



Computação em Nuvem

Fernando Antonio Mota Trinta

Virtualização

Virtualização

- *Não é um conceito recente...*
 - 1960 – IBM M44/44X
 - 70s – OS/370
- *Desinteresse com a chegada do PC*
 - Simples e versátil
 - Sem recursos para virtualização
- *Retomada com novas aplicações*
 - Máquina Virtual Java
 - Computação em Nuvem



O que seria virtualizar?

- Técnica que “mascara” as características físicas de um recurso computacional dos sistemas, aplicações ou usuários que os utilizam (*Enterprise Management Association*)
 - Desktops remotos, de discos virtuais
- O termo máquina virtual foi introduzido na década de 60 como um conceito de sistemas operacionais para indicar uma abstração em software de um sistema computacional em hardware.

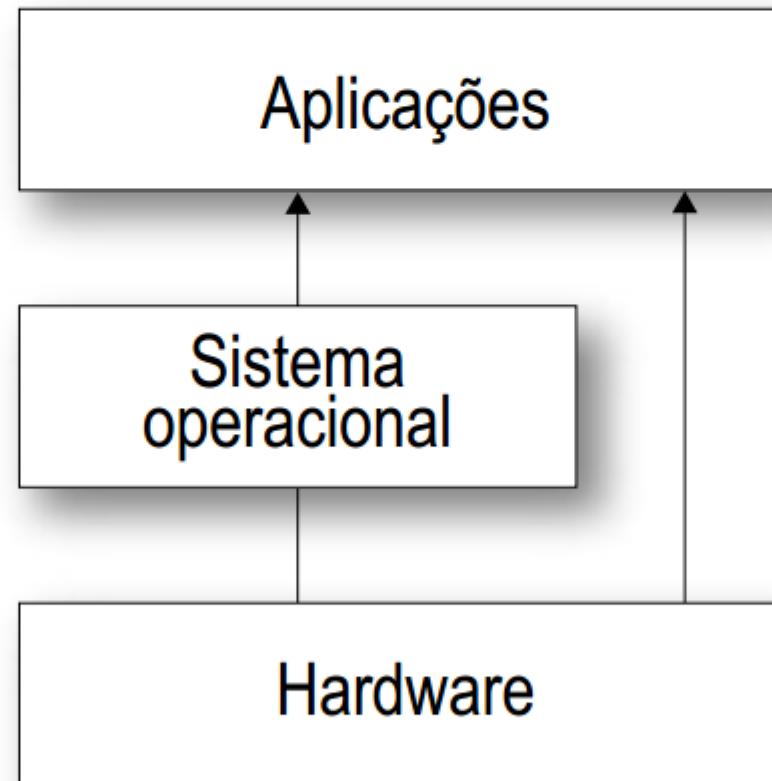


Por que virtualizar?

- *Diminuição de custos*
 - *Uso eficiente de recursos por compartilhamento*
 - *Aumento do ROI (Return on Investment)*
 - *Diminuição de Despesas de Capital e Operação*
- *Aumento no tempo de vida uma tecnologia*
- *GreenIT*
 - *Diminuição de uso de recursos energéticos*



Por que virtualizar?



Por que virtualizar?

- As *interfaces existentes entre os componentes de um sistema de computação* são:
 - *Conjunto de instruções (ISA – Instruction Set Architecture)*
 - *Instruções de usuário (User ISA)*
 - *Instruções de sistema (System ISA)*
 - *Chamadas de sistema (syscalls)*
 - *Chamadas de bibliotecas (libcalls)*

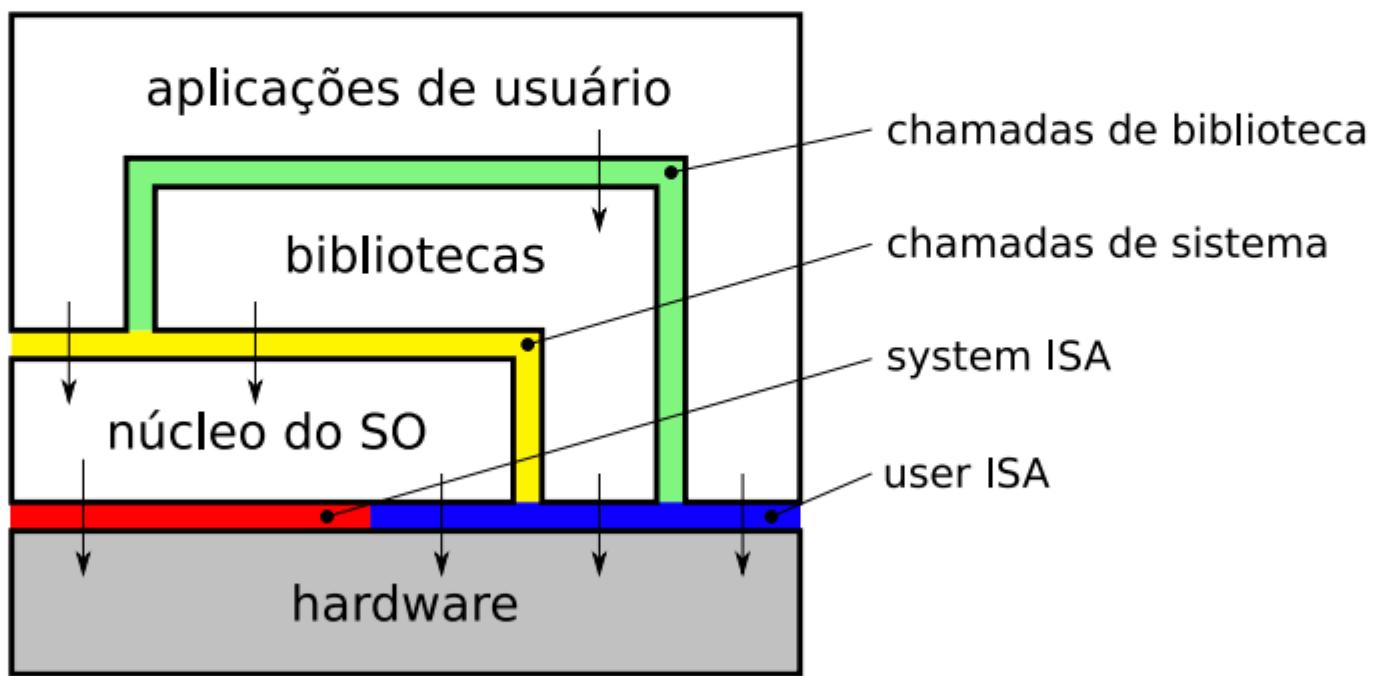


Desvantagem

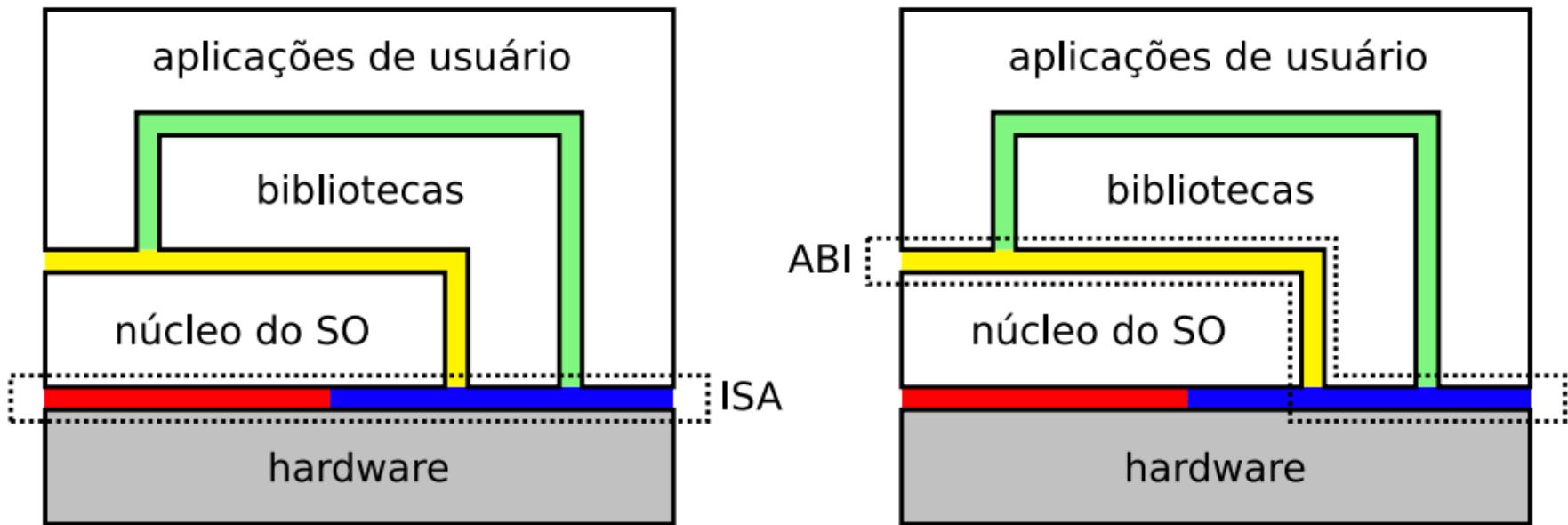
- *Principal problema com a virtualização é questão do desempenho*
 - *Camadas a mais de tradução das instruções causam um overhead no tempo de sua execução*



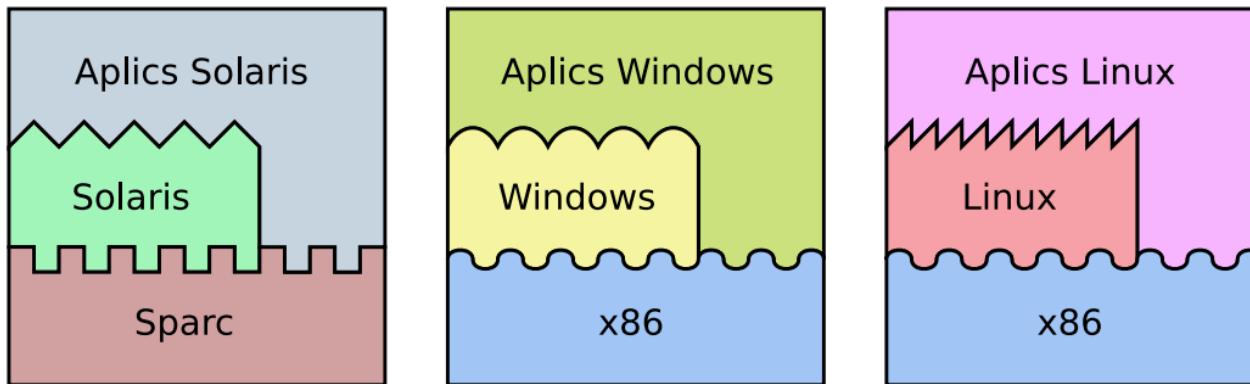
Por que virtualizar?



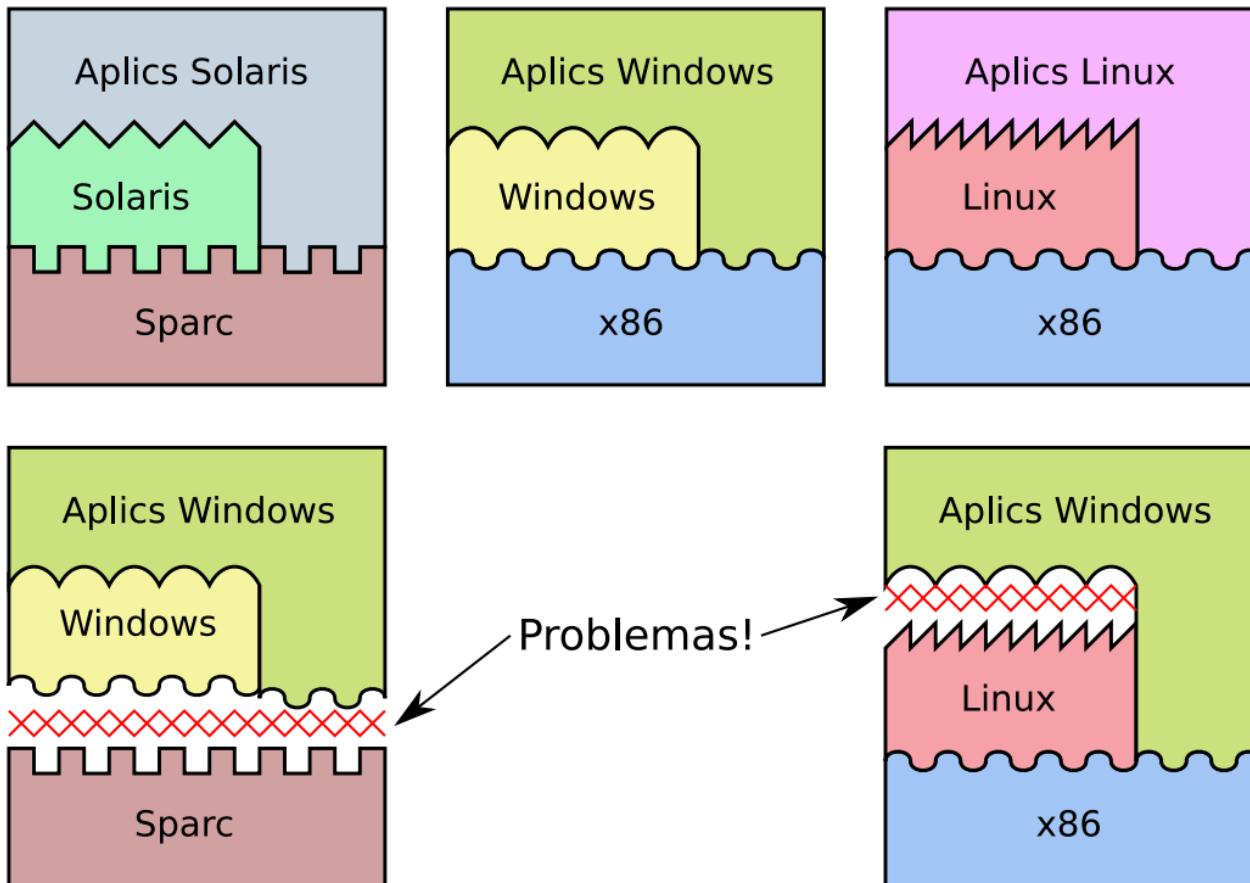
Compatibilidade entre interfaces



Compatibilidade entre interfaces

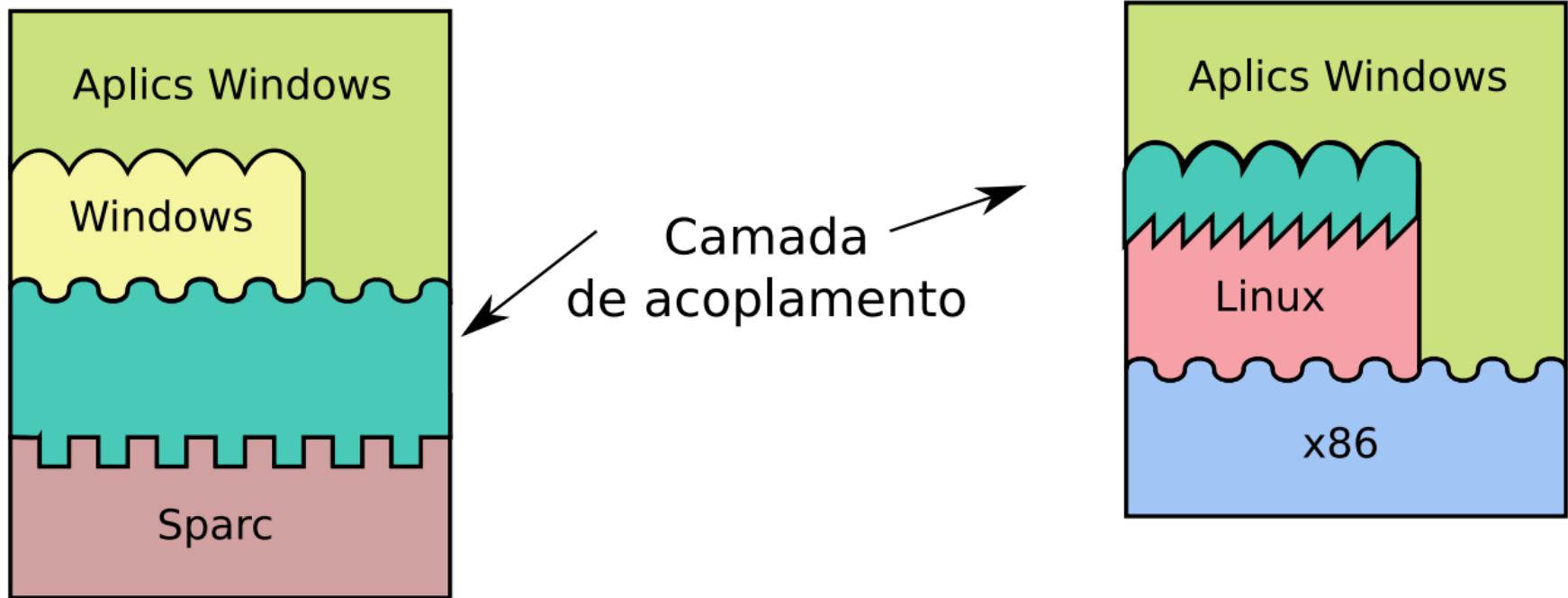


Compatibilidade entre interfaces

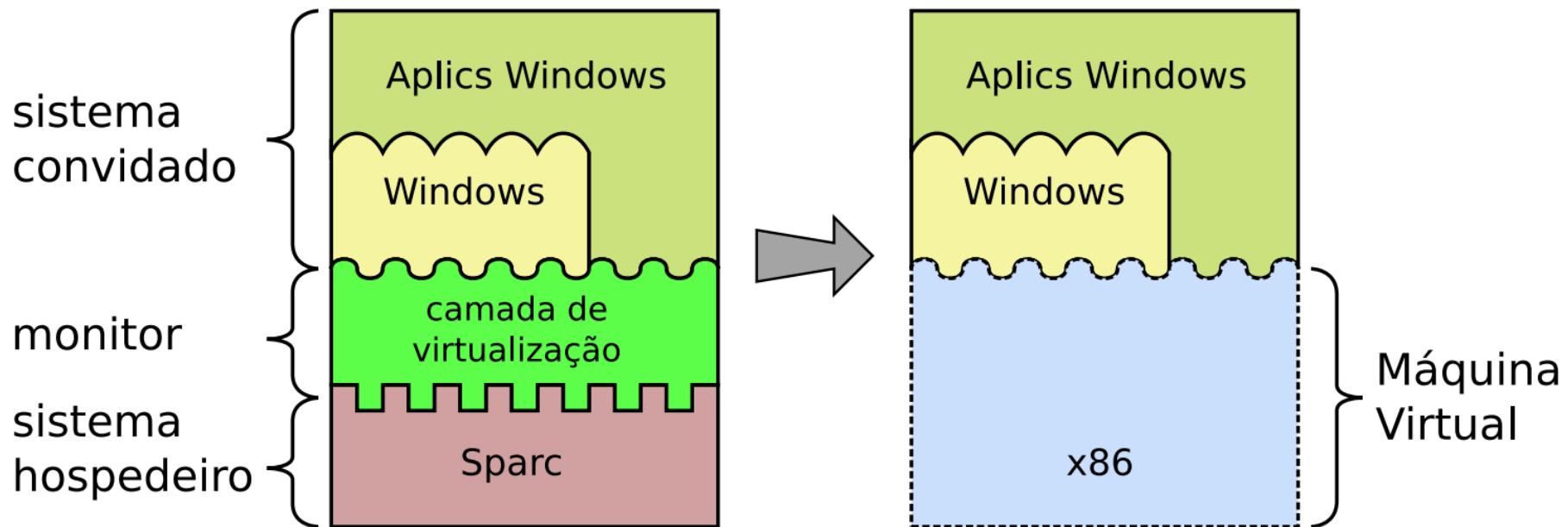


Resolvendo a incompatibilidade

■ *Camada de Virtualização*



Componentes da Virtualização



Três elementos básicos

- *O sistema real, nativo ou hospedeiro (host system), que contém os recursos reais de hardware e software do sistema;*
- *o sistema virtual, também denominado sistema convidado (guest system), que executa sobre o sistema virtualizado; em alguns casos, vários sistemas virtuais podem coexistir, executando simultaneamente sobre o mesmo sistema real;*
- *a camada de virtualização, hipervisor, ou monitor (VMM – Virtual Machine Monitor), que constrói as interfaces virtuais a partir da interface real*



Hypervisor

■ *Definição: software que faz com que um servidor suporte a implantação de MVs. É responsável por suportar esta abstração, e interceptar e emular algumas instruções emitidas pelas MVs*

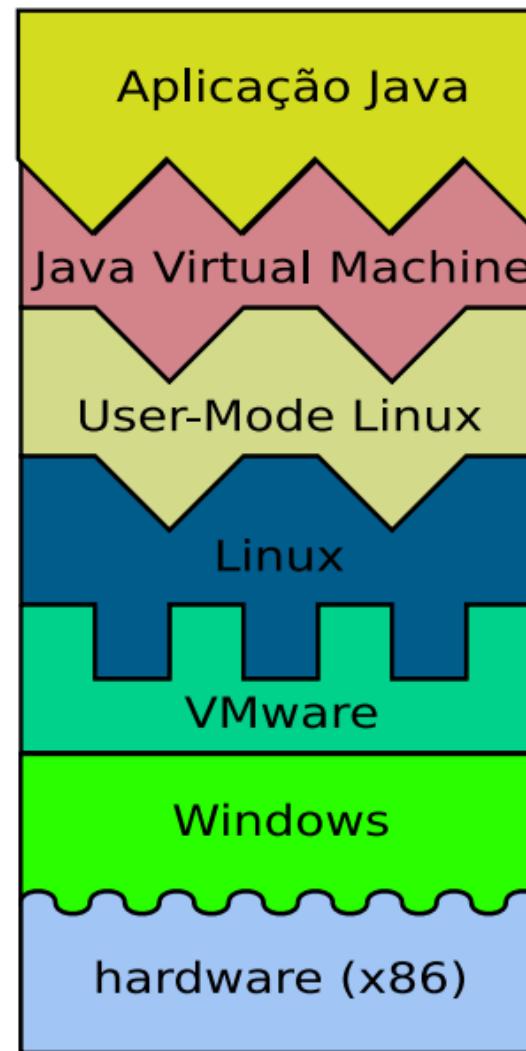
- *Provê uma interface que permite ao usuário inicializar, pausar, serializar e desligar múltiplas MVs*

■ *Propriedades*

- | | |
|-------------------------------|------------------------|
| □ <i>Equivalência</i> | □ <i>Isolamento</i> |
| □ <i>Controle de recursos</i> | □ <i>Inspeção</i> |
| □ <i>Eficiência</i> | □ <i>Recursividade</i> |



Recursividade no Hypervisor



Tipos de Hypervisor

■ *Tipo I (nativo ou bare metal)*

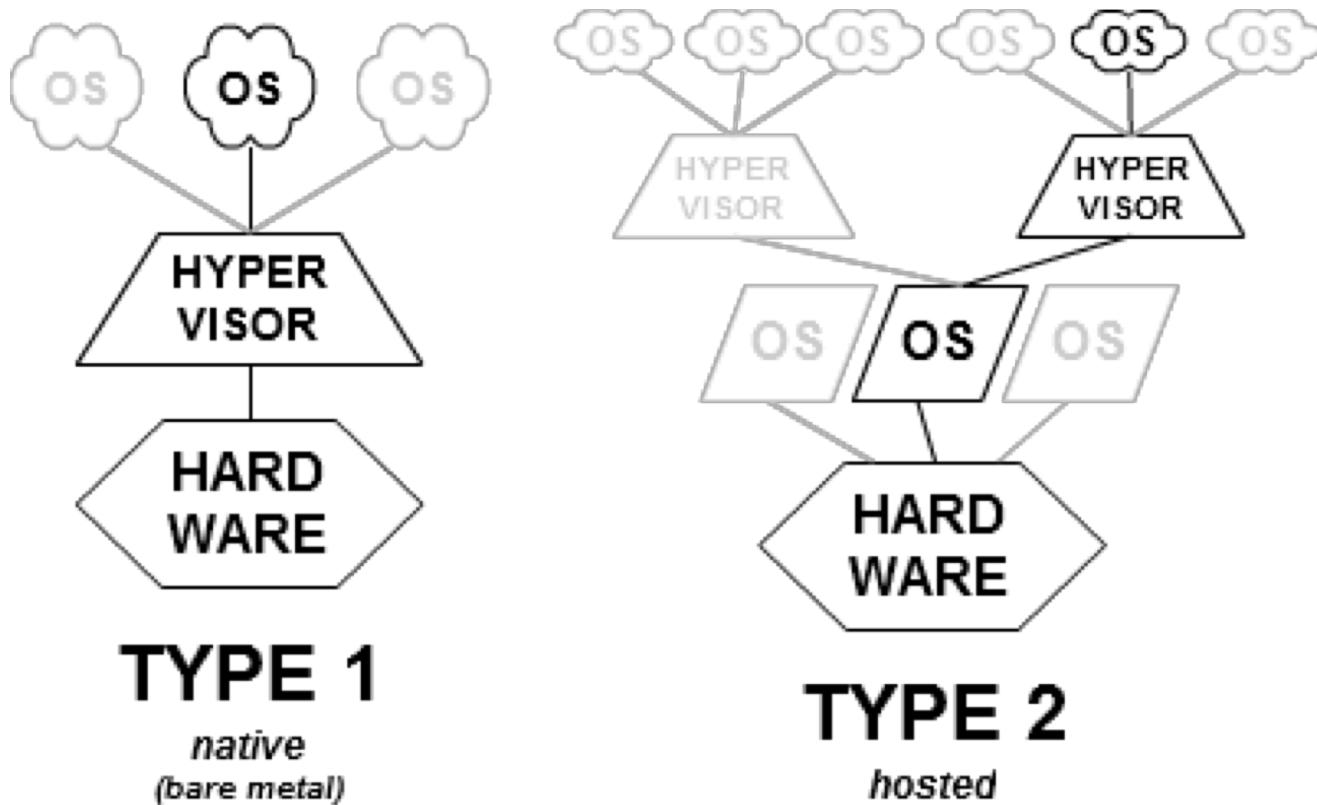
- *Conversa diretamente com o hardware*
- *As MVs rodam diretamente sobre ele*
- *Exemplos:*
 - Citrix XenServer, KVM, VMware ESX/ESXi, Microsoft Hyper-V

■ *Tipo 2 (hosted)*

- *É executado sobre um sistema operacional normal*
- *As MVs roda sobre estas 2 camadas de software*
- *Exemplos:*
 - VMware Workstation e VirtualBox



Tipos de Hypervisor



Tipos de Virtualização (o que virtualizar)

- *Virtualização do SO*
 - *SO em um servidor, cópias a seus usuários*
- *Virtualização de Servidores*
 - *Servidores virtuais compartilhando mesmo hardware*
- *Virtualização de Memória*
 - *Pool de memória disponível compartilhada entre clientes*
- *Virtualização de Armazenamento*
 - *Cloud Storage*
 - *Ex: Dropbox*
- *Virtualização de Rede*
 - *Switchs, roteadores e placas de rede virtuais*
- *Virtualização de Aplicações*



Abordagens de Virtualização

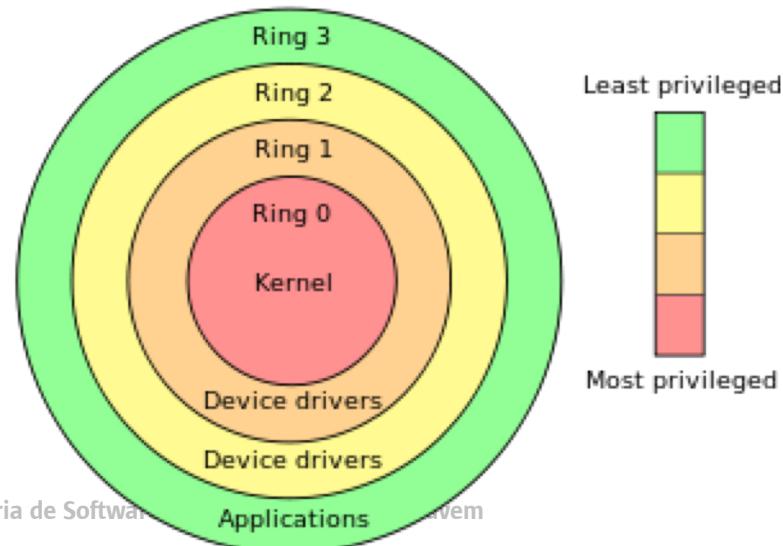
- Existem diferentes maneiras de se implementar virtualização
- Tipos:
 - Virtualização total (*full virtualization*)
 - Paravirtualização (*paravirtualization, PVM*)
 - Virtualização ao nível do sistema operacional (*OS-level virtualization*)
 - Virtualização assistida por hardware (*hardware-assisted virtualization, HVM*)
- A principal diferença entre elas é a maneira como as instruções privilegiadas das MVs chegam de fato ao hardware.



Abordagens de Virtualização

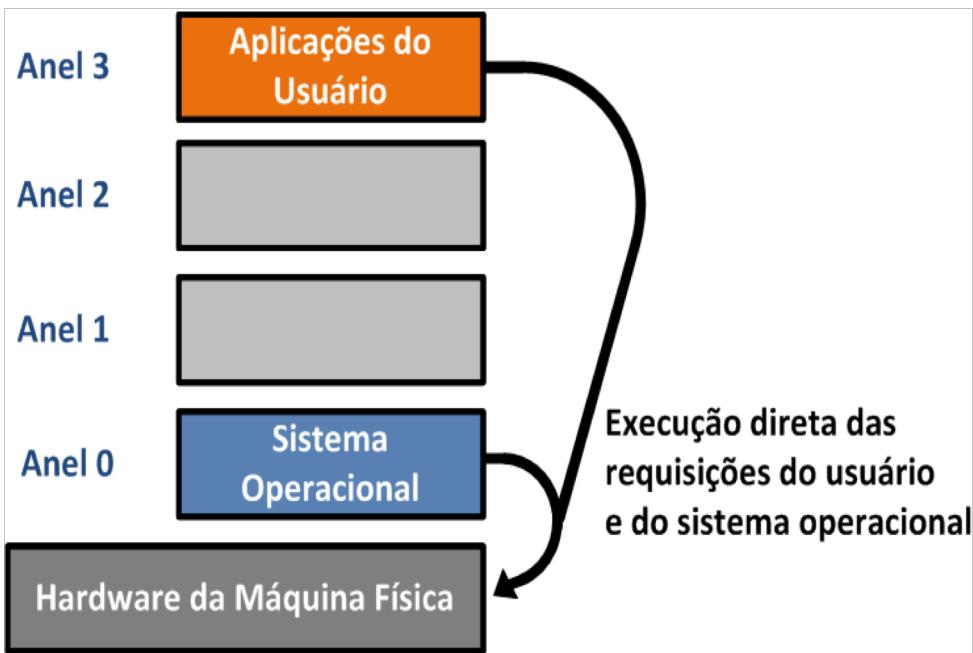
■ Arquitetura x86

- SOs x86 são projetados para funcionar diretamente sobre o hardware, de modo que, naturalmente, eles assumem que têm o controle total sobre o hardware.
- A arquitetura x86 oferece quatro níveis de privilégio, conhecidos como Anel 0, 1, 2 e 3, para sistemas operacionais e aplicativos poderem gerenciar o acesso ao hardware do computador.



Abordagens de Virtualização

■ Níveis de privilégio da arquitetura x86



Algumas instruções sensíveis não podem ser virtualizadas, pois têm semânticas diferentes quando não são executadas no Anel 0

Capturar e traduzir estes pedidos de instrução sensíveis e privilegiadas, em tempo de execução, foi o desafio que originalmente fez a virtualização da arquitetura x86 parecer impossível



Tipos de Virtualização

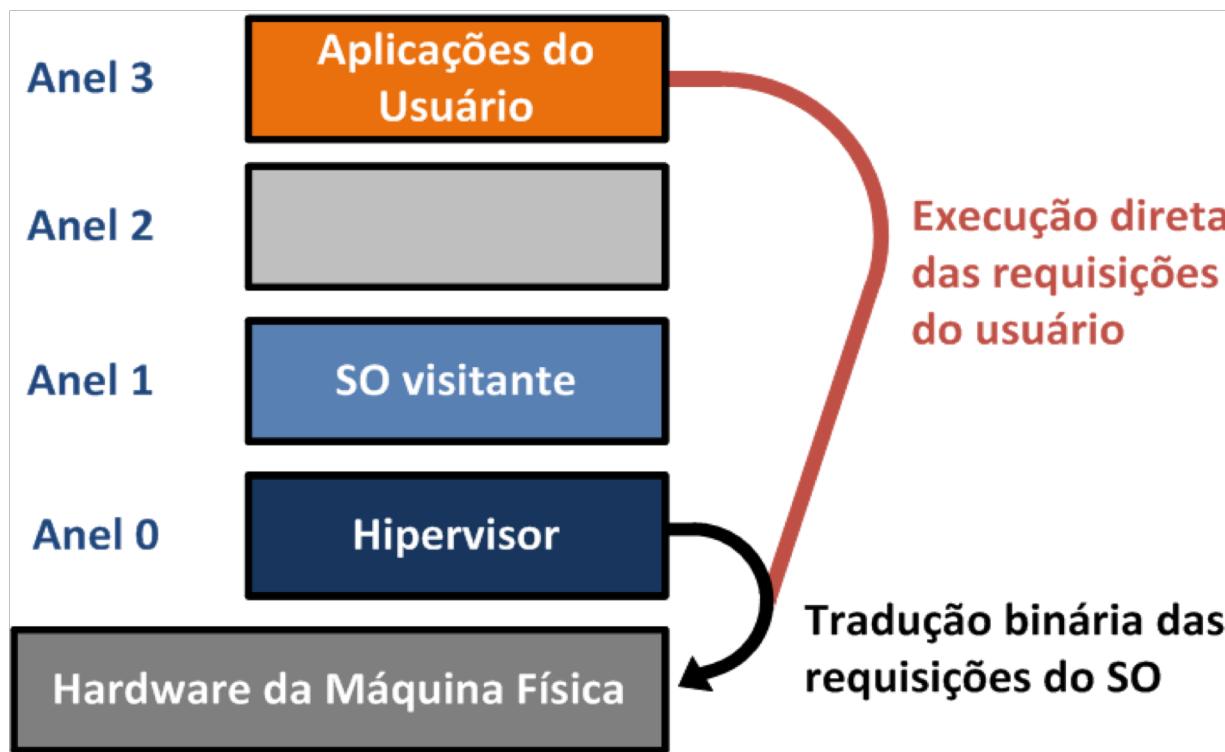
■ Virtualização total

- Fornece uma simulação completa do hardware subjacente através da emulação de hardware
- Dispositivos de hardware artificiais são criados com tudo o que é preciso para executar um SO, sem a necessidade de modificar o kernel do SO visitante
- Utiliza-se uma combinação de tradução binária e técnicas de execução direta para executar as chamadas do sistema
- Chamadas são interceptadas pelo hipervisor, que as mapeia para o hardware real subjacente, enquanto parte do código do nível do usuário pode ser executado diretamente no processador para obter um melhor desempenho
- O SO visitante não tem conhecimento de que está sendo executado em hardware virtualizado
- Exemplos: VMWare Workstation e Virtual Box



Tipos de Virtualização

■ Virtualização total



Tipos de Virtualização

■ Paravirtualização

- Kernel do SO visitante é modificado especificamente para executar no hipervisor
- Envolve a substituição de quaisquer operações privilegiadas, por chamadas para o hipervisor, conhecidas como hiperchamadas (*hypercalls*)
- O hipervisor, por sua vez executa a tarefa em nome do kernel da MV e também fornece interfaces de hiperchamada para outras operações críticas do kernel
- Tenta corrigir os problemas da virtualização total permitindo que os SOs visitantes tenham acesso direto ao hardware subjacente
- SO visitante sabe que está sendo executado em hardware virtualizado
- Exemplo: Xen



Tipos de Virtualização

■ *Full Virtualization*

□ Pros

- *Maior isolamento e segurança entre MVs*
- *Diferentes SOs convidados em execução simultânea*
- *SO convidado sem alteração*
 - *Permite migrar para acesso convencional*

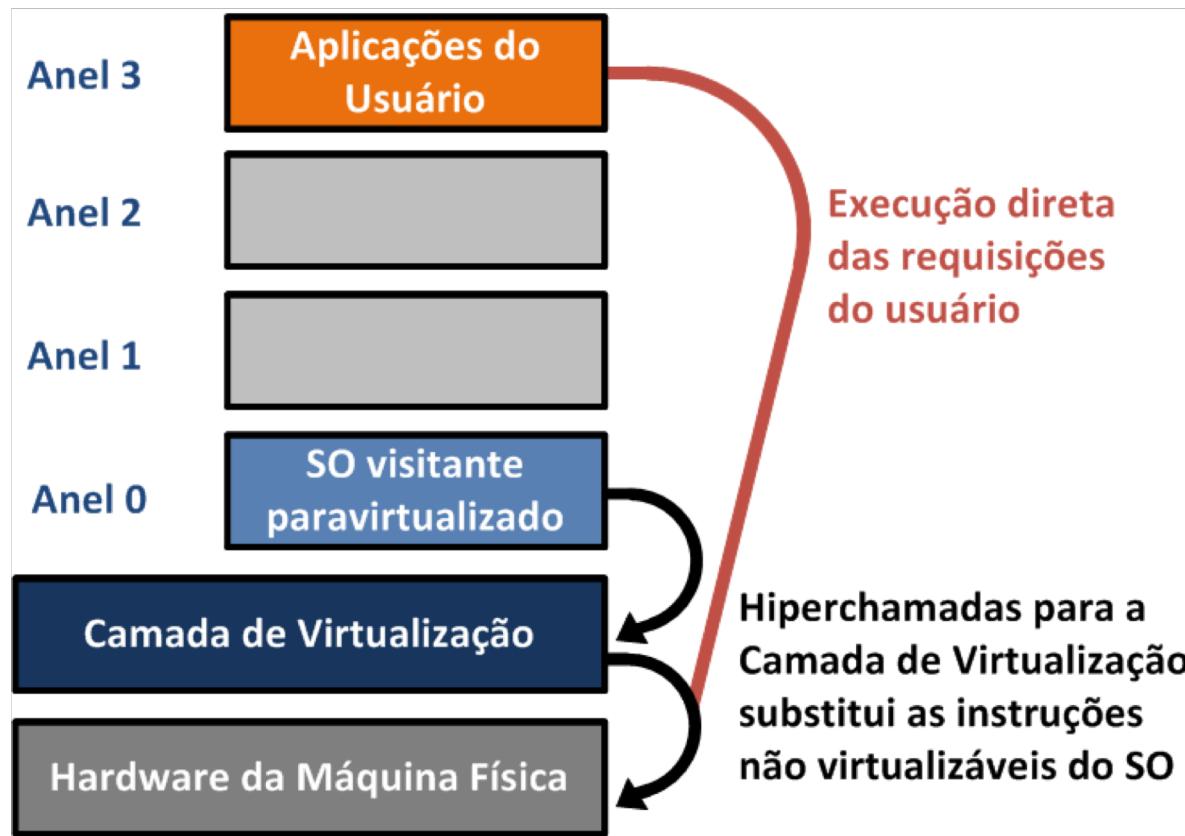
□ Cons

- *Tradução Binária*
 - *Overhead*
- *Necessário suporte adequado entre hypervisor/hardware*



Tipos de Virtualização

■ Paravirtualização



Tipos de Virtualização

■ *ParaVirtualization*

□ Pros

- *Sem overhead de tradução binária*

□ Cons

- *Modificação no SO convidado*
 - *Impossibilita migração para hardware*
- *Falta de retrocompatibilidade*



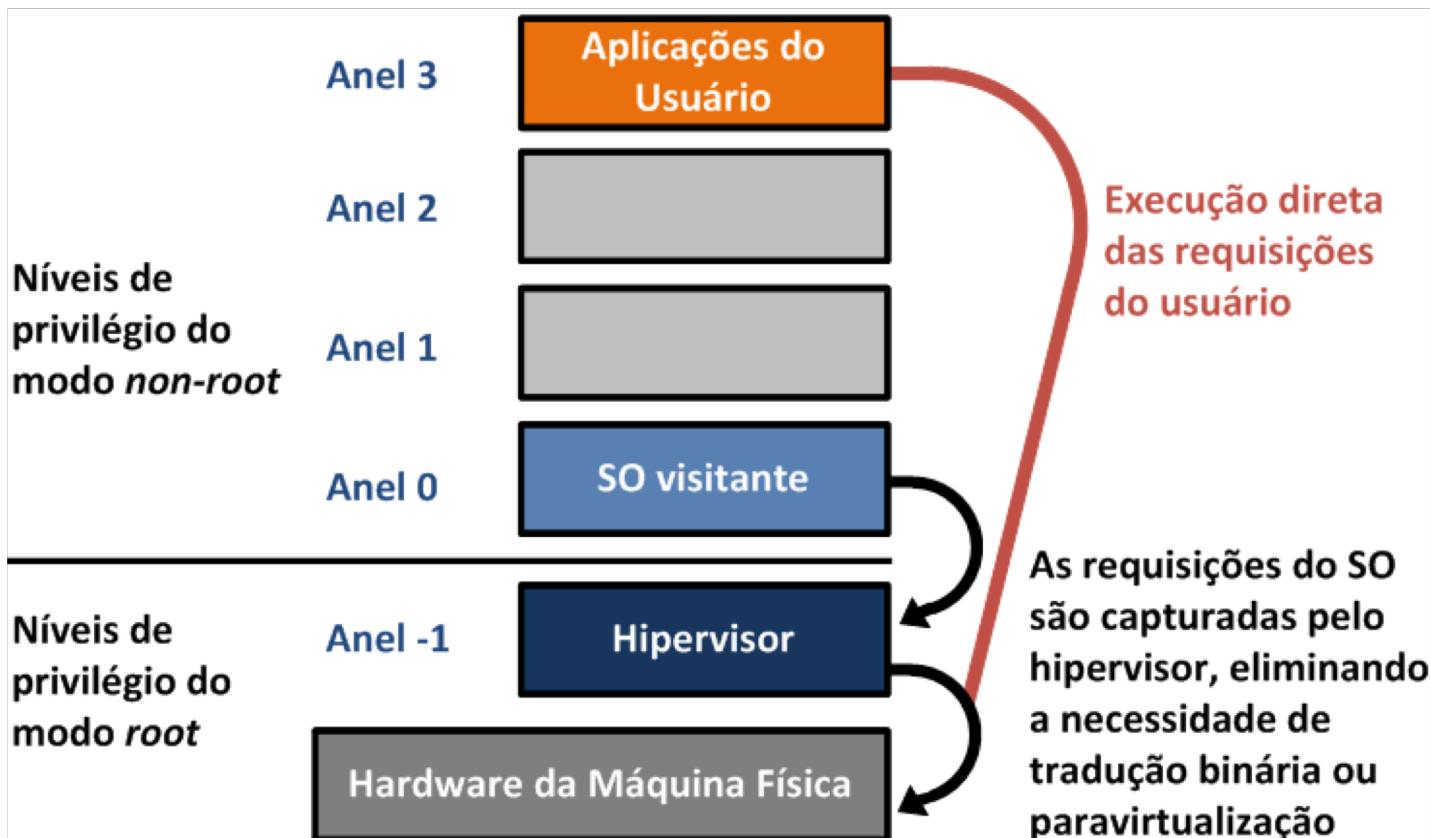
Tipos de Virtualização

- *Virtualização assistida por hardware*
 - Recursos de virtualização adicionados nas últimas gerações de CPUs
 - *Tecnologias Intel VT e AMD-V : oferecem extensões necessárias para executar MVs com SO não modificado, sem as desvantagens inerentes à emulação de CPU da virtualização total*
 - Processadores novos fornecem modo de privilégio adicional (Anel - I)
 - Hipervisor virtualiza eficientemente todo o conjunto de instruções x86
 - *Os hipervisores que suportam esta tecnologia podem funcionar no Anel - I e os SOs visitantes podem utilizar a CPU no Anel 0, como fariam normalmente se estivessem sendo executados numa MF*
 - SOs visitantes não precisam ser modificados
 - *Exemplos: KVM, QEMU, modo HVM do Xen*



Tipos de Virtualização

■ Virtualização assistida por hardware



Tipos de Virtualização

■ *ParaVirtualization*

□ Pros

- *Sem overhead de tradução binária*
- *Sem modificação do SO convidado*

□ Cons

- *Disponibilidade apenas processadores de nova geração*



Outras questão importante

- Segurança
 - Novos tipos de Ameaça
 - Ataques ao SO Convidado
 - Ataques ao SO Hospedeiro

