Stručný úvod do systému IBM i

Systém IBM i - bezpečnost a stabilita

Filip Borůvka

Duben, 2008

OBSAH:

1. Úvod

IBM i (dříve AS/400 či iSeries či System i – z marketingových důvodů bylo několikrát přejmenováno) má předchůdce v systému System/38, který IBM uvolnila v roce 1978 a byl vyvinut na základě nových principů (objektová architektura).
Systém prošel za 30 let své existence několikerým přejmenováním a to jak hardwaru, tak i operačního systému. V textu dále je užíváno pro OS označení, jak IBM i, tak i5/OS a je rovnocenné.

Tabulka 1 - Vývoj jmen hardware a operačního systému

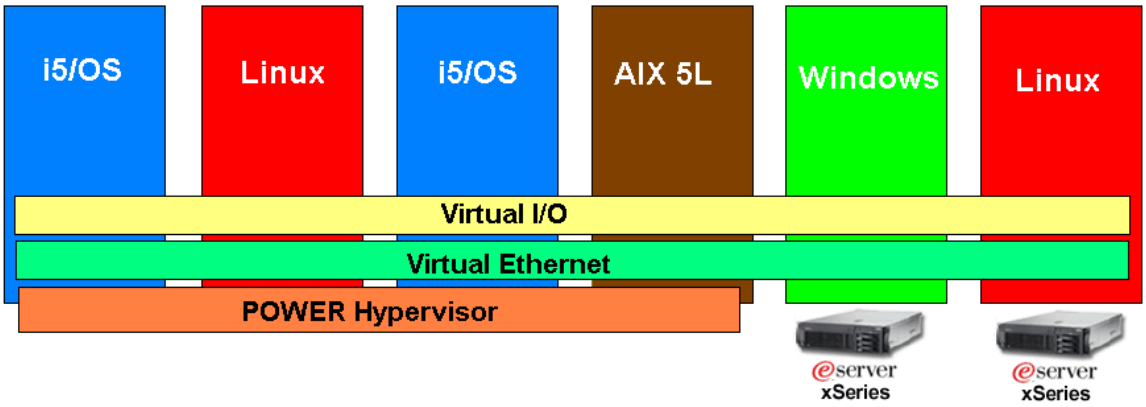
Období		Jméno Hardware	Jméno OS
říjen	1978	System/38	CPF
21. červen	1988	AS/400 (CISC)	OS/400
červen	1995	AS/400 (RISC)	OS/400
říjen	2000	eServer iSeries	OS/400
2. květen	2004	eServer i5	i5/OS
31. leden	2006	System i	i5/OS
duben	2008	Power Systems	IBM i

Zdroj: http://systeminetwork.com/article/they-say-it%E2%80%99s-your-birthday

IBM i je robusní, objektově orientovaný systém s integrovanou relační databází, založený na technologii PowerPC.
Systémy IBM i mohou provozovat prakticky libovolnou aplikaci, neboť se dokáží rychle a snadno přizpůsobit aplikacím, které by mohly být v budoucnosti implementované. Primární operační systém - IBM i (i5/OS) nabízí díky své šíři a rozsáhlé funkčnosti největší přizpůsobení a provozní efektivitu. Toho dosahuje prostřednictvím nativní souběžné podpory aplikací zabudovaných do RPG, COBOL, C, C++, Java, WebSphere a Domino.

Zásadní výhodou systému, je virtualizace s možností vytvoření velkého počtu tzv. LPARů logických partition (10 LPARů na 1 procesor), které jsou z hlediska OS zcela nezávislé. Na jednom fyzickém HW je možno provozovat OS IBM i, Unix, Linux a při vložení speciálního HW i OS Windows. Mezi jednotlivými LPARy je možno dynamicky (za provozu) přesouvat CPU (po 0,1 dílu CPU), operační paměť, jednotlivé karty např. řadiče páskových zařízení, síťové karty. Mezi jednotlivými LPARy je možné komunikovat přes virtuální ethernet, takže komunikace se nedostává do běžné sítě a tím pádem ji nezatěžuje.

Obrázek 1 - Integrace různých OS pomocí LPAR



Zdroj: Vlastní

Systém IBM i je firmou IBM doporučován jako integrační platforma, i5/OS má v sobě implementován PASE, které umožňuje portaci libovolné Unixové nebo Linuxové aplikace. Nejnověji je v IBM i integrován OpenSSL, PHP, MYSQL a IBM uvažuje i o dalších aplikacích.[1]

2. Základní principy

Systém IBM i je založen na tzv. vrstvené architektuře – je navržen tak, aby jednotlivé vrstvy byly zaměnitelné bez zásahu do vrstev ostatních tzn. upgrade HW bez zásahu do vrstvy OS a aplikační vrstvy, upgrade OS bez zásahu do aplikační vrstvy. Tyto podmínky jsou víceméně dodržovány, ovšem v případě zásadních změn, mohou být stanoveny určité prerekvizity (např. nutnost nasazení nové verze OS, bude-li použit procesor nové generace).
Systém IBM i je založen na objektové architektuře, tzn. to co se do systému ukládá nebo se z něj načítá, je objekt (programy, databázové soubory, fronty zpráv, komunikační zařízení a uživatelské účty). Objekt se skládá ze záhlaví (společný tvar pro všechny typy objektů) a funkční části (pro každý typ objektu je jiné).

2.1. Paměť

Veškerá paměť systému operační i disková je adresována jednotně (jedné se o tzv. virtuální paměť), je to jedna souvislá vrstva, takže se uživatel nemusí zabývat o to, kde se jednotlivé objekty nachází – jen se na ně odvolává jménem. Díky použití virtuální paměti, lze bez modifikace aplikačních a systémových programů využívat nových technologií pamětí a procesorů. [2]

[1] ***System i – operační systém***, *http://www-03.ibm.com/systems/cz/i/software/os/*
[2] ***ŽUPKA, Vladimír; kolektiv IBM***. *Základy AS/400. 1. vyd. Praha*

2.2. Licenční programy

Vlastní OS se skládá z jednotlivých modulů – licenčních programů, které je možné instalovat, vyjímat a fixovat samostatně, základní licenční programy jsou v uvedeny tabulce:

Tabulka 2 - Základní označení licenčních programů systému IBM i

Kód	Popis	Použití
5761999	Licence Internal Code	Rozhraní mezi HW a OS
5761SS1	i5/OS	Vlastní operační systém – včetně dalších licenčních podprogramů tzv. options
5761TC1	IBM TCP/IP Connectivity Utilities for i5/OS	Implementace TCP/IP protokolu – Telnet, FTP a další služby
5761DG1	IBM HTTP server for i5/OS	Webový server
5761JV1	IBM Developer Kit for Java	Java Virtual Machine

Zdroj: Vlastní

2.3. Prostředí systému

Systém IBM i má dvě prostředí pro ukládání objektů nebo souborů a to:

- **Objektové prostředí** (Obrázek 2) – objekty jsou uloženy v tzv. knihovnách.

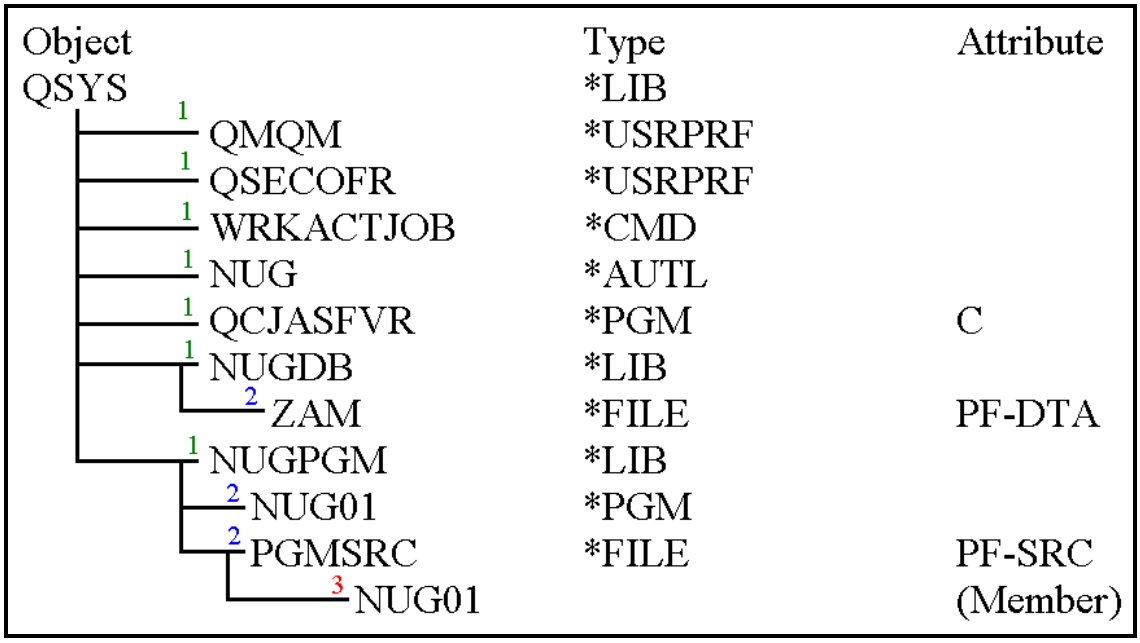
  V tomto prostředí jsou uloženy objekty různých typů (Databázový soubor je objekt typu *FILE, program typu *PGM, příkaz typu *CMD, uživatelský profil tyou *USRPRF.) Každý objekt musí být přiřazen do nadřazené složky, která se nazývá knihovna (library).

  Knihovna je též objekt a to typu *LIB – všechny knihovny a systémové objekty jsou v hlavní systémové knihovně, která se jmenuje QSYS (všechny systémové objekty začínají písmenem Q* a není radno je měnit).

  Systémové objekty mohou být pouze v knihovně QSYS a jedná se o objekty typu Library *LIB, User Profile *USRPRF, Device Description *DEVD, Line Description *LIND, Controller Description *CTLD, Authorization Lists *AUTL. Obrázek 2 podrobně ukazuje objektovou strukturu systému IBM i

  (1 – úroveň knihovna, 2 – úroveň objekt, 3 – úroveň člen (member))

Obrázek 2 – Struktura objektového prostředí

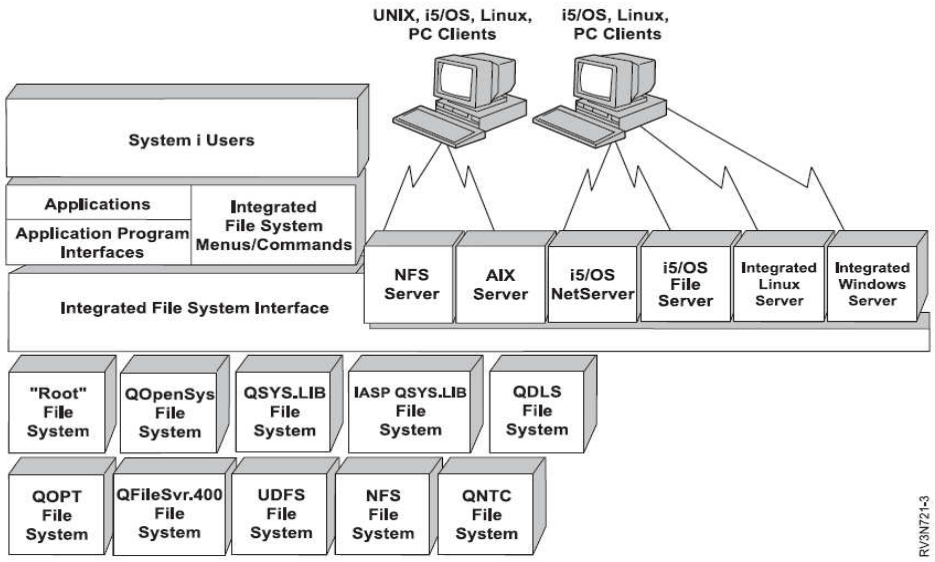


Zdroj: Vlastní

- **Souborové (integrované) prostředí** (IFS) – jsou v něm uloženy soubory kompatibilní se soubory typu UNIX/Linux, Windows, Netware, případně lze vytvořit vlastní souborový systém (filesystem).

  Souborové prostředí je z hlediska funkčnosti stejné jako pro systém Windows, tj. obsahuje adresáře a soubory, jen oprávnění je řešeno podrobněji.

Obrázek 3 – Souborový systém (IFS)



Zdroj: http://publib.boulder.ibm.com/infocenter/systems/scope/i5os/index.jsp?topic=/ifs/rzaaxfsknow.htm

3. Obsluha systému – uživatelské rozhraní

Operační systém IBM i (i5/OS) má perfektním způsobem vymyšlenou a propracovanou obsluhu a práci v režimu příkazové řádky, na základě emulace 5250[3]. Pro správu OS, je též možné použít grafickou nadstavbu - Navigator for i[4].

Práce v systému probíhá pomocí příkazů řídícího jazyka (CL), příkazy jsou koncipovány na základě zkratek pro činnost a objekt činnosti:

Nejdůležitější činnosti:	**Význam:**
ADD, RMV	Add – přidat, Remove – vyjmout
CHG	Change – změnit
DSP	Display – zobrazit
GO	Go – jít (na nabídku v menu)
PRT	Print – tisknout
RST, SAV	Restore – obnovit, Save – uložit
SBM	Submit – předat k dávkovému zpracování
WRK	Work with – pracovat s (objekty, činnostmi, stavy)

Činnost+Objekt činnosti:	**Význam:**
WRKACTJOB	Work with Active Jobs
WRKCMD	Work with Commands
WRKCTLD	Work with Ctl Descriptions
WRKHDWRSC	Work with Hardware Resources
WRKJOB	Work with Job
WRKJOBQ	Work with Job Queue
WRKJRN	Work with Journal
WRKLIB	Work with Libraries

Obdobně lze místo WRK použít i další zkratky pro činnosti.
Pro každý příkaz lze pomocí klávesové zkratky **F4** získat prompt příkazu a použitím **F1** dostaneme nápovědu. Při stisku F1 mimo volby dostaneme nápovědu celkovou, při stisku nad konkrétní volbou dostaneme nápovědu ke konkrétní položce. Pomocí klávesy F9 lze vyvolat dříve zadané příkazy. [5]

4. Zabezpečení

Zabezpečení systému i bylo v systému navrženo už v jeho počátcích, je vždy přítomné a nelze jej obejít – je vždy aktivní, dá se jen řídit jeho úroveň.

[3] http://www-03.ibm.com/systems/i/software/access/
[4] http://www-03.ibm.com/systems/i/software/navigator/
[5] ***ŽUPKA, Vladimír; kolektiv IBM***. *Základy AS/400. 1. vyd. Praha*

Zabezpečení systému se skládá z několika úrovní – Systémové hodnoty (systémový audit, bezpečnostní pravidla); uživatelské a skupinové profily, autorizační listy; Exit pointy (při použití určité funkčnosti je zavolán nadefinovaný program, který provede příslušnou kontrolu)

4.1. Systémové hodnoty

Security system values lze vyvolat příkazem „WRKSYSVAL SYSVAL(*SEC)“, kde zásadní hodnoty jsou:

QSECURITY - System security level
10=Physical security only (no longer supported)
20=Password security only
30=Password and object security
40=Password, object, and operating system integrity
50=Password, object, and enhanced operating system integrity

Běžně se používá hodnota 40, která je plně postačující.

QAUDCTL - Auditing control
Startuje auditní logování

QAUDLVL - Security auditing level
Systémová hodnota říká, které auditní události se budou zapisovat do auditní logů, tzv. žurnálů

Důležité jsou též hodnoty stanovující pravidla pro přihlašování uživatelů:
Maximální počet neplatných pokusů při jejichž překročení je uživatelský profil zablokován QMAXSIGN (3-5), doba expirace hesla QPWDEXPITV (30 dnů), minimální a maximální počet znaků v hesle QPWDMINLEN (8) a QPWDMAXLEN (128), po kolika změnách lze použít stejné heslo QPWDRQDDIF (10-12)

4.2. Uživatelské profily, skupinové profily a autorizační listy

Každý uživatel přistupující do systému musí mít přiřazen jednoznačný profil, v případě aplikací a pro speciální použití se vytvářejí tzv. technické profily
V systémech existují profily, které mají shodné parametry, tj. mají stejné role, tím pádem stejná přístupová oprávnění (např. standardní uživatelský profil – uživatel aplikace, systémové profily v jejich kontextu běží OS, speciální profily – administrátoři, operátoři, bezpečnostní administrátoři, technické účty – aktivní – jsou používaná pro přístup aplikacemi, např. ODBC, FTP a technické účty – pasivní – nejsou běžně použitelné (nemají heslo) a v jejich kontextu pracují běží různé nesystémové aplikace – dávkové úlohy). Každý objekt v systému má nastaveno určité oprávnění a vlastnictví.

Obrázek 4 - Příklad zobrazení nastavení oprávnění v systému

```
Object . . . . . :   QBATCH          Owner  . . . . . :   QPGMR
  Library  . . . . :     QSYS        Primary group  . . :   *NONE
Object type  . . . :   *SBSD         ASP device . . . . :   *SYSBAS

Type changes to current authorities, press Enter.

  Object secured by authorization list  . . . . . .   AUSERS

                        Object
User        Group      Authority
*PUBLIC                 *USE
QPGMR                   *ALL
OPRGRP                  *ALL
```

Zdroj: Vlastní

Oprávnění jednotlivých profilů se používá jen výjimečně, běžně se využívají skupinové profily – do profilu uživatele se nastaví skupinový profil a uživatel pak má přístup na objekty, kde je skupinový profil uveden.
Autorizační listy fungují obdobně jako skupinové profily, ale na jeden objekt může být jen jeden autorizační list, v němž je seznam profilů/skupinových profilů a příslušné oprávnění.

Oprávnění k objektům je následující:
*ALL - je povoleno vše
*CHANGE – nelze objekt vymazat a provádět určité změny
*USE – nelze provádět žádné změny
*EXCLUDE – vše je zakázáno
USER DEF – lze nadefinovat různé objektové a datové přístupy.

4.3. Exit pointy

Exit pointy jsou určité bodu v programu, které jsou vyvolány při vzniku určité události, používá se to zejména pro ověřování přístupu do TCP/IP serverů.
Např. Uživatel se pomocí FTP připojí k systému, zadá svůj uživatelský profil a heslo, po potvrzení uživatele je v FTP vyvolán program, který se podívá o databáze uživatelů mající povolený přístup na FTP server.

5. Databáze

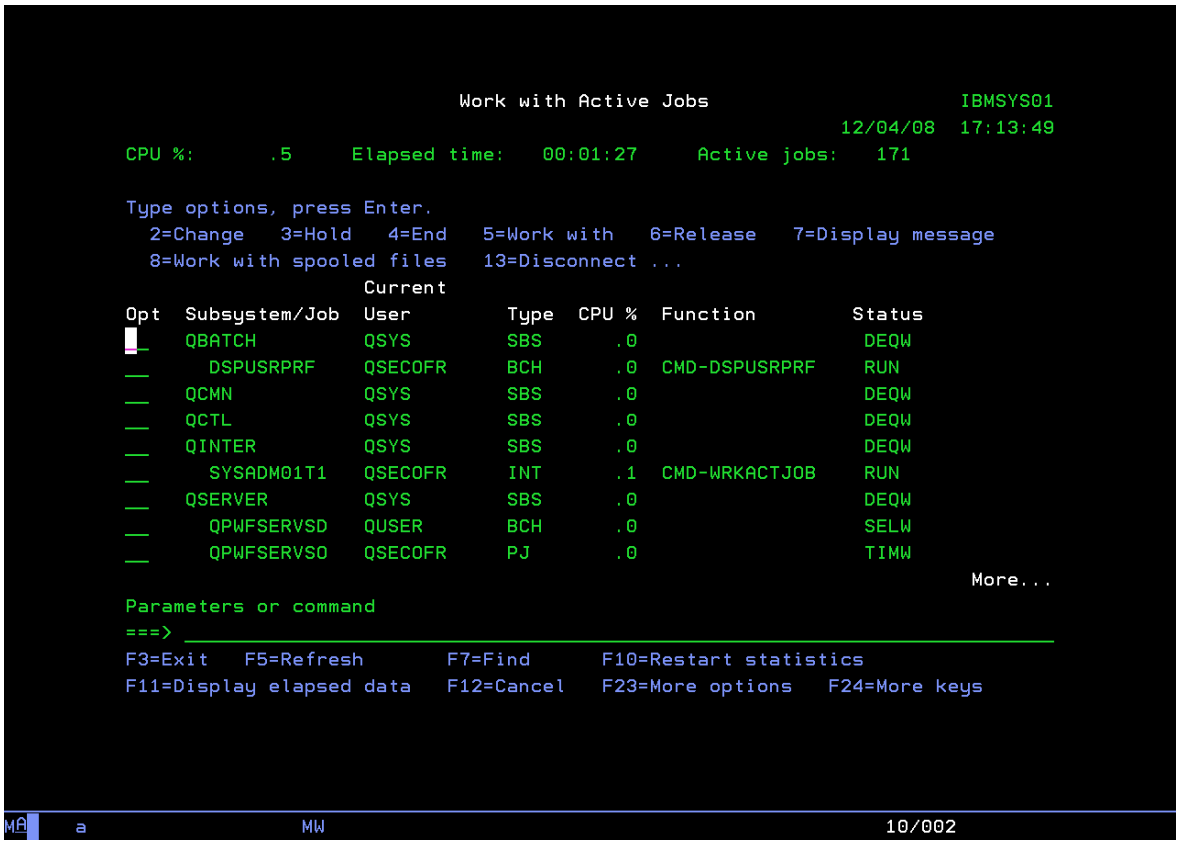
Databáze v Systému IBM i je integrovaná DB2 for i5/OS, je dodávána společně se systémem. DB2 for i5/OS také poskytuje mnoho dalších funkcí a vlastností, např. triggers, uložené procedury a další.
Jako interface do DB2 for i5/OS slouží licenční produkt IBM DB2 Query Manager and SQL Development Kit for i5/OS, který pomáhá zadávat SQL dotazy formou průvodce.
Databáze je tvořena sadou tabulek (objekt typu *FILE, atribut PF-DTA) a logických souborů (*FILE, LF). Veškeré změny v databázi jsou současně se změnou dat v tabulce z důvodu případného návratu k určitému bodu logovány, jedná se o žurnálování. Žurnálování umožňuje nejen vrácení databáze do určitého stavu, ale též dohledat veškeré změny, které byly provedeny a dohledat kdo je, kdy a odkud provedl. Pro práci s databází se používá SQL nebo častěji RPG programy, které jsou nativním programovacím jazykem i5/OS a jsou výrazně výkonnější než SQL. V systému i5/OS je možné též provozovat programovací jazyky C, C++, Cobol, Java. Zdrojové kódy se ukládají do objektů typu *FILE s atributem PF-SRC, v jednom souboru může být více zdrojových položek – memberů. Objekt typu *FILE, PF-DTA mohou

mít také více členů (memberů), ale to se využívá v podstatě pouze pro logy - třeba za každý den jeden, kvůli lepší práci s nimi.

6. Řízení práce (Work Management)

V systému běží úlohy, které jsou pod konkrétními subsystémy, při přihlášení uživatele do systému se vytvoří úloha, které se přidělí do interaktivního subsystému (QINTER). Pokud se spustí dávkové zpracování, je příslušná úloha přidělena do dávkového subsystému (QBATCH)
V úloze je možné řídit různé parametry, priority, logování, tiskové výstupy a řadu dalších (celkem se jedná o 40 parametrů).
Přidělování úloh do subsystémů se provádí na základě nastavení různých parametrů. V subsystému lze nastavovat specifické parametry a to zejména pevné alokování paměti (WRKSHRPOOL) a priority subsystému. Všechny aktivní subsystémy a úlohy lze zobrazit příkazem WRKACTJOB viz obrázek.

Obrázek 5 - Výstup příkazu WRKACTJOB



Zdroj: Vlastní

7. Komunikace

Systém IBM i podporuje komunikační protokoly SNA a TCP/IP.
Před vlastní konfigurací protokolů je potřeba nastavit komunikační linky, na kterých se nastavuje, která fyzická síťová karta bude použita, MAC adresa, rychlost, duplex a popis linky.

7.1. Protokol SNA

Protokol SNA byl vyvinut firmou IBM a sloužil pro komunikaci mezi serverovými systémy a posléze i pro komunikaci Klient-Server. Jedná se o protokol robusní, avšak poměrně složitý při nastavování na rozdíl od protokolu TCP/IP.

V současnosti se od protokolu SNA ustupuje, protože při jeho nativním používání se musí používat síťové prvky, které SNA pakují do TCP/IP a na druhé straně SNA zase rozbalí.
Pro zajištění kompatibility implementovala firma IBM do systému službu AnyNet (SNA over TCP/IP), v této službě je prováděno pakování SNA do TCP/IP protokolu přímo v systému, takže odpadá používání speciálních síťových prvků, navíc nové síťové karty pro midrange a mainframe systémy už protokol SNA nepodporují.

Od verze V5R4 implementovala firma IBM službu Enterprise Extender (EE), která nahrazuje AnyNet, EE je snadnější na konfiguraci a výkonnější (používá UDP porty 12000 – 12004)

7.2. Protokol TCP/IP

Protokol TCP/IP je v systému implementován jako licenční program, některé části jsou licenční podprogramy operačního systému 5722SS1 (Option 12 - Host Servers, option 31 - Domain Name System a kryptografický modul – option 34 - Digital Certificate Manager)
Systém podporuje TCP/IP verze 4 a verze 6.
Hlavní menu TCP/IP se zavolá pomocí příkazu CFGTCP, v tomto menu lze nastavit všechny potřebné parametry (Konfigurace TCP/IP interface, default gateway, Domain information (Host name, Domain name, Domain search list, Host name search priority a DNS servery) globální parametry TCP/IP a parametry jednotlivých služeb (FTP, Telnet, SMTP, NTP, SNMP, DRDA, DDM, RouteD – RIP2, OSPF a další proprietární služby IBM)
V systému je implementována služba NetServer, která emuluje službu sdílení souborů ve Windows (SMB protokol)
Pomocí aplikace DCM – Digital Certificate Manager je možné vytvořit certifikační autoritu (CA), serverové certifikáty a ty přidělovat jednotlivým službám pro možnost komunikace pomocí SSL. V případě potřeby je možné použít i VPN službu. Pro zajištění kontinuity komunikace pří výpadku síťové karty je možné použít virtuální IP adresy, které jsou vázané na konkrétní adresy fyzických rozhraní.

8. Závěr

Systém IBM i je vysoce stabilní, avšak hodně problémů na velkých výpočetních systémech bývá zapříčiněno nedostatkem financí na jejich včasný upgrade a pak nastávají výkonnostní problémy, nepříjemný je pád systému díky vyčerpání diskové kapacity, při výskytu skokového zaplnění diskového prostoru.

Součástí tohoto dokumentu je i prezentace týkající se přehledu IBM i a nutných podmínek pro bezproblémový provoz velkých výpočetních systémů.

9. Zajímavé odkazy

1. Hlavní stránka IBM věnující se systému i (základní popis a obchodní informace)
   http://www-03.ibm.com/systems/i/

2. Stránka pro podporu systému i (Obsahuje informace pro správce systému – knowledge base, informace o fixování systému a další důležité informace)
   https://www-304.ibm.com/systems/support/supportsite.wss/brandmain?brandind=5000027

3. Informační centrum (Kompletní dokumentace k systému)
   https://publib.boulder.ibm.com/iseries/

4. IBM redbooks (Obsahuje detailní informace ke konkrétním tématům, napsané lidmi z praxe, kteří redbook píší v laboratořích IBM formou stáže)
   http://www.redbooks.ibm.com/

10. Seznam použité literatury

1. ŽUPKA, Vladimír; kolektiv IBM. Základy AS/400. 1. vyd. Praha : IBM, 1995.

2. SOLTIS G., Frank. Systém AS/400 zevnitř 1. vyd. Praha : Computer Press, 1997. ISBN 80-7226-012-X

3. Kolektiv IBM. Jak začít pracovat s AS/400 2. vyd. Praha : IBM, 1998.

4. IBM System i : System i – operační systém
Dostupný z WWW:
http://www-03.ibm.com/systems/cz/i/software/os/

5. IBM i5/OS V5R3 a V5R4. Systémová nápověda a systémová menu