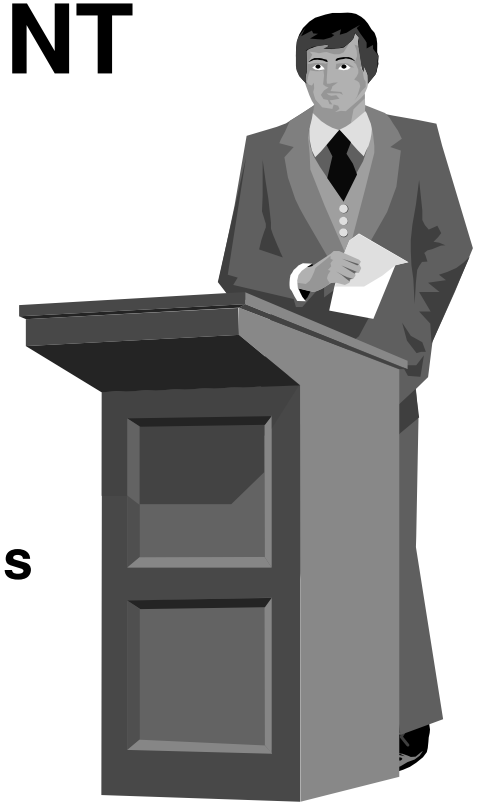
Estudo de Caso
Arquitetura Windows NT

Volnys Borges Bernal
volnys@lsi.usp.br

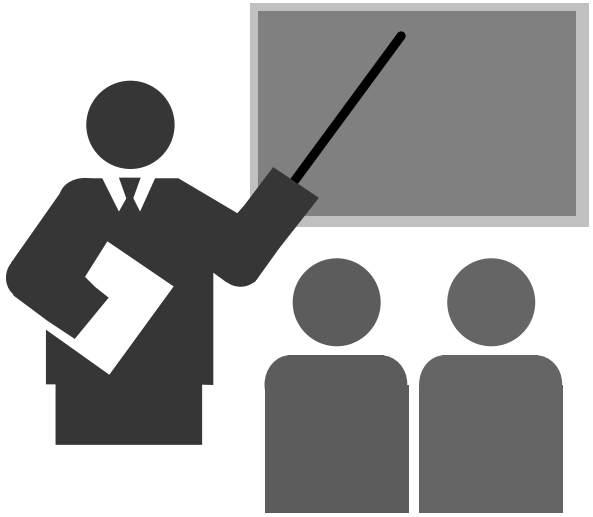
Laboratório de Sistemas Integráveis
http://www.lsi.usp.br/



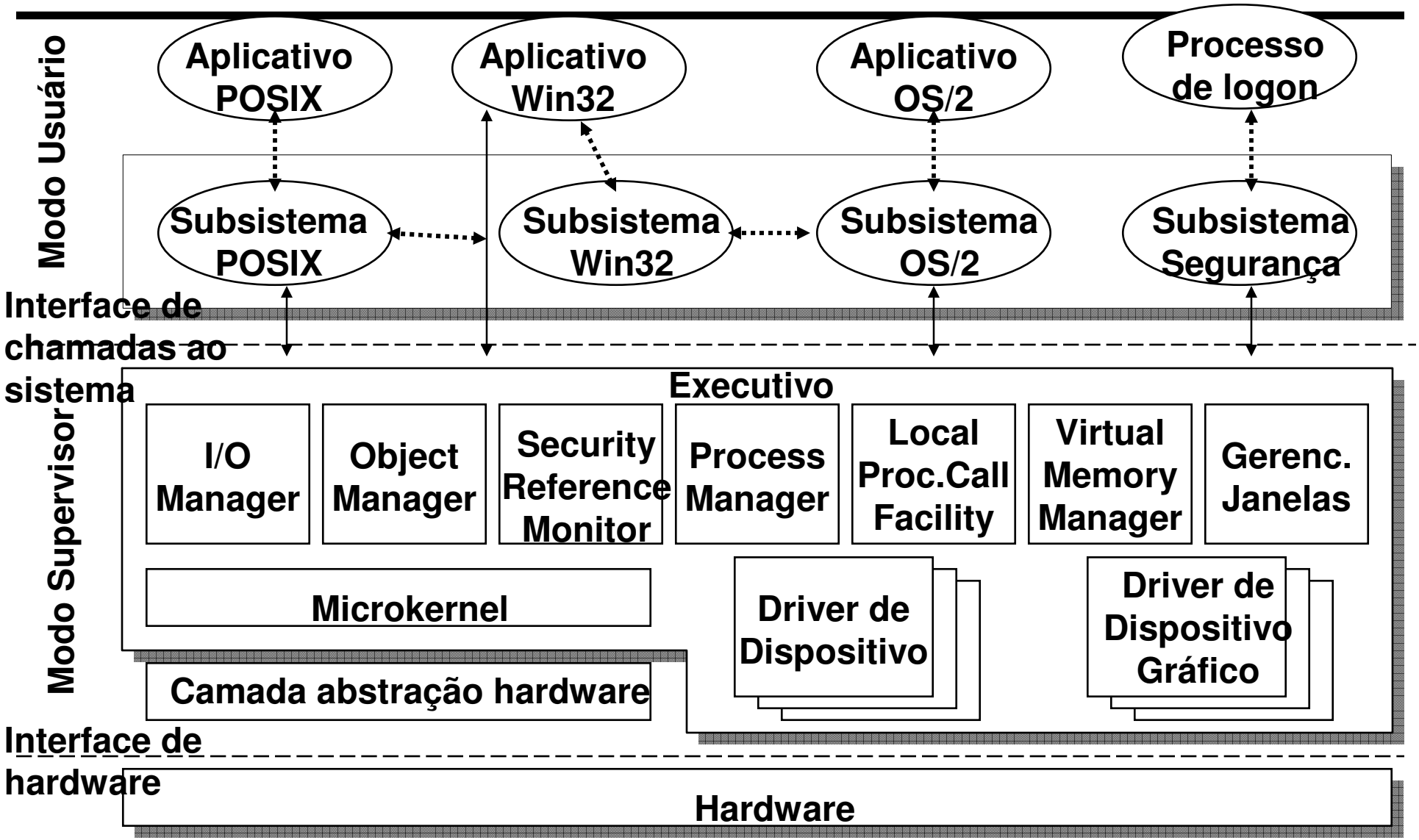
Estudo de Caso: arquitetura Windows NT

- **Sumário:**
  - Visão geral da arquitetura Windows NT
  - Interação entre aplicação e kernel Windos NT
  - Interação entre aplicação e subsistema

Visão geral da Arquitetura WindowsNT



Visão geral da arquitetura WindowsNT



Visão geral da arquitetura WindowsNT

- **Interface de chamadas ao sistema**
  - Chamada também de Interface NT nativa
  - Define o conjunto de serviços que o sistema operacional fornece aos processos: ~250 funções
  - Chamada ao sistema é implementada através de TRAP
    - TRAP = interrupção de software
    - Permite garantir que somente o "*kernel* do NT" será executado em modo supervisor
      - As interrupções são atendidas em modo supervisor
      - O vetor de interrupções é controlado pelo *microkernel*

Visão geral da arquitetura WindowsNT

- **Executivo**
  - Características
    - Monolítico
      - Imagem ntoskrnl.exe contém todo código dos serviços executivos (exceto o Microkernel)
    - Multi-threaded
    - Reentrante

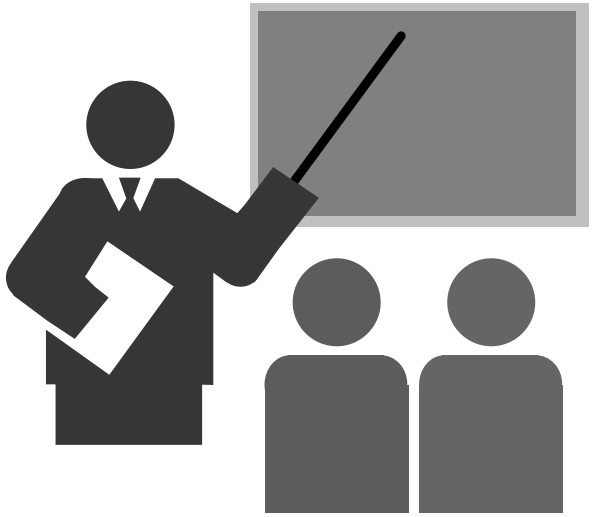
Visão geral da arquitetura WindowsNT

- **Microkernel (também chamado de NT kernel)**
  - Responsável por
    - Escalonamento de *threads* (*dispatcher*)
    - Sincronização
    - Manipulação dos vetores de interrupção
  - Implementa 32 níveis de prioridade
  - Implementa escalonamento preemptivo
  - Implementa sincronização baseada em:
    - *mutex*
    - semáforos
    - eventos
    - *spinlocks*

Visão geral da arquitetura WindowsNT

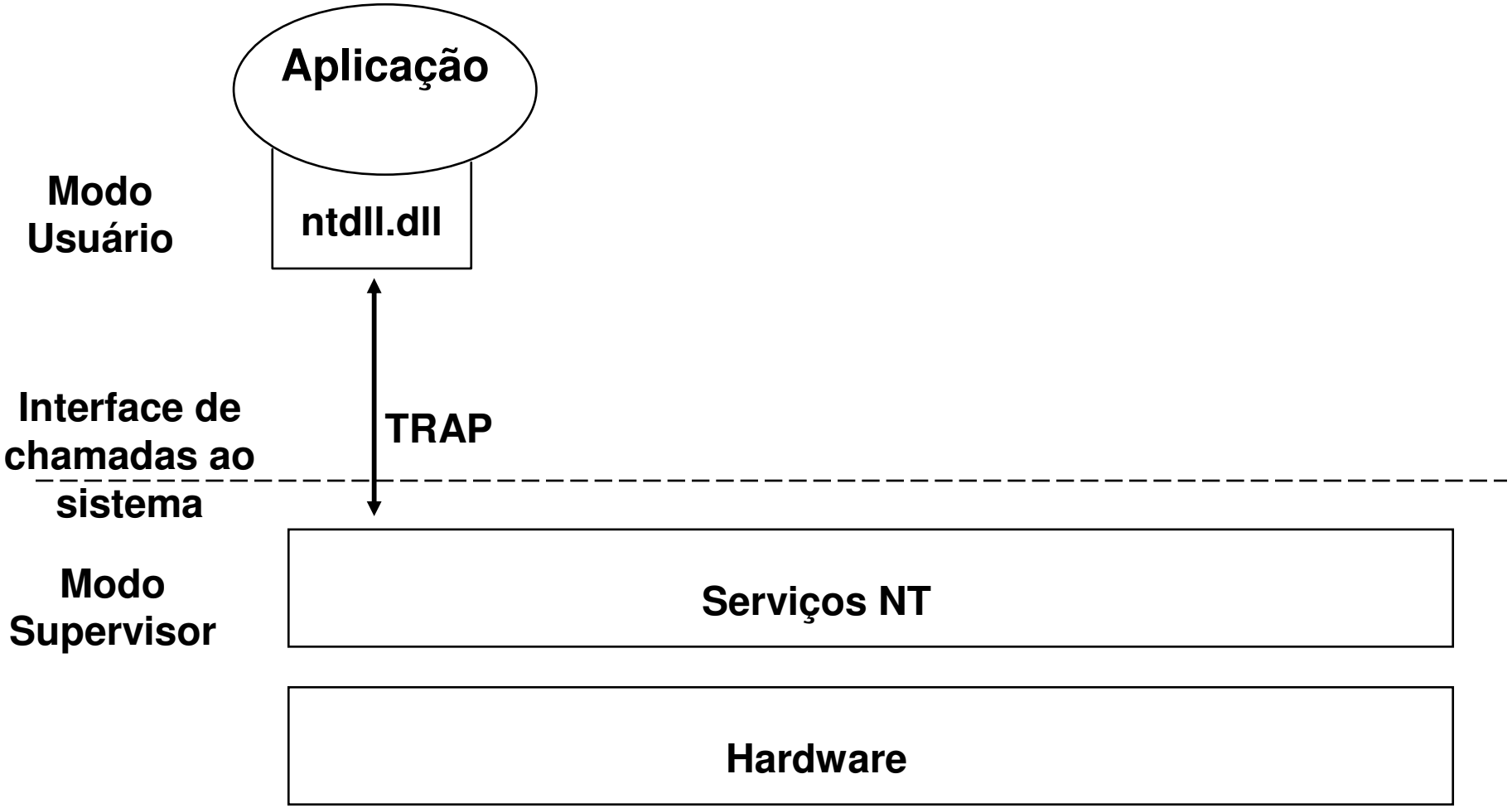
- **HAL**
  - *Hardware Abstraction Layer*
    - (camada de abstração de hardware)
  - Camada utilizada para esconder dependências de arquitetura
  - Exemplo:
    - Sistemas monoprocessadores x multiprocessadores
    - Para cada versão NT são fornecidas 3 versões
      - monoprocessador
      - multiprocessador
      - para depuração (p/ desenvolvimentod e device drivers)

Interação entre aplicação e kernel Windows NT



Interação entre aplicação e kernel

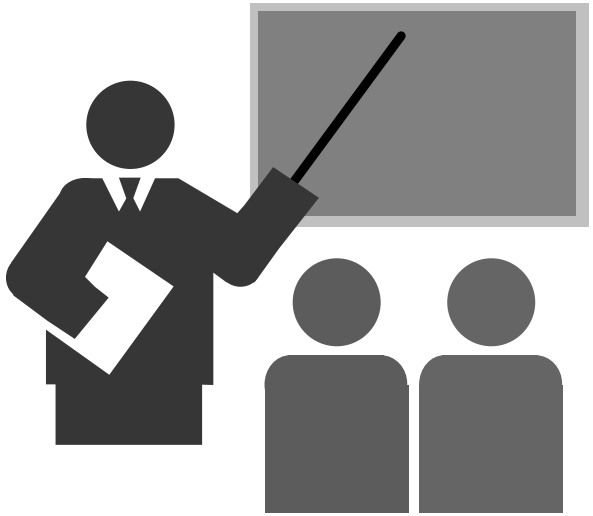
- **Interação entre aplicação e kernel WindowsNT**



Arquitetura WindowsNT

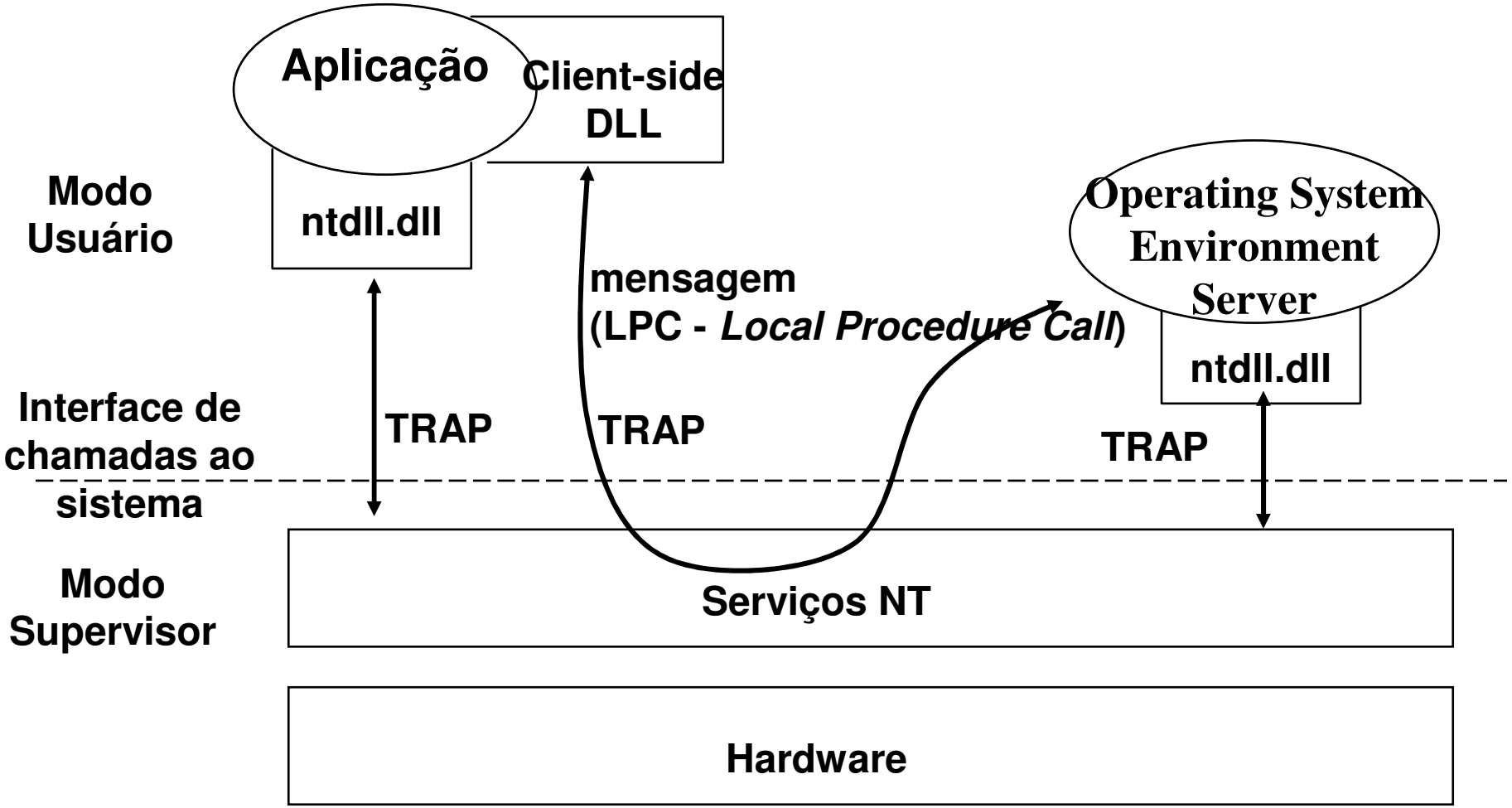
- **Biblioteca NTdll.dll**
  - Biblioteca que fornece funções que encapsulam as chamadas ao sistema WindowsNT

Interação entre aplicação e subsistema



Interação entre aplicação e subsistema

- Interação entre aplicações: LPC (Local Procedure Call)

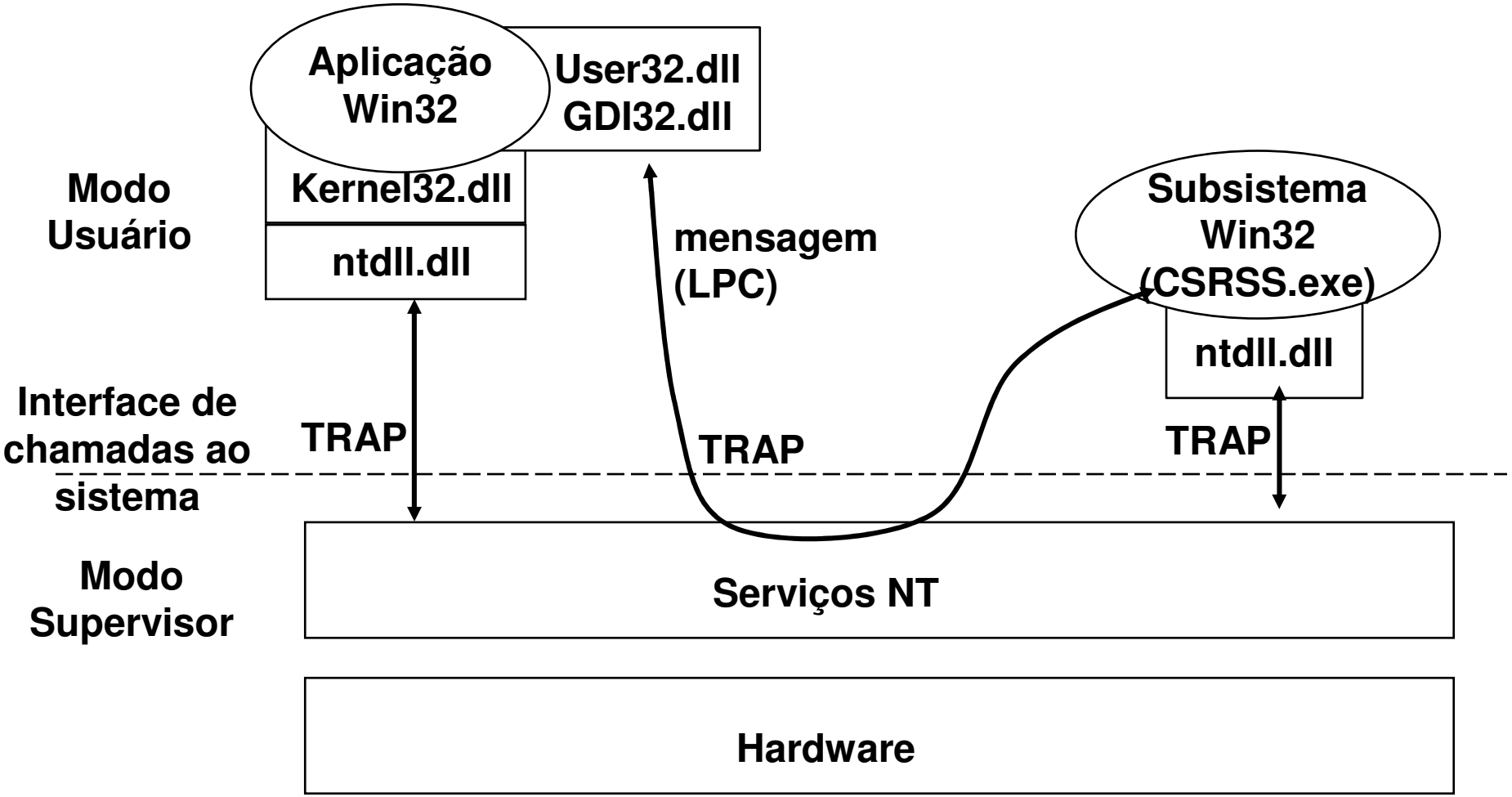


Interação entre aplicação e subsistema

- **LPC x TRAP**
  - LPC possui maior sobrecarga:
    - Cada interação envolve geralmente 2 mensagens (pedido e resposta)
    - Para cada mensagem ocorre:
      - 1 TRAP
      - 1 troca de contexto
        - troca da tabela de páginas
        - atualização de informações de escalonamento
        - troca de todos os registradores
        - ....
  - TRAP é menos custosa
    - envolve somente uma interrupção de software
    - necessário salvar somente parte dos registradores
    - ao final é necessário restaurar os registradores salvos

Interação entre aplicação e subsistema

- **Exemplo: aplicação Windows32**

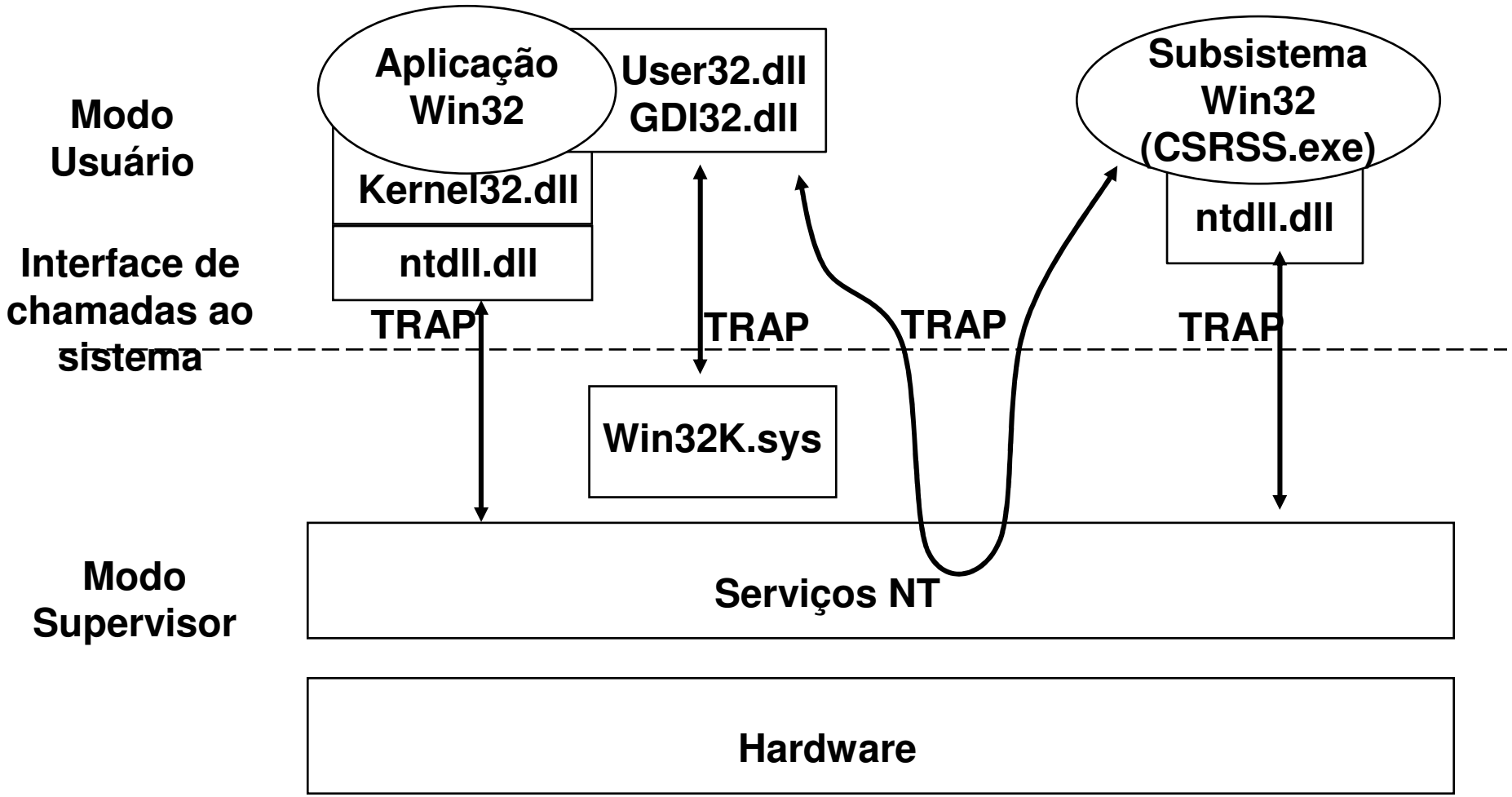


Interação entre aplicação e subsistema

- **Aplicação Windows32 em versão Windows NT 3.51 ou anterior**
  - Utiliza serviços do sistema através das bibliotecas:
    - KERNEL32.dll
    - USER32.dll
    - GDI32.dll
  - KERNEL32.dll
    - A maior parte das funções fornecidas ativam diretamente uma ou mais chamadas nativas WindowsNT.
  - USER32 e GDI32
    - Ativam os serviços do Subsistema Windows32
  - CSRSS.EXE
    - Este processo é o Subsistema Windows32
  - Referência:
    - http://www.windowsitlibrary.com/Content/356/03/1.html

Interação entre aplicação e subsistema

- **Exemplo: Aplicação Windows32 (WindowsNT4 e W2k)**

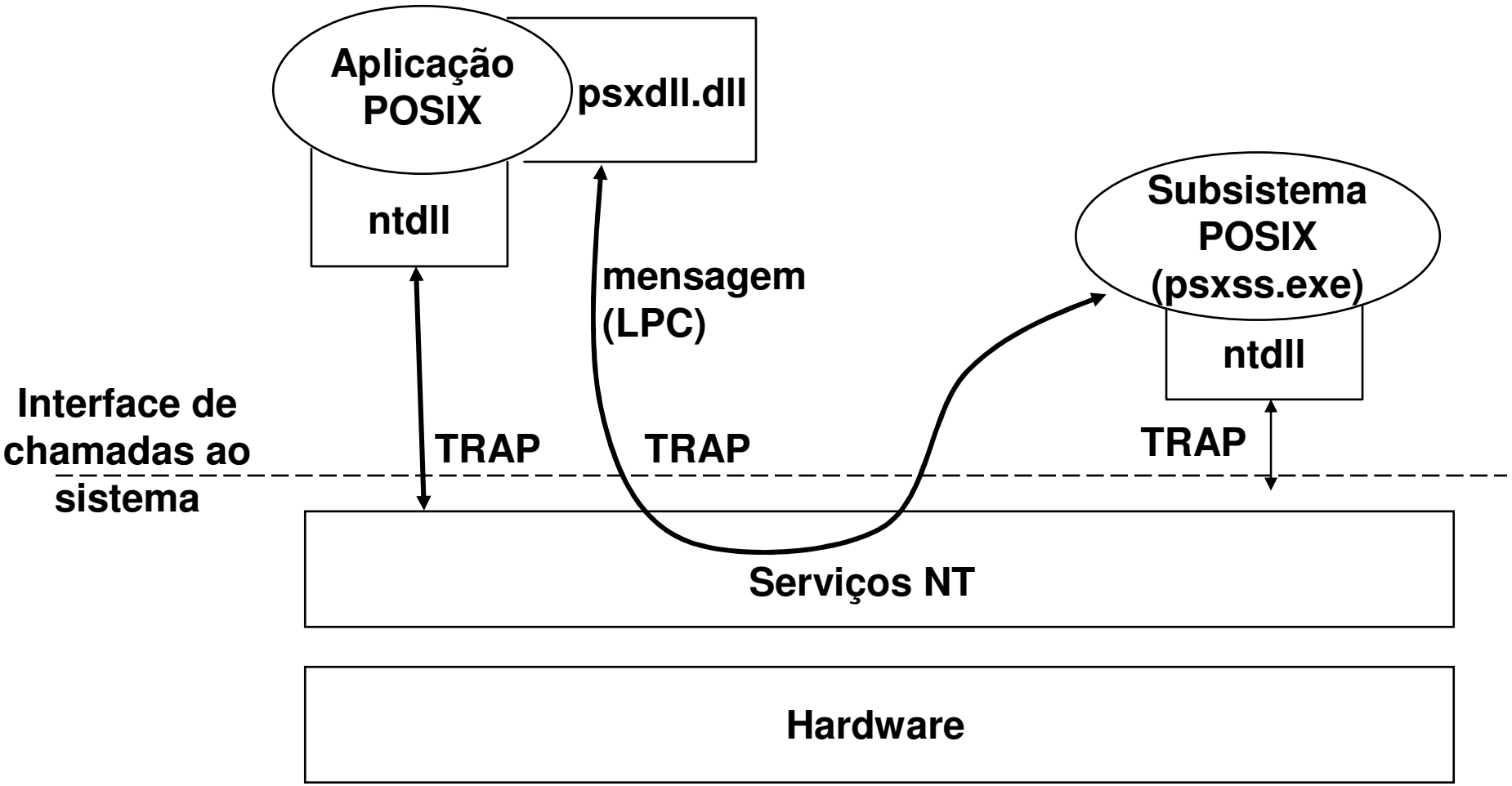


Interação entre aplicação e subsistema

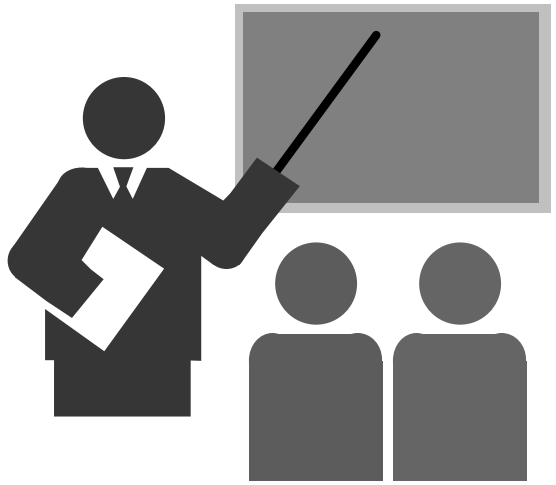
- **Aplicação Windows32 em versão Windows NT 4.0 ou superior (incluindo Windows 2000, Windows 2003)**
  - Utiliza serviços do sistema através das bibliotecas:
    - KERNEL32
    - USER32
    - GDI32
  - Win32k.sys
    - Devido à problemas de desempenho, as bibliotecas USER32 e GDI32 ativam os serviços através de uma chamada a um driver chamado Win32k.sys que é executado em modo supervidor (kernel mode). Tais bibliotecas contém *stubs* que ativam estes serviços utilizando a interrupção 0x2E. A maior parte das funcionalidades foi retirada do Subsistema Windows32 (CSRSS.EXE) e implementada neste driver.
  - CSRSS.EXE
    - Este processo (Subsistema Windows32) ainda é mantido. Entretanto seu papel é limitado a manter suporte a E/S de console.

Interação entre aplicação e subsistema

- **Exemplo: Aplicação POSIX**



Referências Bibliográficas



Referências Bibliográficas

- **Windows 2000 Magazine Online**
  - http://www.winntmag.com/Articles

- **http://www.windowsitlibrary.com/Content/356/03/1.html**