STRUKTURA OS TYPU WINDOWS

IT3-OS-02 (20. 10. 2024)

Prezentace vysvětluje základní struktury používané v operačních systémech Windows. Pokrývá různé typy architektur, včetně monolitických a modulárních struktur, vrstveného uspořádání a modelu klient-server. Dále se zaměřuje na rozdělení systému na režim jádra a uživatelský režim, což zvyšuje stabilitu a bezpečnost systému. Prezentace také popisuje vývoj a rozdíly mezi staršími systémy Windows (např. MS-DOS) a novějšími verzemi, jako je Windows NT a jeho následníci, které používají víceprocesorové a víceuživatelské struktury.

ZÁKLADNÍ POJMY KE STRUKTURÁM OS (I.)

Monolitická struktura je nejjednodušší struktura používaná v jádrech operačních systémů nebo v zařízeních (tiskárny). Systém se skládá z jádra a rozhraní, které zprostředkovává komunikaci mezi jádrem a okolím.

Vrstvená (hierarchická) struktura - části systému jsou uspořádány do vrstev, každá vrstva využívá služeb nižších vrstev, ne naopak. Každá vrstva komunikuje právě jen s okolními vrstvami. Systém je budován od vnitřních vrstev k vnějším, proto vnitřní vrstvy, které jsou obvykle nejdůležitější z hlediska stability a bezpečnosti, bývají nejlépe otestovány.

ZÁKLADNÍ POJMY KE STRUKTURÁM OS (II.)

Virtuální počítače (virtuální stroje) - systém je rozdělen do samostatných modulů (virtuálních počítačů, virtuálních zařízení), každý z nich je zhruba stejně vybaven prostředky (čas procesoru, paměť, apod.), obvykle se nemohou příliš vzájemně ovlivňovat kromě základní komunikace mezi procesy (např. předávání dat a jiných informací).

Abstraktní počítače - systém je také rozdělen na části (resp. některé části jsou vyděleny), ale na rozdíl od virtuálních počítačů abstraktní počítače mají každí svou specifickou funkci

ZÁKLADNÍ POJMY KE STRUKTURÁM OS (III.)

Modulární struktura - systém je členěn do modulů, které lze podle potřeby přidávat (nejlépe za běhu systému). U tohoto typu struktury se předpokládá unifikované rozhraní modulů, přes které může systém komunikovat i s takovým modulem, který v době vzniku systému ještě neexistoval.

Model klient-server - systém má co nejmenší jádro (minikernel, mikrokernel), které obsahuje pouze základní funkce (obvykle pouze funkce řídící činnost ostatních částí systému, jako je přepínání mezi procesy a řízení mechanismu zasílání zpráv mezi procesy), ostatní funkce systému provádějí speciální systémové procesy, které nazýváme servery. Procesy, které spouští uživatel (nejsou systémové), se nazývají klienty, využívají služeb procesů typu server.

MS-DOS

MS-DOS je jednoprocesorový jednouživatelský jednoprogramový lokální univerzální systém. Samotný MS-DOS bez spuštěné nástavby Windows má velmi jednoduchou vrstvenou strukturu. Nejblíže hardwaru je BIOS (Basic Input-Output System) a dále soubor IO.sys, který se stará o obsluhu periferií.

BIOS poskytuje programátorům základní ovládání hardwaru přes *hardwarová a softwarová přerušení*.

Vrstva samotného jádra systému představovaná souborem **MSDOS.SYS** (monolitické jádro). Poskytuje další *softwarová přerušení*, například pro přístup k souborům nebo pokročilejší práci s grafikou.

Vrstva **COMMAND.COM** je textové rozhraní mezi uživatelem a systémem. COMMAND.COM obsahuje sadu vnitřních příkazů. Ostatní příkazy se nazývají vnější příkazy a jsou implementovány jako programy s příponou .exe nebo .com.

Poslední vrstva je k "zjednodušení práce" uživatele. Kromě uživatelem spuštěných programů zde řadíme i dva konfigurační soubory:

- CONFIG.SYS pro nastavení hardwaru
- AUTOEXEC.BAT pro nastavení softwaru

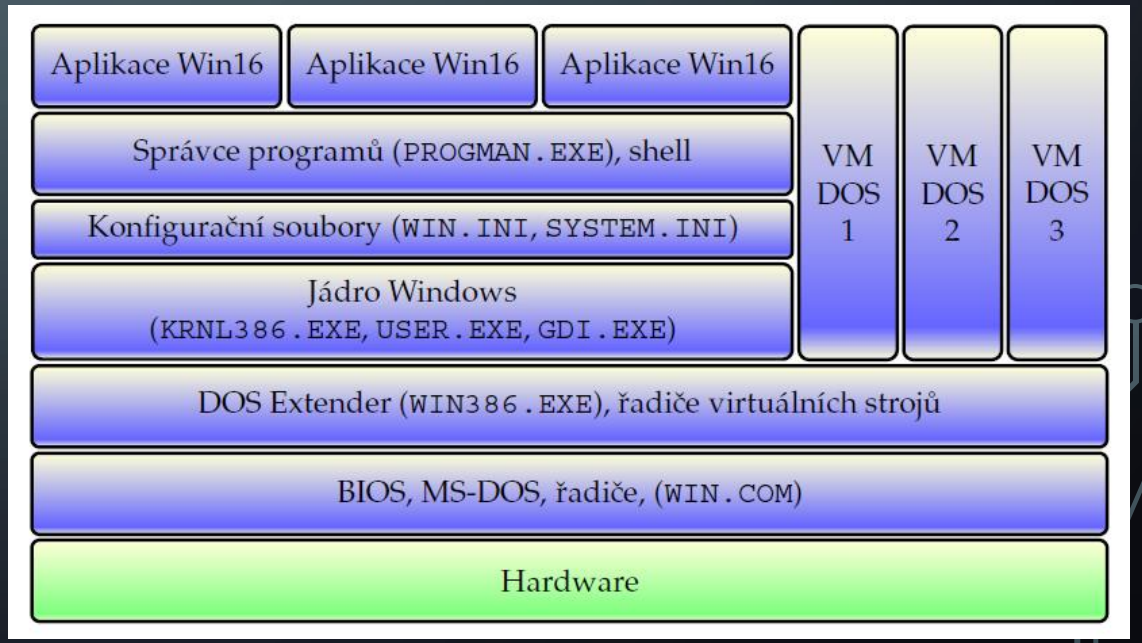
MS-DOS A WINDOWS DO VERZE 3.X (I.)

Když v MS-DOSu 6.22 spustíme **Windows 3.x** struktura systému se v horní části změní. Spodní je část shrnuta (BIOS, MSDOS.SYS) a je k nim je přidán soubor WIN.COM (spuštění Windows) a dále řadiče (ovladače). Windows přidávají multitasking, 16bitové knihovny a ve verzi *3.11 for Workgroups* základní podporu sítě (pouze síť peer-to-peer).

Řadiče (ovladače, drivery) ovládají periferní zařízení pro Windows; řadiče přímo pro Windows jsou spouštěny v souboru SYSTEM.INI pomocí příkazu DEVICE.

DOS Extender je modul pro podporu využití rozšířené paměti (Extended Memory). Je představován souborem Win386.EXE.

Součástí tohoto souboru je také Správce virtuálních zařízení (VMM = Virtual Machine Manager), který ovládá možnosti Windows pro souběh s programy DOSu. Řadiče virtuálních zařízení (VxD) jsou řadiče, které správce virtuálních zařízení potřebuje pro manipulaci s I/O zařízeními pro programy DOSu v rozšířeném módu.



MS-DOS A WINDOWS DO VERZE 3.X (II.)

V další vrstvě je jádro Windows (jádrem OS zůstává MSDOS.SYS), které zde pracuje jako správce prostředků vzhledem k programům běžícím pod Windows (i DOS programům zde spuštěným). Má tři části (soubory:

- **KRNL386.EXE** - plní především úlohu správce paměti a správce procesů (řízení přidělování paměti procesům, přidělování prostředků systému procesům, ...),
- **GDI.EXE** - rozhraní grafického zařízení (obsahuje funkce pro kreslení úseček, vytváření kurzoru, ikony, písmo, ...), cokoliv souvisí se základními funkcemi pro grafický výstup (na obrazovku, tiskárnu apod.),
- **USER.EXE** - uživatelské rozhraní, zdroje, které nepatří do GDI (dialogová okna, menu, okna, tlačítka, ...).

V další vrstvě najdeme konfigurační soubory s příponou **.INI**. Z nich jsou nejdůležitější WIN.INI (konfigurace software a nastavení pro urč. uživatele) a SYSTEM.INI (konfigurace hardware). INI soubory mohou mít také různé programy.

MS-DOS A WINDOWS DO VERZE 3.X (III.)

Následuje vrstva, která rozhraním mezi uživatelem, programy a samotným systémem. Soubor **PROGMAN.EXE** je Správce programů, shell je grafické a textové rozhraní mezi uživatelem a systémem.

Zde zařadímet část **API rozhraní** (Application Programming Interface) reprezentovaného dynamicky linkovanými knihovnami a využívaného procesy pro přístup k systému. Knihovny celého API rozhraní jsou však v různých vrstvách, patří zde také soubory jádra KRNL386.EXE, USER.EXE a GDI.EXE.

Všechny dosud uvedené vrstvy platí pro aplikace psané pro Windows (16bitové aplikace pro Windows do verze 3.x).

DOS programy horní vrstvy nevyužívají. Samotný MS-DOS je jednoprogramový systém, jsou programy napsány bez jakýchkoliv ohledů multitasking. Jsou separovány je do virtuálních počítačích (**VM DOS**), které vytvoří iluzi výlučné existence.

WINDOWS S DOS JÁDREM

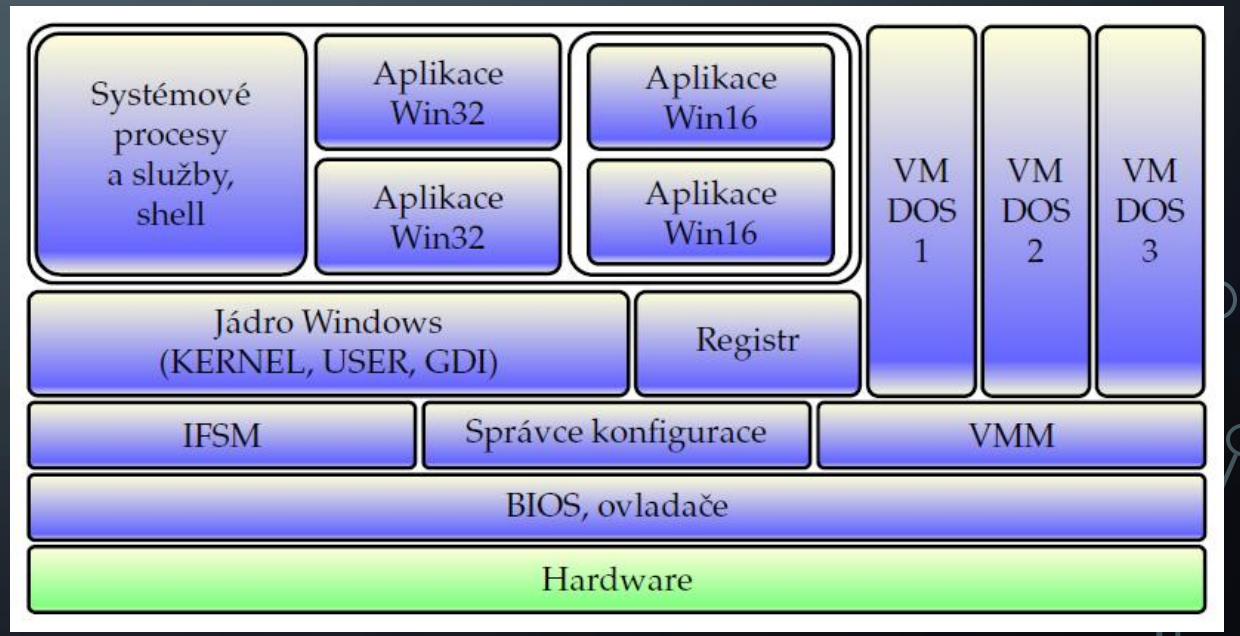
Jedná se již o 32b systém, ale některé knihovny zůstávají 16b.

Nad BIOS jsou nově tři moduly:

VMM je správce virtuálních zařízení (Virtual Machine Manager), vytváří a udržuje prostředí virtuálních počítačů,

IFSM je správce instalovatelných souborových systémů (Installable File Systems Manager),

Správce konfigurace spravuje ovladače hardware na vyšší úrovni, včetně funkce Plug&Play.



WINDOWS S DOS JÁDREM – POPIS JÁDRA

Jádro se skládá ze tří modulů, každý z nich má dvě dynamicky linkované knihovny (jedna pro 16bitové aplikace s příponou EXE, druhá pro 32bitové aplikace s příponou DLL):

- **KERNEL** - multithreading, multitasking, správa paměti, synchronizace objektů, vstupu a výstupu u souborů, atd.,
- **GDI** (Graphics Device Interface) - rozhraní grafických zařízení (obrazovka, tiskárna, plotter, atd.),
- **USER** - také jako u předchozího jde o uživatelské rozhraní (pozor, nejen grafické), tedy vstupy z klávesnice, myši apod.

Registr (Windows Registry) je centrální informační databáze systému, najdeme zde většinu toho, co ve Win 3.x bylo v ini souborech (ty jsou však zachovány kvůli zpětné kompatibilitě). Fyzicky je uložen v souborech SYSTEM.DAT a USER.DAT (*pouze ve Win 9x/ME*).

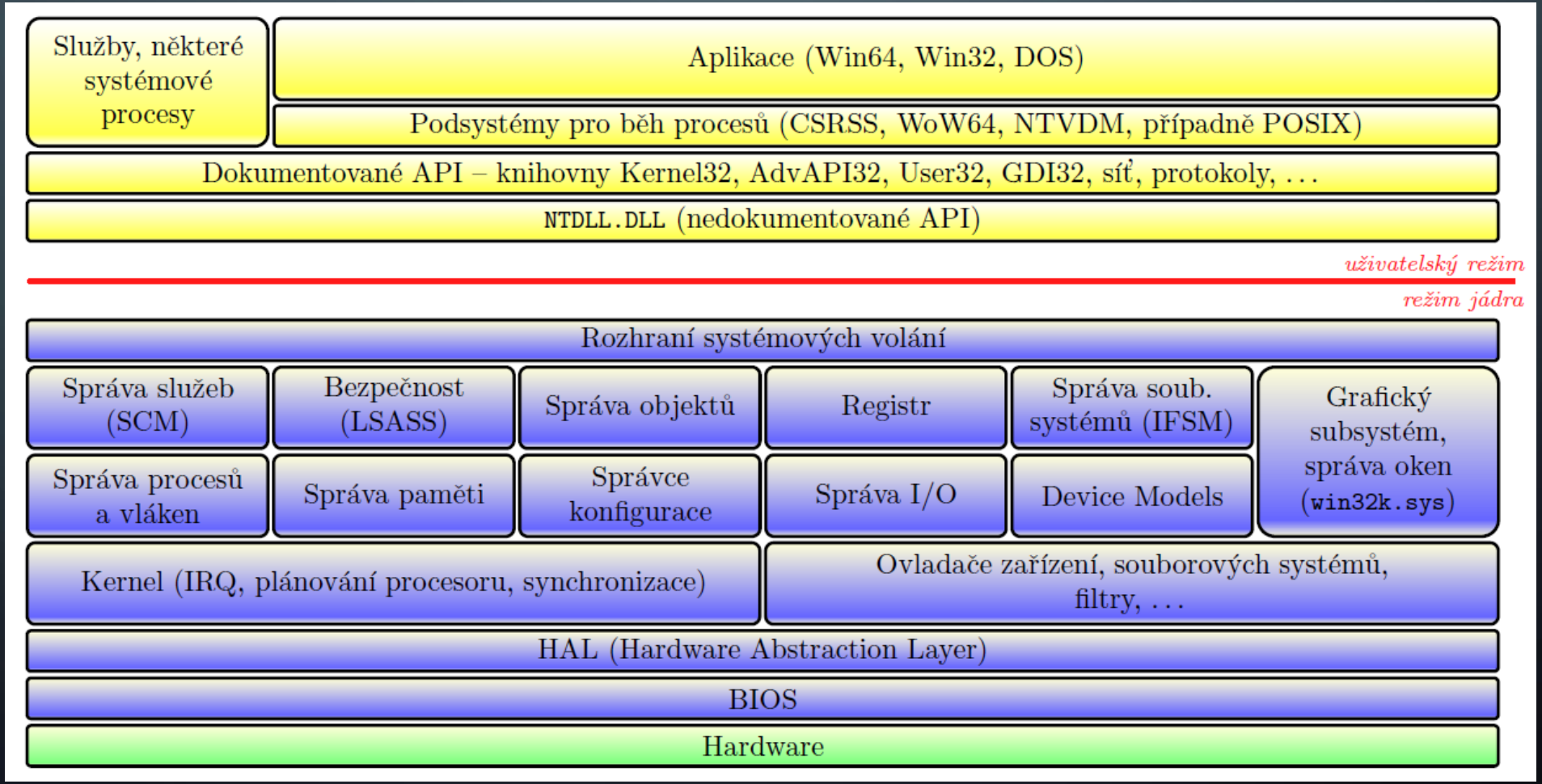
WINDOWS S DOS JÁDREM – BĚH PROCESŮ

- **Win32 aplikace** (psané pro Windows od verze 95 výše) běží všechny ve společném virtuálním stroji, ale každá má svůj vlastní paměťový prostor (pod toutéž číselnou adresou každá z těchto aplikací vidí různá fyzická umístění v paměti),
- **Win16 aplikace** (pro Windows 3.11 a nižší) běží všechny ve společném virtuálním stroji zároveň s Win32 aplikacemi, ale na rozdíl od Win32 aplikací sdílejí jeden společný paměťový prostor (společný pro Win16 aplikace; pod toutéž číselnou adresou vidí všechny Win16 aplikace tentýž objekt v paměti),
- **DOS aplikace** mají každá svůj virtuální stroj, v něm svůj vlastní paměťový prostor.

WINDOWS ŘADY NT DO VERZE XP

- Jádro systému Windows řady NT vznikalo nezávisle na systému MS-DOS, hlavním hlediskem je stabilita a možnosti zabezpečení.
- Inspirace UNIXovými systémy, nejen co se týče vrstvy HAL.
- Systém byl navržen jako víceprocesorový (SMP - symetrický multiprocessing) víceuživatelský multitaskový univerzální síťový systém.

WINDOWS ŘADY NT DO VERZE XP - STRUKTURA



WINDOWS ŘADY NT DO VERZE XP – HAL A KERNEL

Rozdělení do dvou základních částí - části běžící **v privilegovaném režimu** (režimu jádra) a části běžící **v uživatelském režimu**.

HAL je vrstva abstrakce hardware (Hardware Abstraction Layer), rozhraní mezi hardwarem a zbytkem jádra systému. Načítá seze souboru **HAL.DLL**. Je oddělena od ostatních částí systému z důvodu snadnější přenositelnosti systému mezi hardwarovými platformami.

Kernel a **exekutiva** jsou fyzicky uloženy v souboru **NTOSKRNL.EXE** (monolitické jádro). Exekutiva stojí za vším v jádře (modrá oblast) nad HAL kromě kernelu.

Kernel zachytává a obsluhuje přerušení, spravuje procesory (synchronizace přidělování procesorů), apod. Exekutiva je řídicí proces operačního systému, má na starosti řízení celého jádra běžícího v privilegovaném režimu a provoz modulů. Ostatní součásti jádra jsou k jádru linkovány z dynamických knihoven či souborů **.SYS** (moduly, tedy modulární struktura běžícího jádra).

WINDOWS ŘADY NT DO VERZE XP – HAL A KERNEL

Hlavní systémový proces ("System") je ve skutečnosti obrazem toho, co běží v jádře, exportovaným do uživatelského prostoru. Ve skutečnosti nejde o proces, ale o kontejner pro prováděcí vlákna jádra (o vláknech se více dovíme v kapitole o správě procesů).

Ovladače nesouvisejí jen se zařízeními, obecně jde o moduly jádra, které mohou sloužit jak k přístupu k zařízením, sběrnicím apod., ale také to mohou být filtry, přes které procházejí data (šifrování, komprimace, směrování mezi moduly, filtrování/zahazování/třídění, DRM, atd.).

Pro práci s ovladači existuje složitý systém, do kterého se zapojuje rovnou několik na obrázku vyznačených součástí, například **Device Models** (modely ovladačů).

WINDOWS ŘADY NT DO VERZE XP – HAL A KERNEL

Nad ovladači souborových systémů je systém pro jejich správu - **IFSM** - Installable File Systems Manager, který zajišťuje přístup k (předem určeným) souborovým systémům (NTFS, FAT32, UDF apod.). Je využíván modulem pro správu vstupů a výstupů a vyrovnávací paměti.

Správce konfigurace spolupracuje při správě ovladačů, například zajišťuje funkce Plug&Play a Hot-Plug, tedy neustále sleduje stav sběrnic a hlídá připojování nových či již dříve připojovaných zařízení, u nových se pokouší provést instalační a inicializační proceduru.

WINDOWS ŘADY NT DO VERZE XP - GRAFICKÝ SUBSYSTÉM

Moduly pro správu oken a grafiky běží ve Windows řady NT od verze 4 v režimu jádra z důvodu urychlení práce aplikací hodně využívajících grafická zařízení. Tato část jádra se načítá ze souboru **win32k.sys**.

Umístění kódu grafického rozhraní do režimu jádra je neobvyklé. Nevýhodou tohoto postupu je ovšem větší bezpečnostní riziko a riziko porušení stability systému při chybné práci tohoto modulu (pracuje v režimu jádra, proto má přístup do paměti systémových procesů). Další nevýhodou je náročnější postup výměny uživatelského rozhraní za alternativní.

Ve Windows Server od verze 2008 je možné instalovat systém bez GUI (a také bez dalších součástí, které jakkoliv GUI vyžadují) - instalace Server Core.

Grafický subsystém v jádře je modul **GDI**, ve Windows XP i jeho nástavba **GDI+**. Dynamické knihovny **gdi32.dll**, **gdiPlus.dll** a **gdi32Full.dll** jsou pouze přístupovými body k těmto modulům v uživatelském prostoru.

WINDOWS ŘADY NT DO VERZE XP – LSASS A SCM

Bezpečnostní podsystém souvisí především s modulem **LSASS** (Local Security Authority SubSystem). Provádí autentizaci uživatelů, kteří se přihlašují lokálně, a podle databáze v klíči registru SAM určuje přístupová oprávnění.

Správce služeb SCM (Service Control Manager) se načítá ze souboru **services.exe** a zajišťuje běh služeb a komunikaci s nimi. Samotné služby sice běží v uživatelském prostoru, ale obvykle s vyššími oprávněními a bez vazby na konkrétního uživatele, a komunikuje se s nimi především přes modul SCM.

Od Windows NT verze 4 je jádro objektové. V jádře se udržuje databáze objektů a objekty exekutivy jsou exportovány do uživatelského prostoru. Databázi objektů spravuje **Správce objektů**.

WINDOWS ŘADY NT DO VERZE XP – KOMUNIKACE PROCESŮ S JÁDREM

Komunikace procesů s jádrem probíhá tímto způsobem:

- proces spustí určitou funkci či proceduru z dokumentovaného nebo nedokumentovaného **API**
- provede se systémové volání v kontextu jádra,
- v rámci systémového volání je požadavek vyřešen.

Dokumentované rozhraní představují funkce a objekty ze systémových knihoven, jejichž názvy by nám měly být povědomé - **User32.dll**, **GDI32.dll** a další.

Nedokumentované API je soubor **NTDLL.DLL**. Funkce, které se zde nacházejí, již mohou přímo spouštět systémová volání, ale funkce poskytované tímto rozhraním mohou být v každé verzi Windows jiné a mohou vyžadovat jiný způsob volání (spouštění). Proto je lepší používat dokumentované API, které se vždy chová stejně (dokumentovaně). Soubor NTDLL.DLL je rozhraním mezi jádrem a uživatelskám prostorem, obvykle k tomuto rozhraní přistupujeme zprostředkovaně.

WINDOWS ŘADY NT DO VERZE XP - PODSYSTÉMY (SUBSYSTÉMY)

Podsystémy (subsystémy) prostředí jsou rozhraní zajišťující správný a bezpečný běh různých typů procesů. V těchto podsystémech běží aplikace, které ani nemusí být kompatibilní s Windows NT. Podsystémy poskytují aplikacím rozhraní, které překládá komunikaci mezi aplikací a operačním systémem tak, aby si obě strany "rozumněly". Je to především podsystém pro aplikace psané pro 32bitová Windows, MS-DOS a aplikace pro 16bitova Windows Win32, podsystém pro OS/2, POSIX , atd.

Podsystém pro 32b Windows včetně NT (podsystém Win32, v 64bitovém systému se jmenuje prostě Windows) je představován souborem **CSRSS.EXE**, pro **POSIX** je to především soubor **PXSS.EXE** (to je server podsystému). Podsystém Win32/Windows je potřebný také pro běh mnoha systémových procesů, jako jediný spouští hned po startu počítače, ostatní podsystémy jsou spouštěny až na žádost.

Každý podsystém potřebuje kromě svého řídicího programu (například CSRSS.EXE u Win32) také knihovny, obsahují API (Application Programming Interface) daného podsystému. Například ke knihovnám podsystému Win32 patří také knihovny KERNEL32.DLL, USER32.DLL a GDI32.DLL. Součástí podsystému Win32/Windows je mechanismus virtuálních počítačů. Aplikace, která fyzicky zajišťuje běh virtuálních počítačů pro starší aplikace (DOS a Win16), je spouštěna souborem ntvdm.exe (NT Virtual DOS Machine). Při pokusu o spuštění těchto aplikací je nejdřív spuštěna nová instance ntvdm.exe s parametrem - názvem spouštěné DOS či Win16 aplikace s cestou, která již "vnitřně spustí" zadanou aplikaci.

WINDOWS ŘADY NT DO VERZE XP – KOMBINACE ARCHITEKTUR

Windows řady NT nejsou přísně vrstvený systém, ale kombinují více různých architektur pro své různé části. Jsou to tyto architektury:

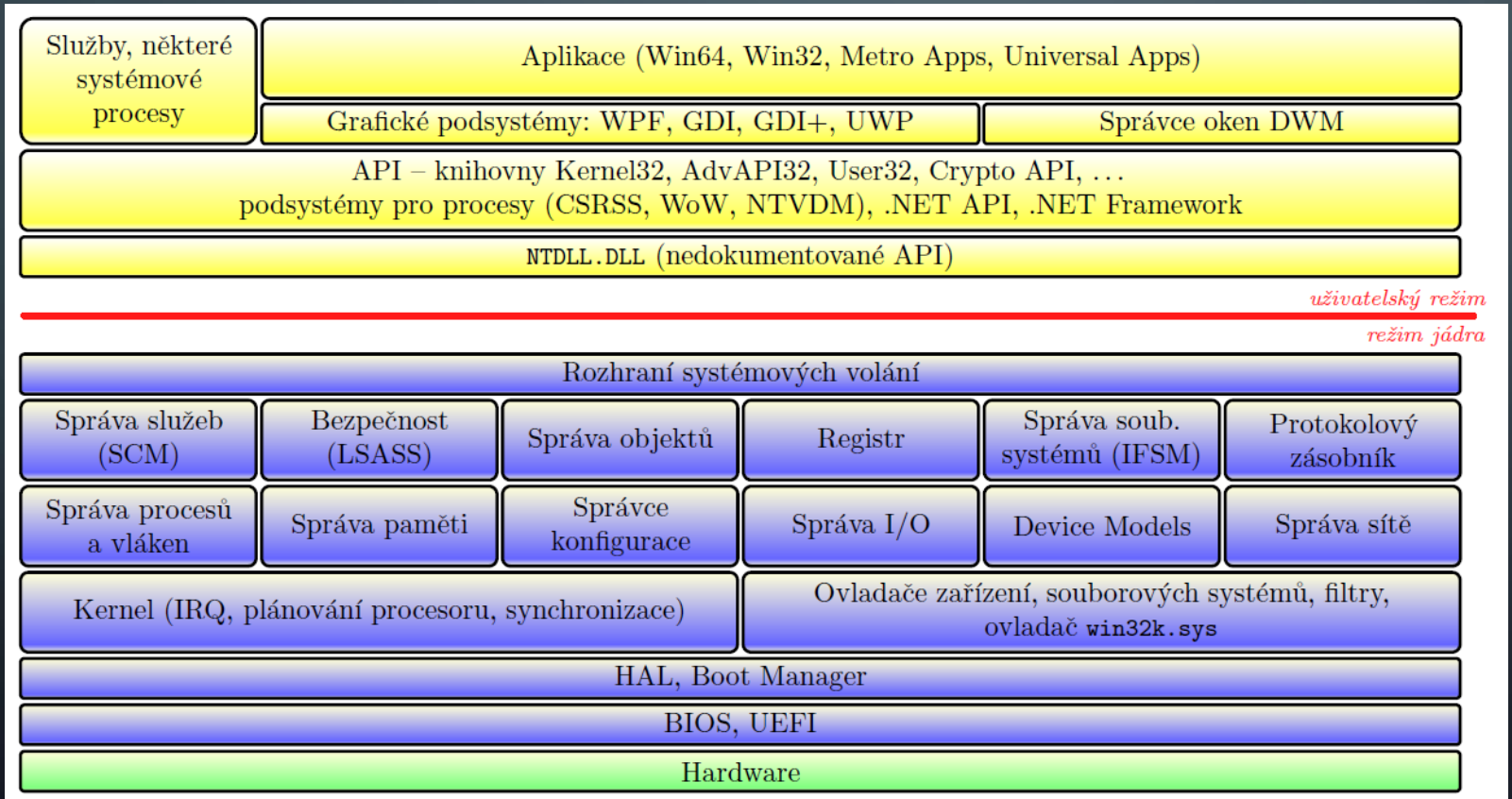
- Jádro je generováno z jediného souboru (**NTOSKRNL.EXE**), z toho pohledu jde o monolitické jádro.
- Vrstvená architektura se uplatňuje především v rozdělení na uživatelský režim a režim jádra.
- Modulární architektura - uzavřené moduly, vnitřně kompaktní, které poskytují služby přes nadefinované rozhraní, komunikace probíhá volně mezi různými moduly, tuto architekturu zde používá exekutiva při řízení správce procesů, správce paměti, I/O systému, ovladačů, atd. (modulů běžících v privilegovaném režimu).
- Architektura klient-server se uplatňuje v API (Application Programming Interface), což je sada dynamicky linkovaných knihoven, zde považovaných za servery, procesy z vyšších vrstev (klienti) využívají jejich služeb (přes knihovnu **NTDLL.DLL**).

WINDOWS ŘADY NT DO VERZE XP – BĚH PROCESŮ

- Win32 aplikace běží všechny ve společném virtuálním stroji, každá má svůj vlastní paměťový prostor (pod toutéž číselnou adresou každá z těchto aplikací vidí různá fyzická umístění v paměti),

- DOS a Win16 aplikace mají každá svůj virtuální stroj, v rámci virtuálního stroje svůj vlastní paměťový prostor.

WINDOWS OD VERZE VISTA A SERVER 2008



Tento obrázek platí hlavně pro **Windows 10**, ale odpovídá i všem předchozím systémům od verze Vista a Server 2008.

WINDOWS VISTA (I.)

- Jádro Windows Vista bylo oproti svým předchůdcům zcela přepracováno.
- Má vnitřní strukturu modulárního typu.
- Celý síťový zásobník (podpora sítě) byl přesunut do režimu jádra a doplněn protokol IPv6
- Část implementace grafického rozhraní byla z jádra přesunuta do uživatelského prostoru
- Přidána podpora UEFI

WINDOWS VISTA (II.)

Důsledky:

- snadnější rozšiřitelnost jádra,
- stejné instalační médium pro všechny varianty Visty (Home Premium, Ultimate, apod.), při instalaci se podle typu licence rozhodne, která varianta bude nainstalována (jsou instalovány jen vybrané moduly),
- nejsou rozlišeny jazykové varianty, existuje samostatný modul pro jazyk. Opravné balíčky mohou být jazykově nezávislé.

WINDOWS VISTA (III.)

Windows Presentation Foundation (**WPF**, také Avalon) je součástí rozhraní .NET Framework. Je to grafický podsystém, tedy především eviduje okna a jiné grafické komponenty vkládané do oken ve stromové struktuře zohledňující jejich vnořování, a zajišťuje správu oken (a dalších grafických komponent). Také plocha je považována za okno, podobně různé panely včetně hlavního panelu plochy.

Desktop Window Manager (**DWM**) je kompozitní správce oken, který provádí vykreslování oken, jejichž strukturu spravuje WPF. Zatímco WPF se stará o data, DWM vykresluje, zajišťuje jakési primitivní 3D zobrazení (Flip3D, průhlednost apod.), náhledy, animace, reaguje při změně rozlišení monitoru, atd.

Od verze Vista je uplatňována funkce **ASLR** (**Address Space Load Randomization**) - knihovny se při načítání do paměti neukládají vždy na stejné místo, ale na náhodně zvolenou adresu.

WINDOWS 7

Většina změn je ve vnitřní struktuře jádra, v řízení a provozu grafického rozhraní, a také ve způsobu využívání a nastavení systému.

Pro jádro byl použit koncept **MinWin** - co nejmenší základní jádro (téměř mikrojádro), ostatní části "širšího jádra" (tj. toho, co běží v privilegovaném režimu) jsou moduly, tedy opět další krok k modulárnosti jádra. Do MinWin patří především kernel (tvrdé jádro). MinWin je samostatnější než původní část jádra, důsledkem je rychlejší start systému a celkově lepší odezva.

Změny v používání API, využívání virtuálních DLL knihoven. Reálně běží výrazně méně služeb než ve Windows Vista a nastavení jsou celkově přizpůsobena novým typům hardwaru. Služby spuštěné při běhu systému mohou být dočasně zastaveny, pokud SCM usoudí, že zrovna nejsou zapotřebí.

Windows 7 přišel se zcela novým řešením problémů s nekompatibilitou aplikací. U vybraných verzí lze použít funkci **XP Mode** pro provoz starších aplikací.

WINDOWS 8, 10

Ve Windows 8 se objevily **Metro Apps**, ve Windows 10 pak **Universal Apps**. Také pro ně bylo třeba vytvořit vlastní grafický subsystém (nesouvisí s .NET, takže žádné WPF) - pro Metro Apps to bylo **WinRT API**, pro jejich nástupce Univesal Apps to je **Universal Windows Platform** (UWP).

Do jádra Windows 10 přibyl **Windows subsystem for Linux**, který umožňuje spouštění aplikací programovaných pro Linux.

Hlavní změny jsou opět v uživatelském prostoru a grafickém rozhraní, včetně vybavenosti různými nástroji.

SERVEROVÉ EDICE WINDOWS

Serverové edice Windows používají totéž jádro jako desktopové edice, jen je jinak nakonfigurováno, v registru mají některé položky jinou hodnotu (zejména položky týkající se sítě) a další nástroje.

Verze jádra	Serverový systém	Desktopový systém
NT 6.0	Windows Server 2008	Windows Vista
NT 6.1	Windows Server 2008 R2	Windows 7
NT 6.2	Windows Server 2012	Windows 8
NT 6.3	Windows Server 2012 R2	Windows 8.1
NT 10.0	Windows Server 2016	Windows 10

V tabulce vidíme označení verze jádra a označení verzí serverových a desktopových Windows používajících příslušné jádro.

SHRNUTÍ

- Operační systémy typu Windows mají složitou strukturu, skládající se z jádra a dalších vrstev, které umožňují stabilní běh systému a správu hardwarových prostředků.
- Existuje několik typů strukturních operačních systémů: monolitická , vrstvená , modulární a model klient-server .
- Systémy jako MS-DOS používají monolitická jádra, zatímco novější verze Windows, počínaje řadou NT, jsou modulární a víceprocesorové.
- Rozdělení na uživatelský režim a režim jádra poskytuje vyšší stabilitu a bezpečnost systému.
- Windows NT a jeho následovníci až do Windows 10 kombinují různé architektury pro optimalizaci výkonu a zabezpečení.

KONTROLNÍ OTÁZKY

- Jakou funkci plní BIOS v systému MS-DOS?
- Který soubor se stará o spuštění Windows v MS-DOS?
- Co je úkolem HAL ve Windows řady NT?
- Co zajišťuje Desktop Window Manager (DWM) ve Windows Vista?