^N (32 - N)$.
4. Portanto, dois endereços não podem ser usados:
 - O endereço de rede (primeiro, com todos os bits de host a 0).
 - O endereço de broadcast (último, com todos os bits de host a 1).

Portanto, o nº de nós válidos é: $2^{(32 - N)} - 2$

Ex: Se a máscara for 255.255.255.0 (24 bits de rede)

$$\hookrightarrow 32 - 24 = 8 \text{ bits de host}$$

O prefixo /30

é o menor possível

para redes IPv4

$$\hookrightarrow \text{nº endereços possíveis} = 2^8 = 256$$

↳ 254 nós válidos

utilizáveis (N maior = + redes pequenas com mais dispositivos)

permittendo (N menor = - redes maiores com mais dispositivos em cada uma)

conectar

apenas

dois hosts.

Subnetting: Técnica de dividir redes maiores em sub-redes menores
para usar melhor o espaço de endereços IP.

Private IP addresses

Os endereços IP privados são usados dentro de redes internas e não são rotulados diretamente na internet. Estão definidos em 3 faixas específicas:

- 1) 10.0.0.0 /8 (de 10.0.0.0 a 10.255.255.255)
- 2) 172.16.0.0 /12 (de 172.16.0.0 a 172.31.255.255)
- 3) 192.168.0.0 /16 (de 192.168.0.0 a 192.168.255.255)

→ Para acessar a Internet, utiliza-se o NAT (Network Address Translation), que traduz o endereço privado para um endereço IP público, para a comunicação externa, e ao retornar, converte o IP público novamente para o privado.

Public IP addresses

Os endereços IP públicos são endereços globais e rotulados na internet.

São atribuídos ao roteador da rede pelo provedor de Internet (ISP).

Função: permitem que dispositivos dentro de uma rede privada se comuniquem com o mundo exterior.

IP assignment

1. Atribuição Dinâmica (DHCP):

- A maioria dos dispositivos não precisa de um endereço fixo, apenas os servidores.
- O DHCP atribui automaticamente um IP a dispositivos na rede.

2. Atribuição estática

- Endereço fixo, usado para servidores e dispositivos de rede (routers, switches, firewalls).

Domain Naming System (DNS)

↳ responsável por mapar endereços IP e nomes de domínio numa enorme base de dados distribuída globalmente.

Ex: Quando digitamos `www.isep.ipp.pt`, o DNS converte esse nome de domínio para o endereço IP correspondente.

\$ nslookup www.ese.isep.ipp.pt

↳ para explorar as propriedades de mapeamentos DNS, permitindo consultar um endereço ip associado a um ^{nome} domínio.

Properties of DNS mappings

- Todos os hosts têm um nome de domínio local definido como localhost
- Este nome de domínio está sempre mapeado para o endereço de loopback 127.0.0.1
- O endereço de loopback é usado para estabelecer uma ligação com a mesma máquina.

\$ nslookup localhost

→ saída: Address: 127.0.0.1

\$ hostname

para saber o

nome de domínio

real do host local

→ saída: lmmmacbook.isep.ipp.pt

Mapeamento um-para-um: um nome de domínio pode corresponder a um único endereço ip específico.

\$ nslookup lmmmacbook.isep.ipp.pt

Address: 128.2.210.175

Mapeamento um-para-muitos: vários nomes de domínio podem ser mapeados para o mesmo endereço ip. (frequentemente utilizado em situações como o virtual hosting).

- O servidor web distingue entre os sites através do cabeçalho host em pedidos HTTP

\$ nslookup cs.mit.edu

Address: 18.25.0.23

\$ nslookup eecs.mit.edu

Address: 18.25.0.23

→ O nslookup pode ser usado para:

- obter o endereço ip associado a um domínio
- procurar o nome de domínio associado a um endereço ip

Dominios inválidos ou não configurados:

Nem todos os domínios têm um endereço ip válido associado.

→ Ou porque o nome de domínio ainda não foi configurado ou o endereço ip associado é inválido ou foi removido.

Mapeamento de vários domínios para vários ip's:

Este tipo de configuração é usado principalmente para:

- tolerância à falhas

↳ garante que se um servidor falhar, os pedidos podem ser redirecionados para outro servidor ativo.

- distribuição de carga

↳ permite distribuir o tráfego por vários servidores para evitar sobrecargas e melhorar o desempenho.

\$ nslookup www.dei.isef.ipp.pt

Address: 193.136.62.80

 || || . 81

 || || . 82

Internet Connections

Modelo cliente-servidor: A maioria das aplicações baseia-se neste modelo.

- um processo servidor e um ou mais processos cliente.
- o servidor gera um recurso e fornece serviços manipulando esse recurso para os clientes.
- o servidor é ativado por um pedido de um cliente.

Formas de comunicação:

• TCP (transmission control protocol)

- envia fluxos de bytes por uma conexão orientada;
- garante comunicação confidencial com uma sessão estabelecida entre hosts.

• UDP (user datagram protocol)

- envia datagramas individuais sem manter uma conexão persistente;
- é menos confiável, mas mais rápido e eficiente para certos casos;

Identificação de uma conexão

Identificação única: A conexão é identificada pelos endereços de socket dos pontos finais (par de sockets): (cliaddr: cliport, servaddr: servport).

Exemplo: (128.2.194.242: 51213, 208.216.181.15: 80)

(cliente: IP 128.2.194.242 e porta efimera 51213 (atribuída automaticamente))

Servidor: IP 208.216.181.15 e porta bem conhecida 80 (HTTP).

Virtualization

A virtualização é o processo de criar uma versão virtual de algo que normalmente seria físico, como um computador, sistema operacional (SO), dispositivo de armazenamento ou recursos de rede.

No contexto de virtualização de máquinas, começamos com uma máquina física, que tem hardware (como processadores, memória, dispositivos de entrada/saída) e software (um sistema operacional ativo). O sistema operacional controla o hardware dessa máquina.

→ Com a virtualização, podemos simular máquinas ou sistemas dentro dessa máquina física, permitindo criar várias máquinas virtuais que operam de forma independente, mas compartilham os recursos físicos da máquina real. Desta forma, conseguimos rodar múltiplos sistemas operacionais ou serviços sem precisar de hardware adicional.

Virtualização de hardware (ou virtualização de plataforma) :

- Cria uma máquina virtual que funciona como um computador real, com o seu próprio sistema operacional.
- A máquina física que hospeda a máquina virtual é chamada de host, e a máquina virtual que opera na plataforma é chamada de guest.

Virtualização a nível de aplicação :

- Permite que um aplicativo seja executado em diferentes sistemas operacionais e arquiteturas de computador, de maneira portável.
- O aplicativo é geralmente executado através de um interpretador ou compilador just-in-time (JIT) [Exemplos: Java Virtual Machine, Erlang, Common Language Runtime].

→ Uma máquina virtual simula um computador completo dentro de outro computador, permitindo rodar vários sistemas operacionais ao mesmo tempo, sem que eles interajam entre si (são completamente isoladasumas das outras!).

Cloud Computing

→ Consiste em fornecer recursos de computação, software ou dados de forma compartilhada, como um serviço sob demanda.

→ A virtualização de computação, armazenamento e rede fornece a base para ambientes de nuvem flexíveis e escaláveis.

Hipervisor

↳ O hipervisor é o software que gerencia as máquinas virtuais e permite que várias VMs compartilhem o mesmo hardware físico, sem que o sistema operacional ou os aplicativos percebam.

Tipos de virtualização

- Tipo 1: Nativo / Bare Metal → a principal diferença está na instalação do hipervisor. No tipo 1 ele vai diretamente ser instalado no hardware físico. No tipo 2 ele depende de um sistema operacional existente.
- Tipo 2: Hospedado

A virtualização permite armazenar o estado completo de uma VM num arquivo, incluindo o disco, memória, CPU e dispositivos. Esse estado pode ser salvo em snapshots e restaurado quando necessário.

A migração de VMs permite mover a VM para outro computador, copiando a sua imagem. Isto pode ser feito de forma otimizada enquanto a VM ainda está em funcionamento, num processo chamado migração ao vivo.

↳ oferece flexibilidade e mobilidade

The virtual data center

Clusters de máquinas: um centro de dados virtual é composto por um cluster de máquinas, cada uma a gerir um conjunto de máquinas virtuais. A utilização é otimizada ao colocar muitas VMs em cada nó do cluster.

Recuperação de falhas simplificada: Se o hardware falhar, a imagem da VM pode ser copiada para outro local. Se o software falhar, a VM pode ser reiniciada a partir de um snapshot.

→ O centro de dados virtual pode permitir a terceiros inserir imagens de VMs de forma segura.

→ O hipervisor pode observar e registrar todas as interações de hardware/software das VMs.

Um **Storage Area Network (SAN)** geralmente dá suporte ao Centro de Dados Virtual (VDC), oferecendo armazenamento partilhado e de alto desempenho para as VM's.

→ assegura que as VM's tenham armazenamento rápido e seguro.

Thin Client

Um thin client é um computador leve e otimizado para aceder a aplicações ou áreas de trabalho de uma plataforma de computação baseada em servidor remoto.

- O servidor fornece a maior parte do poder de computação, incluindo o lançamento de programar, execução de cálculos e armazenamento de dados.
- O thin client apenas proporciona entrada/saída para teclado, rato, monitor, som e portas USB.

Containers

Sobre carga associada à implementação em VM's :

1. Sobre carga de I/O : o acesso a dados pode ser mais lento em VM's devido à sobre carga da camada de virtualização.
2. Sobre carga de inicialização do sistema operativo por VM : cada VM precisa de inicializar o seu próprio sistema operativo, o que aumenta o tempo e recursos necessários para iniciar.
3. Sobre carga de memória e disco : Cada VM tem a sua própria cópia do sistema operativo e dos dados, o que resulta em duplicação e utilização inefficiente dos recursos.

Sobre carga torna-se dominante em grande escala : quando se executam muitas VM's num único servidor, a sobre carga de recursos (devido ao sistema operativo de cada VM e ao hipervisor) pode ser significativa.

Comparação com containers →

Containers partilham o sistema operativo do host, o que resulta em menos sobre carga em comparação com as VM's.

→ permitem uma maior densidade de ambientes isolados no mesmo hardware, aumentando a eficiência.

Containers

1. Instâncias isoladas de programas: Um container é uma instância isolada de um programa ou serviço, que executa de forma independente no mesmo sistema.

2. Espaço de utilizador (Kernel partilhado): Ao contrário das VM's, os containers partilham o mesmo kernel do sistema operativo, o que os torna mais leves e rápidos.

3. Isolamento de recursos: Cada container tem acesso apenas aos recursos atribuídos a ele, como ficheiros e dispositivos, garantindo que os programas em containers diferentes não interfiram uns com os outros.

Vantagens dos containers em relação a VM's:

- arranque mais rápido;
- alta densidade;
- baixa sobrecarga de I/O;
- não dependem de suporte CPU especializado

[mais rápidos, leves, eficientes]

Limitações dos containers:

1. complexidade de implementação: a gestão e implementação dos containers é + complexa.

2. Restrição de plataforma: não permitem executar sistemas operativos diferentes no mesmo host (não é possível executar Windows num host Linux). Dependem do kernel do sistema operativo do host.

3. Dificuldade na migração: o estado de um container não é completamente isolado do host, o que dificulta a migração direta entre máquinas.

No prática, os containers só tratados como efêmeros: em vez de migrar, o container antigo é terminado, e um novo é iniciado noutro lugar.

4. Segurança limitada: containers têm acesso a muitos sistemas callidos do kernel, o que aumenta a superfície de ataque. Uma vulnerabilidade no kernel pode comprometer todos os containers a correr no mesmo sistema.

Docker

↳ Combina várias tecnologias do Linux para simplificar a criação e gestão de containers.

Componentes principais do Docker:

1. namespaces:

- Oferecem isolamento de recursos, permitindo que cada container veja apenas uma parte específica do sistema, como interfaces de rede e sistemas de ficheiros.

2. control groups (cgroups):

- Gerem os recursos de hardware, como CPU, memória e disco, garantindo que os containers partilham recursos de forma justa e respeitem limites definidos.

3. UnionFS

- Utiliza sistemas de ficheiros em camadas para tornar os containers leves e rápidos, facilitando o reuso de camadas comuns entre containers.

4. Libcontainer

- Biblioteca que abstrai a complexidade de criar e configurar containers, permitindo uma containerização fácil de aplicações.

Docker client-server architecture

- O cliente envia comandos e pedidos ao servidor (Docker Daemon), que realiza as operações de criar, gerir e distribuir containers.

Funções de cada componente:

• Cliente Docker

- É a interface que o utilizador utiliza para interagir com o Docker.
- Executa comandos como docker build, docker run ou docker push.

• Docker daemon

- É o serviço que executa as tarefas principais: construir, gerir e executar containers e manipular imagens Docker.

• Conexão cliente - servidor

- O cliente e o Daemon comunicam através de uma API REST, utilizando:
 - Sockets Unix (em sistemas locais)
 - Interfaces de Rede (para ligações remotas)

Summary

Máquinas virtuais vs containers

Máquinas Virtuais (VMs)

Vantagens

- isolamento forte e segurança entre ambientes;
- permitem rodar diferentes sistemas operativos no mesmo hardware;
- suportam migração prática, sendo possível mover VM's entre máquinas físicas;

Desvantagens

- Demora no arranque do sistema operativo;
- Sobrecarga significativa de disco, memória e hipervisor;

Containers

Vantagens

- arranques rápidos (milisegundos);
- sobrecarga de I/O praticamente nula;
- alta densidade, permitindo milhares de containers numa única máquina;

Desvantagens

- Isolamento de segurança mais fraco, dependendo do Kernel partilhado.

* As técnicas complementam-se em muitos casos:

- Utilizar VM's para isolar utilizadores diferentes (melhor segurança);
- Utilizar containers para isolar aplicações/serviços de um único utilizador (maior eficiência).