Jaroslav Horák
Milan Keršláger

Počítačové sítě pro začínající správce

3. aktualizované vydání

chybí slovník (je o něm zmínka v textu)

str. 46 špatný obrázek
obr. na str. 40 – ***Obrázek 1.40:*** *Provedení WiFi karet* – neni uplny

Opravit záhlaví - na sudých stranách nebude název knihy, ale podkapitola

Computer Press, a.s.
Brno
2006

Počítačové sítě pro začínající správce
3. aktualizované vydání

Jaroslav Horák, Milan Keršláger

Vydalo nakladatelství Computer Press, a.s. jako svou 2172. publikaci.

Vydavatelství a nakladatelství Computer Press, a.s.,
nám. 28. dubna 48, 635 00 Brno, knihy.cpress.cz

ISBN 80-251-0892-9

Prodejní kód: K1210

Odborná korektura: Michal Opatřil
Jazyková korektura: Veronika Macková, Josef Novák
Vnitřní úprava: Jaroslav Novák
Sazba: Pavel Kynický
Rejstřík: Iva Vilímská
Obálka: Jaroslav Novák

Komentář na zadní straně obálky: Ivo Magera
Technická spolupráce: Jiří Matoušek, Petr Klíma, René Kašík
Odpovědný redaktor: Jindřich Jonák
Technický redaktor: Jiří Matoušek
Produkce: Petr Baláš

Computer Press, a.s., nám. 28. dubna 48, 635 00 Brno
tel.: 546 122 111, fax: 546 122 112
Objednávejte na: **knihy.cpress.cz**
distribuce@cpress.cz

Bezplatná telefonní linka: **800 555 513**

Dotazy k vydavatelské činnosti směřujte na: **knihy@cpress.cz**

Máte-li zájem o pravidelné zasílání informací o knižních novinkách do Vaší e-mailové schránky, zašlete nám zprávu, obsahující váš souhlas se zasíláním knižních novinek, na adresu **novinky@cpress.cz.**

Obsah

Úvod

Proč počítačovou síť?

Osobní počítače se dnes již zabydlely nejen v podnicích, ale i v domácnostech. O jejich výhodách určitě nikdo nepochybuje. Pokud se však „sejde“ více počítačů pohromadě, nastávají starosti:

- Jak zajistit, aby určitá data byla stále aktuální? Kupříkladu je na několika počítačích nainstalován účetnický program a my potřebujeme, aby se každá změna okamžitě objevila na všech počítačích (nová faktura, úbytek ve skladu, platba pokladnou …).
- Jak přenést data z jednoho počítače na druhý? Chcete zkopírovat soubor, který se však nevejde na disketu (a to je dnes běžné).
- Chcete něco vytisknout, ale tiskárna je připojená k jinému počítači.

Řešení těchto problémů nabízí vzájemné propojení počítačů – vytvoření počítačové sítě. Dnes je tato technologie hojně používaná, její zřízení nepředstavuje u menších sítí žádné velké náklady.

Výhody sítí

V předešlém odstavci jsme si nastínili některé důvody proč se sítě používají, nyní je shrnu. Síť nám tedy umožňuje:

Sdílet data: soubor, v němž máme důležitá data, je společný pro všechny uživatele sítě.

Snadno přenášet data: překopírovat data z jednoho PC do druhého není žádný problém, nepotřebujeme diskety, nejsme omezeni jejich kapacitou.

Sdílet hardwarové prostředky: už jsme si říkali, že pro všechny počítače v síti nám stačí jedna tiskárna. Obecně však můžeme využívat pro společnou práci i jiné hardwarové prvky: modemy, skenery, disky pro ukládání dat apod.

Komunikace v síti: je další velkou výhodou sítí. Mezi jednotlivými počítači mohou putovat zprávy, či dopisy. Dnes se hojně využívá propojování celých sítí k Internetu, všichni pak mají k dispozici služby Internetu (e-mail, prohlížeč…).

Ochrana dat: o ní jsem se ještě nezmiňoval. Spočívá v možnosti soustředit všechna důležitá data na jedno místo v síti (typicky na speciální počítač – server). Zde uložená data je pak možné zpřístupnit jen některým uživatelům a jiným je skrýt. Snazší a levnější je také pravidelné zálohování dat nahromaděných na discích serveru.

Druhy sítí

Kritérií, podle nichž můžeme sítě dělit, je více. Mezi hlavní patří klasifikace sítí podle rozlehlosti.

Sítě LAN (Local area networks): ty jsou omezeny na jedno lokální místo – jeden podnik, místnost, budovu. Zajišťují sdílení lokálních prostředků (tiskáren, dat, aplikací). Hlavně jim je věnována tato kniha.

Sítě WAN (Wide area networks): rozlehlé sítě. Ty se skládají z více vzájemně propojených sítí LAN. Jejich spojování se provádí speciálními linkami či bezdrátově. Rozlehlost sítí může být různá, od sítí městských či firemních (firma s pobočkami ve více městech, zemích či kontinentech), až po nejznámější celosvětovou síť – Internet. Jim se však v této knize věnovat nebudu.

Můžeme se setkat i s termínem **síť MAN** (Metropolitan area network). Metropolitní (městská) síť je menší než síť WAN, ale větší než síť LAN.

Pro praktickou činnost není dělení sítí podle velikosti tak důležité, navíc může být obtížné rozhodnout kde končí síť LAN a začíná MAN, či kde síť MAN přechází do sítě WAN. Proto jsem zařadil tabulku, shrnující charakteristické vlastnosti sítí.

Tabulka 1.1: Sítě podle velikosti

síť	charakteristika
LAN	místní (lokální), pro přenos dat se používají kabely
MAN	rozsah jednoho (amerického) města, udává se velikost do 75 km, kromě kabelových linek bývají jednotlivé sítě spojeny bezdrátově.
WAN	propojují sítě vzdálené desítky km. Pro propojení podsítí používají nejčastěji telekomunikační linky.

Základní prvky sítě

Co to tedy je počítačová síť? Odpověď nám dává obrázek, jde o souhrn hardwarových a softwarových prvků, které zprostředkují vzájemnou spolupráci počítačů.

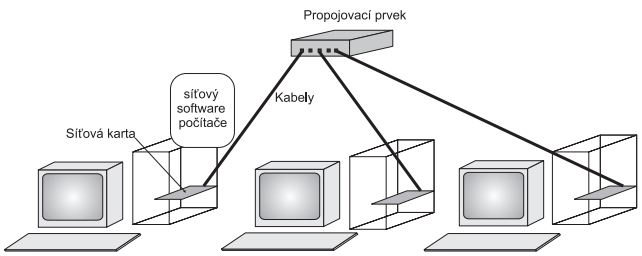
Vybavení počítače

Samotný počítač musí být vybaven programem, který podporuje vzájemnou spolupráci. To naštěstí není žádný problém, protože síťová podpora je obsažena ve všech dnes používaných verzích operačních systémů Windows (Windows 98, ME, NT, 2000, XP).

Hardwarovým prvkem, jenž musíme do PC doplnit, je síťová karta. Ta spojí počítač s kabeláží, a umožní jeho fyzické připojení k síti.

Prvky sítě mimo PC

Jak vidíme z obrázku, je dalším síťovým elementem kabeláž spojující jednotlivé počítače. Její součástí bývají také aktivní prvky propojující síťové prvky, zesilují či filtrují přenášená data apod.



Obrázek 1.1: *Prvky počítačové sítě*

Klasické dělení součástí sítí

Obvykle se síťové prvky člení na:

- **síťové počítače** (běžná PC pracující v síti)
- **síťový hardware** (síťové karty v počítačích, kabely, aktivní prvky v kabeláži)
- **síťový software** (programy na síťových stanicích, případně serverech)
- Při plánování a výstavbě počítačové sítě nesmíme zapomínat ani na správně vyškolenou obsluhu – správce sítě a organizační schémata nutná pro síťový provoz. Nezbytné je také zaškolení obsluhy síťových stanic.

Kapitola 1

Hardwarové prvky sítí

V této kapitole si popíšeme základní komponenty nutné pro činnost sítě. Výsledkem kombinace těchto prvků bývají sítě různých topologií, standardů a vlastností.

Popis začneme přenosovými médii, jimiž se šíří signál. K dispozici jsou tři základní typy médií:

- **metalické kabely** – „klasická" přenosová média založená na měděném vodiči, kterým se přenáší elektrické signály
- **optické kabely** – jimiž se přenášejí světelné impulzy, v nichž jsou zakódována data
- **vzduch** – kterým se šíří elektromagnetické vlnění, médium pro přenos dat bezdrátovými sítěmi.

Kabely

U dnešních síti se používají především kroucené dvojlinky, jimž je věnován nejpodrobnější popis. Časté jsou také optické kabely, dříve hodně používané koaxiální kabely téměř nenajdeme (a také se jim v knize věnovat nebudeme).

Při výkladu se setkáme s několika pojmy, jež budou vysvětleny v následujících kapitolách (topologie, Ethernet), případně jejich význam najdete ve slovníku na konci knihy. Jednou z důležitých vlastností síťových kabelů je rychlost s jakou mohou přenášet data. Ta se vyjadřuje v Mb/s (megabity za sekundu, anglicky megabyte per second – Mbps), nejčastěji se u sítí LAN setkáme s rychlostí 100 Mb/s, rychle se rozšiřují síťové prvky pro rychlost 1000 Mb/s neboli Gb/s (Gigabity za sekundu). Dřívější rychlost 10 Mb/s je již minulostí.

Kroucená dvojlinka (twisted pair cable)

Je odvozena od telefonního kabelu a dnes je nejrozšířenějším metalickým vodičem v sítích LAN. Kabel kroucené dvojlinky se skládá z 8 vodičů, tvořících 4 páry.

Elektrický signál, který je vodiči přenášen, je náchylný na rušení, které vzniká vzájemným působením vodičů. U kroucené dvojlinky spočívá ochrana proti vzájemnému rušení v „kroucení". Oba vodiče tvořící jeden pár jsou navzájem zkrouceny, pravidelně střídají svoji vzájemnou polohu. Také páry jsou navzájem překrouceny. Tím se mini-malizuje ovlivňování jednoho vodiče druhým a vzájemné vlivy vodičových párů.

V praxi se nejčastěji setkáváme s kabely kategorie 5 nebo 5e. Oba typy kabelů mají čtyři páry vodičů a stejné konektory RJ 4. Kabel kategorie 5 se používá pro rychlost do 100 Mb/s, kategorie 5e je určena pro přenosy Gb/s. Do praxe jsou uváděny také nové kabelové standardy, kabely kategorie 6 a 7, určené pro nejrychlejší Gb a 10Gb přenosy. Jednotlivé kategorie se liší vnitřní konstrukcí, která dovoluje zvyšovat šířku přenosového pásma. (Přenosové pásmo je parametr udávající jak velký rozsah signálů je kabel schopný přenést. Čím je přenosové pásmo širší, tím lépe). Pokud chceme skutečně dosáhnout normovaných rychlostí, musíme kabely připojit ke kabelovým a aktivním prvkům (zásuvky, switche...) odpovídajících kategorií.

Pro kroucenou dvojlinku je typická hvězdicová topologie (viz dále).

> ***Poznámka:*** *V češtině se pro kabel twisted pair vžil název dvojlinka, přestože ve skutečnosti je v jednom kabelu dvojlinek více. Přesný název by asi mohl být „kabel ze zkroucených párů".*

Následující tabulka ukazuje základní parametry nejpoužívanějších kabelů. Kategorie 6 a 7 jsou relativně nové a jejich definice se ještě upřesňují. Proto jsou jejich údaje spíše informativní, dále se budeme věnovat kabelům kategorií 5.

Tabulka 1.2: Vlastnosti kroucené dvojlinky

název kabelu	standard	označení	rychlost přenosu	konektor	šířka pásma
Kroucená dvojlinka	100 Base - T	Kategorie 5	100 Mb/s	RJ - 45	100 MHz
Kroucená dvojlinka	1000 Base - T	Kategorie 5e	1000 Mb/s	RJ - 45	125 MHz
Kroucená dvojlinka	1000 Base - TX	Kategorie 6	1000 Mb/s	RJ - 45	250 MHz
Kroucená dvojlinka	1000 Base - TX2	Kategorie 7	1000 Mb/s	GC45, TERA	600 MHz

V podstatě se můžeme setkat s dvojím provedením dvojlinky:

Nestíněná kroucená dvojlinka – UTP

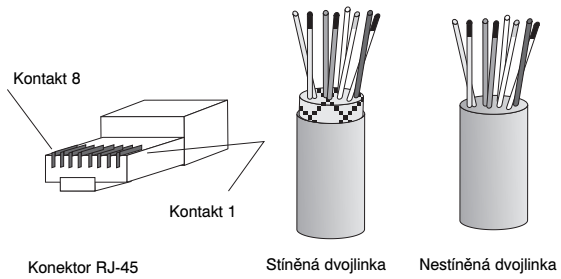
(Unshielded Twisted Pair)

Jednotlivé páry jsou vloženy do vnější plastické izolace. Je nejpoužívanějším vodičem v kabeláži sítí LAN.

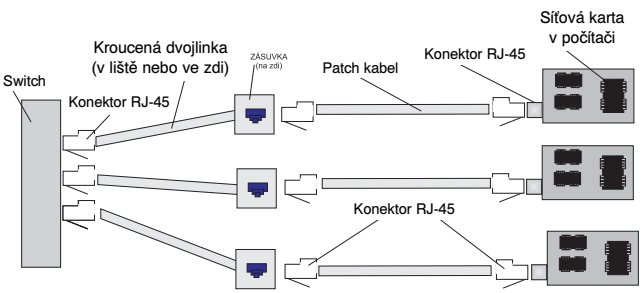
Stíněná kroucená dvojlinka – STP

(Shielded Twisted Pair)

Od nestíněného kabelu se liší kovovým opletením – stíněním, zvyšujícím ochranu proti vnějšímu rušení. Stíněn může být každý pár uvnitř kabelu, nebo se stíní pouze plášť kabelu, takový vodič se pak označuje jako Screened (ScTP). STP a ScTP kabely jsou samozřejmě dražší než nestíněný kabel a používají se jen tam, kde k vnějšímu rušení dochází.



Obrázek 1.2: *Kroucená dvojlinka a konektor RJ-45*



Obrázek 1.3: *Prvky kabeláže založené na kroucené dvojlince*

Praktické provedení

Zjednodušený princip kabeláže ukazuje obrázek. Pro kabeláž twisted pair je nutný prvek, kterým jsou jednotlivé kabely spojeny, nazýváme jej Switch (poznámka českého vydavatele: výraz „switch" se správně do češtiny překládá jako přepínač, ale původní termín je v odborné veřejnosti častěji používán, proto v dalším textu uvádíme termín switch) a jsou mu blíže věnovány kapitoly *Aktivní prvky kabeláže* a *Strukturovaná kabeláž*. V praxi se kabely ze Switche nepřipojují přímo k počítači (i když možné to je), ale do zásuvek RJ-45, z nichž potom vede kabel k počítači. Pro kabel počítač – zásuvka se používá termín patch kabel.

Kabel používaný v sítích LAN se skládá ze čtyř párů (tedy osmi vodičů). U kabelů používaných pro rychlost 100 Mb/s se využívají pouze 2 páry, zbylé 2 jsou nevyužity. U rychlejší varianty – s rychlostí 1000 Mb/s (neboli Gb/s), je nutné použít všechny 4 páry. Pokud je stávající rozvod proveden kabeláží kategorie 5e, není s přechodem na rychlejší Ethernet problém, v opačném případě je většinou nutná také výměna kabeláže. Využití vodičů v kabelu (pro nejpoužívanější síťový standard Ethernet) ukazuje tabulka. Její první řádek se ještě vrací k dnes již staré (ale občas ještě dosluhující technologii 10 Mb/s).

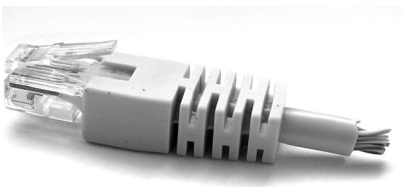
Tabulka 1.3: Využití vodičů v kabelu

Síťový standard	Rychlost [Mb/s]	Vodiče 1, 2	Vodiče 3, 6	Vodiče 4, 5	Vodiče 7, 8
10 BASE - T	10	TX	RX		
100 BASE - TX	100	TX	RX		
1000 BASE - T	1000	Bi	Bi	Bi	Bi

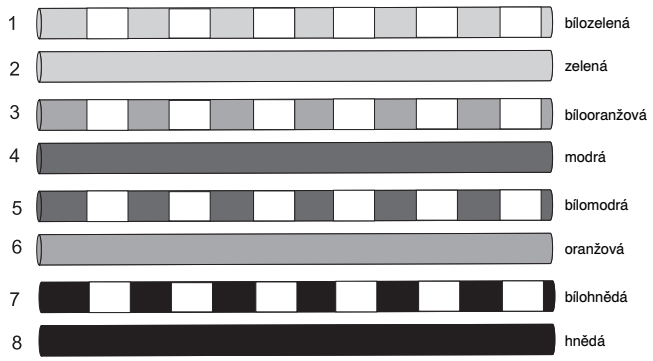
Zkratky v tabulce mají následující význam:

- TX = vysílání (Transmit)
- RX = přijímání (Receive)
- Bi = obousměrný režim (bi-directional)

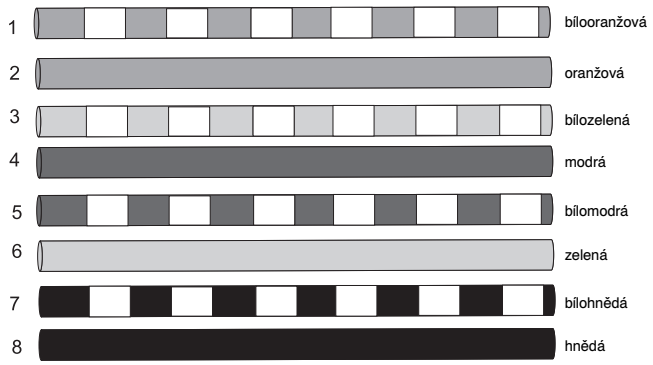
Vodiče jednoho páru jsou navzájem zkrouceny. Oba dráty mají stejný barevný základ, ale jeden z vodičů páru má barvu kombinovanou s bílou. Všechny vodiče se zakončují v konektoru RJ-45. Barevné značení vychází z norem TIA/EIA 568-A a TIA/EIA 568-B, varianta B je u nás patrně rozšířenější. Barevné značení jednotlivých vodičů v párech ukazují obrázky. Vidíme, že v každém barevném schématu je jeden pár vodičů rozdělený (ve skutečnosti je i rozdělený pár smotán a v kabelu veden společně, k rozdělení dojde až při připojování vodičů ke konektoru RJ-45).



Obrázek 1.4: *Konektor RJ-45*

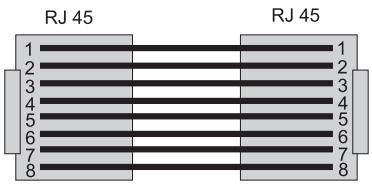


Obrázek 1.5: *Barevné schéma TIA/EIA 568-A*

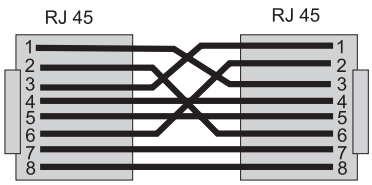


Obrázek 1.6: *Barevné schéma TIA/EIA 568-B*

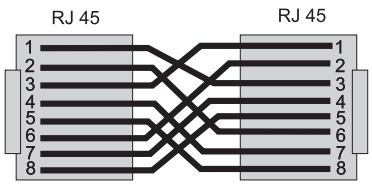
Propojovací kabely počítač – zásuvka, zásuvka – switch, či počítač – switch se zapojují na obou koncích stejně. Pokud však propojujete jen dva PC, není nutný switch a počítače můžeme spojit přímo. Kabel však musí být zapojen kříženě (aby vysílání přicházelo na příjem a naopak). Někdy potřebujeme křížené zapojení také při propojování switchů (novější switche dokáží překřížení simulovat a propojují se nekříženými kabely). Jednotlivé varianty ukazují obrázky:



Obrázek 1.7: *Přímé zapojení*



Obrázek 1.8: *Křížené zapojení pro kabel 100 Mb/s*



Obrázek 1.9: *Křížené zapojení pro kabel 1000 Mb/s*

- přímé zapojení je jednoduché, čísla pinů v obou konektorech kabelu jsou stejná
- v případě 100 Mb/s (norma Ethernet 100 BASE – TX) již křížené zapojení čísla pinů konektorů stejného kabelu mění. Víme také, že vodiče 4, 5, 7, 8 nejsou použity, a tak je není třeba křížit
- u 1000 Mb/s (norma Ethernet 1000 BASE – T) se používají všechny vodiče, a tak se také všechny kříží.

Při zapojování kabelů oceníme tabulky s barevným značením vodičů, které následují.

Tabulka 1.4: Křížené zapojení 100 Mb/s

1. konektor RJ-45	barva	2. konektor RJ-45	barva
1	bílo oranžová	1	bílo zelená
2	oranžová	2	zelená
3	bílo zelená	3	bílo oranžová
4	modrá	4	modrá
5	bílo modrá	5	bílo modrá
6	zelená	6	oranžová
7	bílo hnědá	7	bílo hnědá
8	hnědá	8	hnědá

Tabulka 1.5: Křížené zapojení 1000 Mb/s, TIA/EIA 568-A

1. konektor RJ-45	barva	2. konektor RJ-45	barva
1	bílo zelená	1	bílo oranžová
2	zelená	2	oranžová
3	bílo oranžová	3	bílo zelená
4	modrá	4	bílo hnědá
5	bílo modrá	5	hnědá
6	oranžová	6	zelená
7	bílo hnědá	7	modrá
8	hnědá	8	bílo modrá

Tabulka 1.6: Křížené zapojení 1000 Mb/s, TIA/EIA 568-B

1. konektor RJ-45	barva	2. konektor RJ-45	barva
1	bílo oranžová	1	bílo zelená
2	oranžová	2	zelená
3	bílo zelená	3	bílo oranžová
4	modrá	4	bílo hnědá
5	bílo modrá	5	hnědá
6	zelená	6	oranžová
7	bílo hnědá	7	modrá
8	hnědá	8	bílo modrá

Optický kabel (fiber optic cable)

Je založen na odlišném principu než předešlé kabely. Data nejsou přenášena elektricky v kovových vodičích, ale světelnými impulsy ve světlovodivých vláknech.

Řez kabelem ukazuje obrázek. Základní prvek kabelu – optické vlákno (jsou minimálně dvě, pro každý směr jedno, běžně bývá v kabelu několik párů světelných vláken) je vloženo do vrstvy sekundární ochrany, která zabraňuje mikroohybům kabelu (ty by utlumovaly průchod světelného paprsku vláknem). Konstrukční vrstva zvyšuje pevnost kabelu. Vše je uloženo v plastovém vnějším krytu.

Existují dva druhy optických kabelů, které se liší způsobem vedení paprsku ve vlákně:

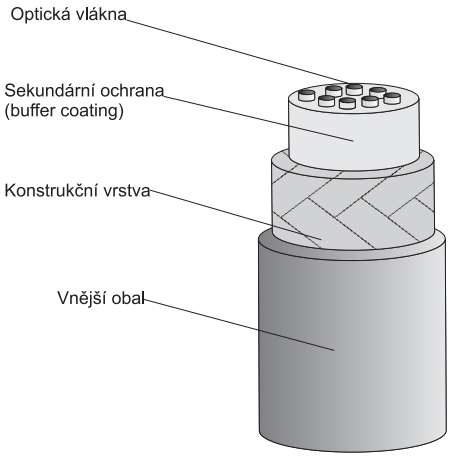
Mnohovidové

U nichž se paprsek odráží od pláště vlákna. Během přenosu je původní světelný paprsek rozložen na více světelných částí, tzv. vidů. Na konec kabelu pak dojde původní paprsek rozložený na několik vidů. Příjemce provede součet jednotlivých vidů a dostane původní informaci. Vidy však dorazí k cíli s určitým časovým odstupem – přenášený údaj je zkreslen.

Kabel má horší optické vlastnosti (proměnlivý index lomu), je však levnější a lépe se s ním pracuje. U sítí LAN se používají převážně tyto kabely.

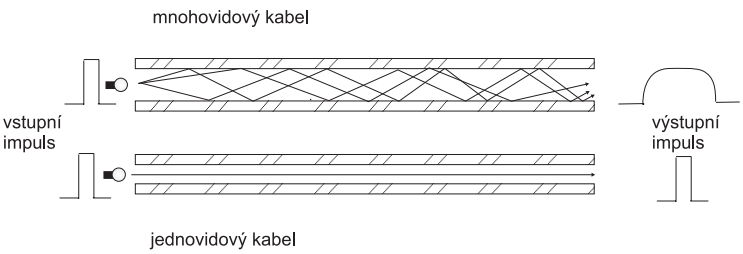
Jednovidové

V nichž je index lomu mezi jádrem a pláštěm optického vlákna velmi malý. Kabelem prochází jen jeden paprsek (jeden vid) bez lomů a ohybů. Jednovidové kabely mají lepší optické vlastnosti a tím vyšší přenosovou kapacitu, dokáží přenést signál na delší vzdálenost než mnohovidové, jsou ale dražší.



Obrázek 1.10: *Optický kabel*

Koncovky



Obrázek 1.11: *Jedno a vícevidové optické vlákno*

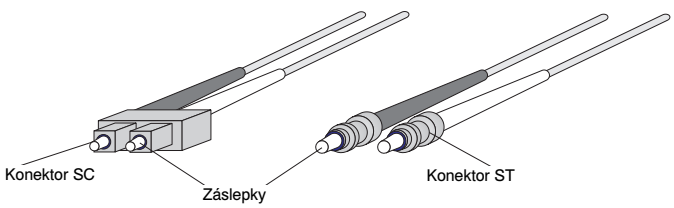
Podobně jako předešlé druhy vodičů, je také optický kabel ukončen normovanou koncovkou. Převážně se používají dva typy zakončení:

- kulatý konektor ST
- hranatý konektor SC

Konektory ukazuje obrázek. Při manipulaci s kabelem musejí mít konektory nasazenu záslepku!

Příslušenství optických kabelů

Optickým kabelem přenáší data světelný paprsek, ale ze síťové karty počítače vystupují údaje ve formě elektrických impulsů. Proto je na konci každého kabelu nutný **převodník** (transceiver). Jeho úkolem je převod elektrických paprsků na světelné impulsy a naopak. Převodník bývá často zabudován ve switchích. Switch pak má několik portů pro kroucenou dvojlinku a alespoň jeden port pro optický kabel. Tím dojde k propojení obou kabelových soustav.

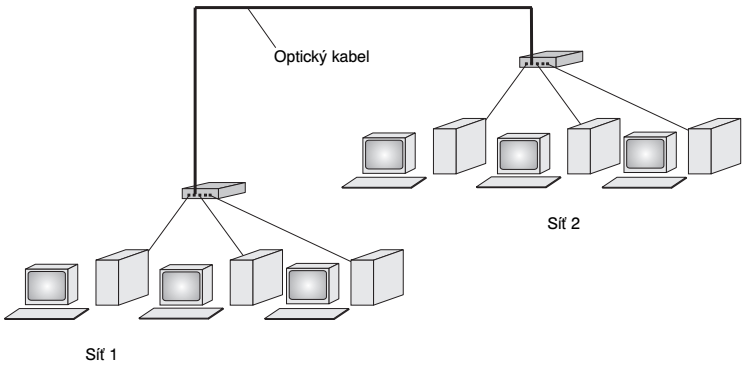


Obrázek 1.12: *Konektory optického kabelu*

Dalším prvkem, který se využívá v optické kabeláži je **konvertor**. Ten dovoluje napojit optický kabel na kroucenou dvojlinku. Má tedy zdířku pro optický kabel a kroucenou dvojlinku. Jeho elektronika zároveň převádí světelný paprsek na elektrické impulsy.

Optické kabely mají mnoho výhod: přenos dat na velké vzdálenosti (řádově kilometry), vysokou kapacitu přenášených dat a rychlost 100 Mb/s. Další jejich výhodou je absolutní odolnost proti všem elektromagnetickým rušením a vysoká bezpečnost přenášených dat (optické signály nejde odposlouchávat).

Jejich hlavní nevýhodou je cena optické kabeláže. Vlastní kabel drahý není, ale ostatní prvky kabeláže jsou již dražší. Složité a drahé je především konektorování.



Obrázek 1.13: *Typické použití optického kabelu*

Optické rozvody se většinou nepoužívají k připojování jednotlivých počítačů, kde by se jejich montáž prodražila. Najdeme je v páteřních vedeních, která spojují jednotlivé sítě. Zde se využije jejich rychlost, kapacita a přenos dat na velké vzdálenosti. Dále se používají k propojování síťových segmentů mezi budovami. Důvodem je výše uvedená odolnost proti všem elektromagnetickým rušením (např. bleskům) a galvanické oddělení budov.

Srovnání jednotlivých typů kabelů

Závěrem uvádím tabulku v níž jsou shrnuty vlastnosti dříve popsaných kabelů.

Tabulka 1.7: Srovnání kabelů

typ kabelu	výhody	nevýhody	použití
Kroucená dvojlinka	Levná, jednoduchá montáž, rychlost 100 a 1000 Mb/s	Musí se používat aktivní prvek – Switch	Dnes standard
Optický kabel	Rychlost 100 a 1000 Mb/s, odolnost proti rušení, přenos na dlouhé vzdálenosti. Galvanické oddělení spojovaných sítí.	Drahé příslušenství a montáž (především konektorů)	Pro propojování jednotlivých sítí nebo budov.

Trocha teorie

Pro další výklad je nutné vysvětlit některé teoretické pojmy, nutné pro pochopení práce počítačových sítí. Jde o základní principy práce, normy a uspořádání sítí.

Komunikace v sítích

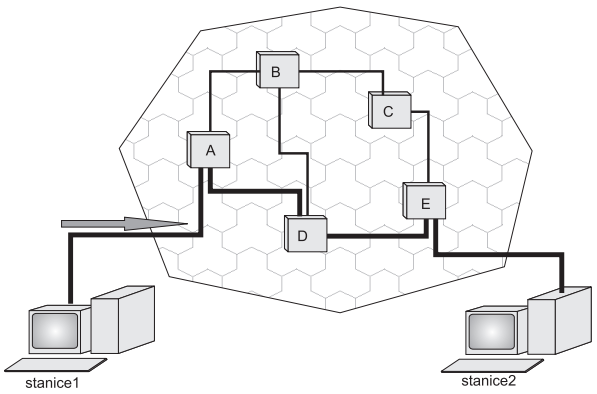
Komunikace mezi stanicemi může probíhat podle dvou základních komunikačních modelů:

Sítě spojové (with connection)

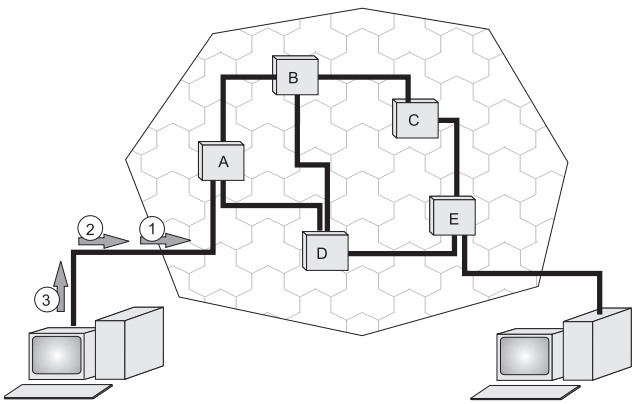
Přesněji nazývané sítě s navazováním spojení. Před zahájením výměny dat je nutné mezi oběma koncovými stanicemi navázat spojení. Koncové uzly v síti se musí nejdříve domluvit s aktivními prvky a následně vytvořit kanál, prostřednictvím něhož budou přenášena data. Na našem ilustračním obrázku vidíme příklad:

1. nejdříve se vytvoří spojení *stanice 1 – uzel A – uzel D – uzel E – stanice 2.*
2. potom se uskuteční přenos dat, která se přenášejí v souvislém proudu.

Tento způsob práce je typický pro telefonní sítě, u sítí LAN (s výjimkou sítě ATM) se s ním nesetkáme.



Obrázek 1.14: *Spojový přenos dat*



Obrázek 1.15: *Paketový přenos dat*

Sítě nespojové (connectionless)

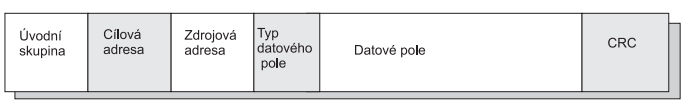
Sítě bez navazování spojení pracují tak, že přenášená data rozdělí na malé balíčky – pakety (packet). Ty putují sítí, až dorazí k cíli. Samozřejmě vše tak jednoduché není. O tom kudy budou pakety putovat rozhodují jednotlivé uzly sítě. Ty si přečtou cílovou adresu, kterou si paket nese s sebou (paket je popsaný v následující kapitole) a rozhodnou kam paket pošlou. Každý paket tak může putovat vlastní cestou, dokonce mohou pakety dorazit do cíle ve špatném pořadí (např. paket 3 před paketem 1). Ve skutečnosti je v sítích k dispozici řada aktivních prvků, kterými jsou pakety filtrovány a usměrňovány – přepojovány. Tento způsob výměny dat je v sítích LAN typický, označujeme jej jako přepojování paketů (packet switching).

Opět vidíme příklad na obrázku. Při přenosu dat ze stanice 1 do stanice 2 jsou data rozdělena na tři pakety. Jejich trasa v síti je definována jednotlivými uzly. Uzel A rozhodne zda paket pošle do uzlu B nebo D, bude-li cílem uzel B, může pak paket putovat do uzlu D nebo E atd.

Paket

Z předešlého výkladu již víme, že přenášená data se v sítích dělí na malé části, balíčky – pakety. Paket je tedy množina dat uzpůsobená k přenosu. (Soubor kopírovaný z jednoho PC do druhého je nejdříve rozložen na pakety, přenesen a pak zpětně složen.)

Na obrázku vidíme příklad datového paketu pro síťový standard Ethernet (síťové standardy jsou popsány dále). Paket začíná úvodní synchronizační skupinou bajtů. Následuje cílová adresa (kam paket míří), zdrojová adresa (odkud byl paket vyslán). Nejdůležitější (a nejdelší) je datové pole, v němž jsou uložena přenášená data. Je uvedeno krátkým polem popisujícím typ přenášených dat. Paket je ukončen polem kontrolního součtu (CRC). To umožňuje zkontrolovat správnost přenesených dat.



Obrázek 1.16: *Datový paket*

Model ISO/OSI

Počítačové sítě vyvíjelo více firem, zpočátku to byly uzavřené a nekompatibilní systémy. Hlavním účelem sítí je však vzájemné propojování, a tak vyvstala potřeba stanovit pravidla pro přenos dat v sítích a mezi nimi. Mezinárodní ústav pro normalizaci ISO (International Standards Organization) vypracoval tzv. referenční model OSI (Open Systems Interconnection), který rozdělil práci v síti do 7 vzájemně spolupracujících vrstev.

Jak již bylo řečeno, model ISO/OSI rozděluje síťovou práci na vrstvy. Princip spočívá v tom že vyšší vrstva převezme úkol od podřízené vrstvy, zpracuje jej a předá vrstvě nadřízené. Vertikální spolupráce mezi vrstvami (nadřízená s podřízenou) je věcí výrobce sítě. Model ISO/OSI doporučuje jak mají vrstvy spolupracovat horizontálně – dvě stejné vrstvy modelu mezi různými sítěmi (či síťové prvky různých výrobců) musejí spolupracovat.

Model je důležitý především pro výrobce síťových komponent. V praktické práci se sítí jej moc nevyužijeme. Umožňuje však pochopit principy práce síťových prvků a zároveň patří k základní terminologii sítí. Proto se o něm alespoň stručně zmíním. Práci jednotlivých vrstev nastiňuje tabulka.

Tabulka 1.8: Úkoly vrstev modelu ISO/OSI

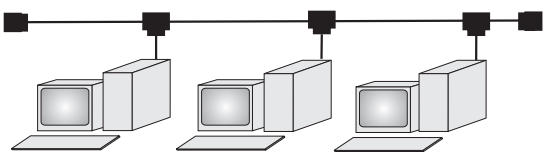
Aplikační vrstva (Application Layer)	Je určitou aplikací (např. oknem v programu) zpřístupňující uživatelům síťové služby. Nabízí a zajišťuje přístup k souborům (na jiných počítačích), vzdálený přístup k tiskárnám, správu sítě, elektronické zprávy (včetně e-mailu)…
Prezentační vrstva (Presentation Layer)	Má na starosti konverzi dat, přenášená data mohou totiž být v různých sítích různě kódována. Tato vrstva zajišťuje sjednocení formy vzájemně přenášených údajů. Dále data komprimuje, případně šifruje… V praxi často splývá s relační vrstvou.
Relační vrstva (Session Layer)	Navazuje a po skončení přenosu ukončuje spojení. Může provádět ověřování uživatelů, zabezpečení přístupu k zařízením…
Transportní vrstva (Transport Layer)	Typickou činností transportní vrstvy je dělení přenášené zprávy na pakety a opětovné skládání přijatých paketů do zpráv (při přenosu se mohou pakety pomíchat či ztratit).
Síťová vrstva (Network Layer)	Je zodpovědná za spojení a směrování mezi dvěma počítači nebo celými sítěmi (tj. uzly), mezi nimiž neexistuje přímé spojení. Zajišťuje volbu trasy při spojení (mezi uzly bývá více možných cest pro přenos paketu)… (Volbu trasy nazýváme směrováním – routingem).
Linková (spojová) vrstva (Data – link Layer)	Uskutečňuje přenos údajů (datových rámců) po fyzickém médiu, pracuje s fyzickými adresami síťových karet, odesílá a přijímá rámce, kontroluje cílové adresy každého přijatého rámce, určuje, zda bude rámec odevzdán vyšší vrstvě…
Fyzická vrstva (Physical Layer)	Popisuje elektrické (či optické), mechanické a funkční vlastnosti: jakým signálem je reprezentována logická jednička, jak přijímací stanice rozezná začátek bitu, jaký je tvar konektoru, k čemu je který vodič v kabelu použit…

Topologie sítí

Topologie je způsob, jakým jsou stanice v síti propojeny. Topologie je prvkem síťového standardu a podstatně určuje výsledné vlastnosti sítě. Úzce souvisí s kabeláží.

Sběrnicová topologie (bus topology)

Ke spojení stanice je použito průběžné vedení, od stanice ke stanici. Stanice se k vedení připojují pomocí odbočovacích prvků (např. T-konektorů). Tato topologie se používá především v sítích s koaxiálním kabelem.



Obrázek 1.17: *Sběrnicová topologie.*

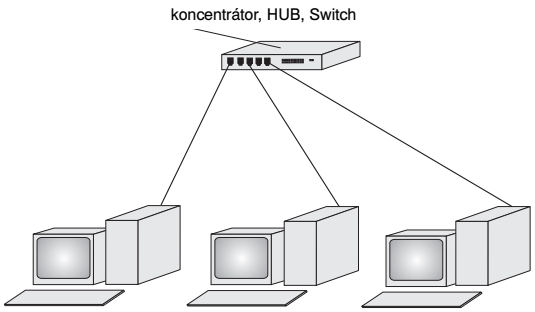
Ke spojení stanice je použito průběžné vedení, od stanice ke stanici. Stanice se k vedení připojují pomocí odbočovacích prvků (např. T – konektorů). Tato topologie se používala především v sítích s koaxiálním kabelem, dnes ji najdeme zřídka.

Výhodou sběrnice je to, že kabel vede od stanice ke stanici, s čímž souvisí poměrně malá spotřeba kabelu a nízká cena kabeláže. Nevýhodu představuje velký počet spojů v kabelu, což je příčinou mnoha potíží a poruch. Další nepříjemností je principiální nespolehlivost topologie. Jakékoliv přerušení sběrnice znamená havárii celé sítě – přerušení komunikace mezi všemi stanicemi. Dalším problémem je obtížná lokalizace poruchy.

Hvězdicová topologie (star topology)

Každá stanice je připojena vlastním kabelem, nejčastěji kroucenou dvojlinkou. Kabely od stanic jsou pak soustředěny do rozbočovače (koncentrátoru, HUBu dnes především Switche), který tvoří jakýsi střed sítě. K hvězdicovému propojení stanic se používá kroucené dvojlinky. Hvězda je dnes nejčastěji používanou topologií.

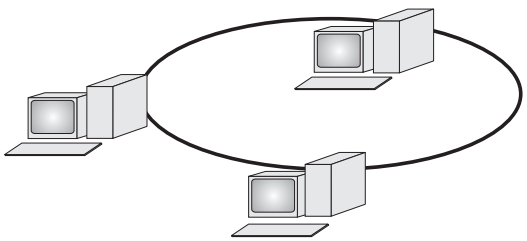
Výhodou je nízká náchylnost k chybě. Porucha jednoho kabelu vyřadí z činnosti pouze jednu síťovou stanici. Také lokalizace poruchy je podstatně jednoduší než u sběrnicové topologie.



Obrázek 1.18: *Hvězdicová topologie*

Kruhová topologie (ring topology)

Spojovací vedení stanic vytváří souvislý kruh, což dovoluje použít metodu postupného předávání zpráv (token) – viz dále. Nevýhoda je podobná jako u sběrnice – přerušení vodiče znamená poruchu celé sítě. To se řeší zdvojováním kabelu (např. u sítí IBM Token Ring).



Obrázek 1.19: *Kruhová topologie*

Páteřní vedení (backbone)

Závěrečný odstavec je věnován pojmu páteřní vedení, pojmu, který nemusí být každému jasný. V podstatě jde o vedení, kterým jsou propojeny ostatní segmenty sítě. Veškerá komunikace stanic přesahující jeden síťový segment pak prochází právě tímto vedením. Je jasné, že od něho požadujeme vysokou přenosovou rychlost – minimálně 100 Mb/s, raději Gb/s.

Tabulka 1.9: Porovnání topologií

topologie	výhoda	nevýhoda	rozsah použití
Sběrnice	Nízké pořizovací náklady	Poruchovost, obtížné vyhledávání místa závady, porucha kabeláže vyřadí celou síť	Dožívá ve starších kabelážích
Hvězda	Spolehlivá, rychlá	Nutnost koncentrátoru (switchů)	Dnes nejpoužívanější
Kruh	Pravidelné předávání zpráv v kruhu	Stejné jako u sběrnicové topologie, řeší se zdvojením vedení	Používají ji méně rozšířené sítě IBM Token Ring a FDDI

Přístupové metody

Tyto techniky popisují pravidla, jimiž se řídí přístup síťových stanic ke kabelu. V podstatě jde o to, jak zabezpečit, aby do sítě vysílala v jednom okamžiku pouze jedna stanice. Při současném vysílání více stanic dojde totiž k vzájemnému rušení, což znemožní přenos dat. Přístupová metoda, stejně jako topologie, je jedním z podstatných znaků síťového standardu.

CSMA-CD (Carrier-sense Multiple Access with Collision Detection), metoda náhodného přístupu

Rozhodování o tom, která ze stanic bude vysílat, probíhá následovně: Stanice, která chce vysílat, zkontroluje, zda již nevysílá jiný počítač. Pokud tomu tak je, počká až bude na spojovacím kabelu klid. Když zjistí, že je na kabelu volno, začne vysílat. Může se však stát, že ve stejném okamžiku začne s vysíláním i jiná stanice (proč ne, vedením neprocházely žádné signály). Proto vysílající stanice kontroluje, zda signály šířící se vedením odpovídají tomu, co sama vysílá. Pokud tomu tak není (po kabelu tedy posílá signály i jiný počítač), stanice se odmlčí a po náhodně stanovené době se pokusí o nové vysílání.

Výhodou této metody je její jednoduchost a tím i rychlost a nízká cena komponent. Nevýhoda spočívá v tom, že se stoupajícím počtem stanic se zvyšuje pravděpodobnost kolizí (tj. současného vysílání, jehož následkem je přerušení vysílání). V mezních případech může dojít až k zahlcení sítě. Tuto nepříjemnou vlastnost lze podstatně eliminovat použitím přepínačů (switch) a mostů, které nepropouštějí pakety do těch částí sítě, kam nepatří (výrazně se tak sníží vzájemné zarušování). (Jde o aktivní prvky kabeláže, jimž je věnována příští kapitola.) Další nevýhodou metody náhodného přístupu je její nedeterministická povaha – přidělování vysílacího času je náhodné, a tak nelze zaručit, za jak dlouho bude zpráva doručena. Proto se tento způsob řízení vysílání nehodí pro řízení provozu v reálném čase.

CSMA-CD je používána u síťového standardu Ethernet, normy u sítí LAN nejvíce rozšířené.

Token ring

Princip je jednoduchý. Sítí koluje speciální paket – token. Vysílat může jen ta stanice, která momentálně token vlastní. Právo vysílat má tedy v jednom okamžiku jen jedna stanice. Token si stanice postupně předávají. Je tak zajištěno spravedlivé rozdělování vysílacího času mezi stanice. Metoda Token ring se používá v sítích s kruhovou topologií – kde paket token může putovat od jedné stanice k druhé (po kruhu, v němž jsou stanice zapojeny).

Výhodou metody token je její odolnost proti zahlcení i při vysokém zatížení sítě (stanice se navzájem neruší) a její deterministická podstata (vysílání je pravidelně přidělováno všem stanicím). Nevýhodná je její složitost a o něco nižší rychlost (část činnost sítě je věnována oběhu paketu s tokenem).

Token bus

Je kopií předešlé metody, ale pro její činnost není nutná kruhová topologie. Každá stanice v síti obdrží logickou adresu (v síti se tak vytvoří logický kruh.). Token pak cyklicky putuje od adresy k adrese.

Vlastnosti takovéto sítě odpovídají metodě token ring, u token busu ještě přibývá nutnost logické adresace stanic.

Závěrem připomenu to, co již bylo řečeno mezi řádky dříve. Přístupové metody jsou dvojího typu:

- **Stochastické**, založené na náhodném přístupu k médiu. Typickým představitelem je Ethernet.
- **Deterministické**, kdy přístup k médiu je řízen – metody Token.

Aktivní prvky kabeláže

Po nutné teoretické odbočce se opět vracíme k síťové kabeláži, k prvkům, bez nichž sítě nemohou fungovat.

Model ISO/OSI formuje představu o tom, co vše je potřeba zajistit pro úspěšnou komunikaci v síti. Už první tři vrstvy (fyzická, linková a síťová) bezprostředně zajišťující komunikaci mají poměrně složité úkoly. Část z nich je integrovaná do elektroniky síťové karty, data přenese kabel, ale výběr trasy, kontrola správnosti paketů, rozhodnutí do které sítě má packet projít a kam ne, či mnoho dalších úkolů musejí provádět další prvky vložené do kabeláže. Tyto prvky aktivně ovlivňují dění v síti – proto jim říkáme aktivní prvky. (Síťové komponenty, které se na přenosu dat aktivně nepodílejí nazýváme prvky pasivními – např. kabely).

Zesilovač, opakovač (repeater)

Je nejjednodušším aktivním prvkem, protože pouze zesiluje (opakuje) jím procházející signál. Konstrukčně se jedná o krabičku se dvěma stejnými konektory. Používá se tam, kde je kabel tak dlouhý, že by na jeho konci už nebyl dostatečně silný signál. Nejčastěji jej najdeme u koaxiálních sítí.

Převodník (transceiver, media konvertor)

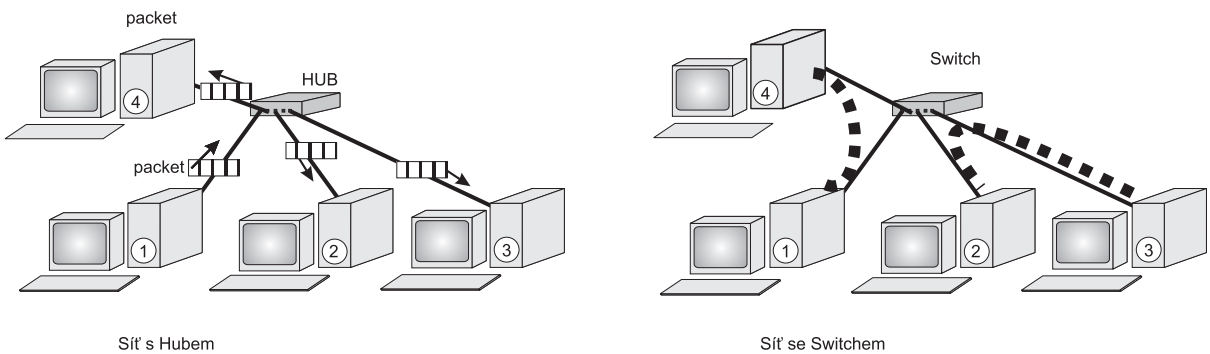
Je podobný zesilovači. Kromě toho, že signál zesiluje, převádí jej ještě z jednoho typu kabelu na jiný (např. kroucenou dvojlinku na optický kabel).

Rozbočovač, koncentrátor (Hub)

Byl nezbytným prvkem v sítích s hvězdicovou topologií (ale dnes jej nahradily switche). Jeho základní funkcí je rozbočování signálu, neboli větvení sítě.

Switch

V dnešních sítích se s Huby téměř nesetkáme. Většina sítí pracuje podle normy Ethernet (popsané v kapitole *Standardy síťového hardwaru*), pro niž je typická přístupová metoda CSMA – CD. Nevýhodou metody je postupné zahlcování sítě, stoupající s počtem stanic. Switch tuto nevýhodu výrazně eliminuje, odděluje totiž komunikující stanice od zbytku sítě. V podstatě vytvoří virtuální okruh mezi momentálně komunikujícími stanicemi. Příklad vidíte na obrázku. Pokud je v síti HUB a stanice 1 posílá paket stanici 4, je paket poslán všem stanicím sítě (ale pouze stanice 4 jej přijme). Je-li centrem sítě switch vytvoří se mezi oběma stanicemi spojení, oddělené od stanic ostatních. Komunikující stanice nejsou zahlcovány cizími pakety, nedochází ke zpomalování sítě a výměna dat mezi koncovými stanicemi probíhá maximální rychlostí. Na obrázku pak vidíme příklad dvou komunikačních kanálů: mezi stanicemi 1–4 a 2–3.

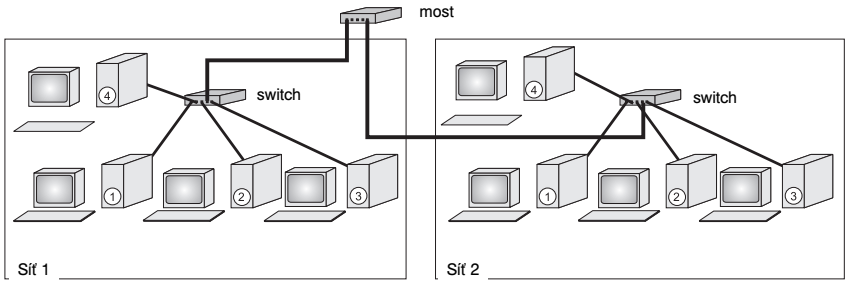


Obrázek 1.20: *Princip switche*

Most (bridge)

Most má podobné vlastnosti jako switch, je také schopen oddělit od sebe určité části sítě. Most je zařízením starším, jehož hlavním úkolem je oddělení síťových segmentů. Most je inteligentním prvkem, který se zajímá o přenášená data, plní dvě funkce:

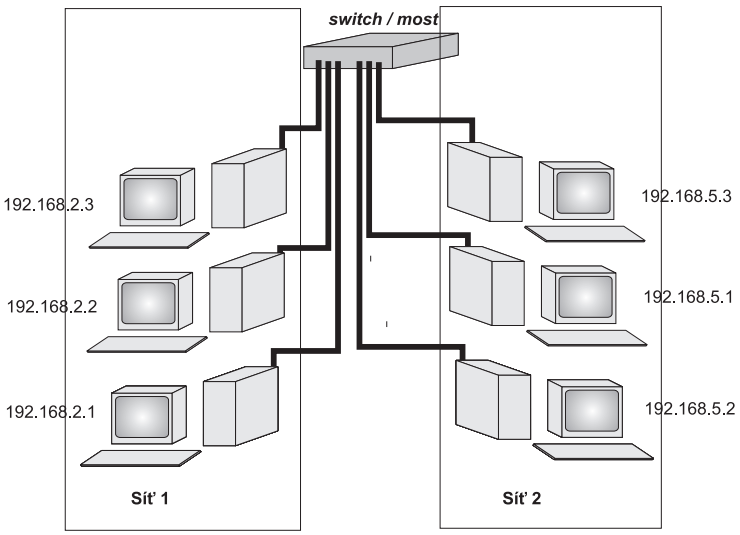
- **filtraci paketů**: Ta vychází z toho, že most si přečte cílovou adresu paketu. Paket pak propustí pouze do té části sítě, v níž je obsažen cíl paketu. Filtrováním se podstatně snižuje zatížení sítě, protože pakety neputují do síťového segmentu kam nepatří.



Obrázek 1.21: *Princip mostu*

- Druhou výhodou mostů je to, že dokáží **propojit dvě sítě různých standardů** Pracují totiž v linkové vrstvě ISO/OSI, takže fyzické odlišnosti sítí je neovlivňují.

Most může být realizován mnoha způsoby. Velmi často bývá integrován do switchů, ty pak nejenže síť rozbočují, ale zároveň filtrují přenášené pakety. Druhá velmi častá realizace mostů je softwarová. Funkci mostu plní síťový operační systém, který filtruje pakety mezi několika síťovým kartami.



Obrázek 1.22: *Adresové segmenty*

Na obrázku vidíte dvě sítě, které jsou odděleny mostem. Ten zajistí to, že pokud pakety putují ze stanice v síti 1 do stanice v síti 1, nejsou vpuštěny do sítě 2 (a naopak). Pokud však jsou pakety určeny pro druhou síť, jsou mostem propuštěny. Na obrázku (princip mostu) vidíte jedno z možných uspořádání, místo hardwarového mostu si můžete představit počítač s dvěma síťovými kartami. Pak bude funkci mostu zajišťovat operační systém. Nejčastěji je síť rozdělena (segmentována) pomocí adres. Takové řešení ukazuje obrázek. Zde existují dva adresové segmenty, první 192.168.2.x a druhý 192.168.5.x. Vzájemně jsou propojeny kombinovaným přepínačem s mostem. (V příkladu jsem předběhl výklad, adresaci – konkrétně protokolem IP vysvětluje kapitola *Protokol TCP/IP*).

Směrovač (router)

Je zatím nejinteligentnějším aktivním prvkem, s nímž jsme se setkali. Pracuje na úrovni síťové vrstvy ISO/OSI. Shromažďuje informace o připojených sítích a pak vybírá nejvýhodnější cestu pro posílaný paket. Má v sobě zabudova-

nou filtraci paketů, kterou doplňuje o inteligentní směrování. U sítí LAN se s ním nesetkáme často, typické je použití při připojování sítí k Internetu.

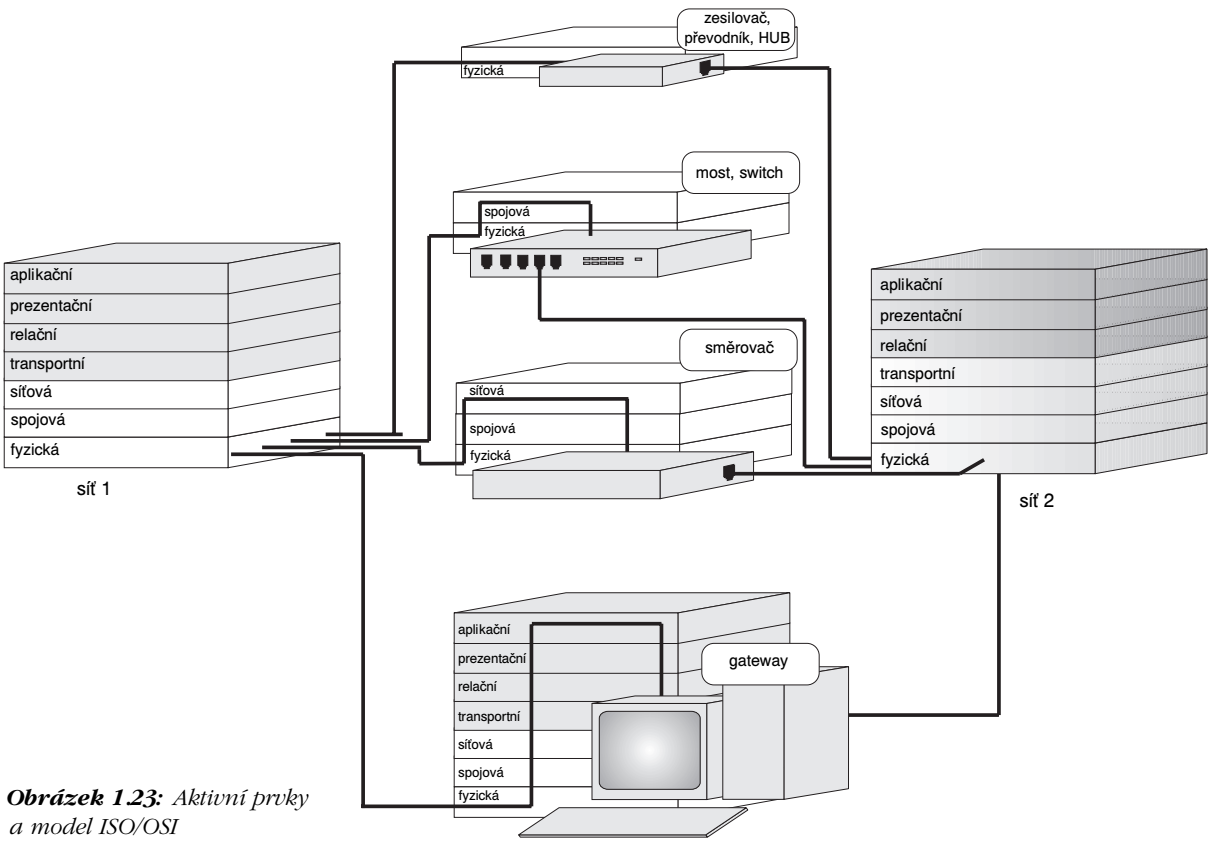
Brána (Gateway)

Pracuje až na nejvyšší úrovni vrstvy ISO/OSI – aplikační. Slouží k připojování sítí LAN na cizí prostředí, například k sálovým počítačům IBM.

Tabulka 1.10: Přehled aktivních prvků

Aktivní prvek	Funkce	Vrstva ISO/OSI
zesilovač	Zesiluje signály	fyzická
převodník	Převádí signály mezi různými typy kabelů	fyzická
rozbočovač (hub)	Rozvádí signály do všech větví sítě	fyzická
most	Filtruje pakety	linková
switch	Propojuje komunikující stanice	linková
směrovač	Směruje pakety	síťová
brána	Propojuje dvě rozdílné sítě	aplikační

Závěrečný obrázek představuje dvě sítě, reprezentované dvěma modely ISO/OSI. Mezi nimi jsou naznačeny aktivní prvky a jejich souvislost s modelem ISO/OSI.



Obrázek 1.23: *Aktivní prvky a model ISO/OSI*

Standardy síťového hardwaru

V předešlých kapitolách jsme si popsali části síťového hardwaru i zásady jeho práce. Jednotlivé síťové prvky je možné různě kombinovat (používat určité topologie, různé přístupové metody, jiné kabely, kabeláž doplňovat o aktivní prvky, používat různé varianty paketů…). Tato variabilita však působí proti základnímu poslání sítí, různě sestavené sítě se spolu nemusí domluvit. Proto byly přijaty normy – standardy, které definují základní požadavky na technické provedení síti. Normalizaci provádí organizace *IEEE* (Institute of Electrical and Electronics Engineers), tudíž jednotlivé normy nesou její označení. Pro počítačové sítě LAN jsou důležité standardy uvedené v tabulce:

Tabulka 1.11: Základní standardy IEEE pro sítě LAN

standard	určení
IEEE 802.3	Standardy sítě Ethernet
IEEE 802.4	Sběrnicové sítě s metodou přístupu token
IEEE 802.5	Kruhové sítě s metodou přístupu token
IEEE 802.11	Pro bezdrátové sítě

S normou IEEE se setkáme v technických parametrech všech síťových hardwarových komponent, proto je nutné popsat si jednotlivé normy. Z praktického hlediska nás nejvíce zajímají tyto standardem definované vlastnosti:

- Přístupová metoda
- Topologie sítě
- Typ kabelu, jeho délka, způsob připojení stanic (konektor)
- Rychlost přenosu dat

Norma se zabývá důkladným popisem všech detailů sítě, např. složením datového paketu, tvarem elektrických signálů atd. Při běžné práci se sítí nás však nejvíce zajímají výše uvedené vlastnosti. Při popisu jednotlivých norem se podrobněji zastavíme u těch, které se v sítích LAN nejvíce používají.

Ethernet (pro rychlost 10 Mb/s)

S pojmem Ethernet jsme se již několikrát setkali. Nejrozšířenější standard sítí LAN nelze totiž při popisu síťových komponent ignorovat. Od roku 1976, kdy jej navrhla firma Xerox, se vyvíjel a dnes tak existuje více jeho variant. Mezi základní znaky Ethernetu patří kolizní přístupová metoda CSMA/CD. Lze použít různé topologie a kabely (tím se zabývají jednotlivé specifikace Ethernetu). Díky rozšířenosti Ethernetu je příjemné velké množství aktivních prvků, které jsou na trhu k dispozici.

Při stavbě Ethernetové sítě je nutné dodržovat topologická pravidla, především délku segmentů a celé sítě. Kolizní přístupová metoda totiž předpokládá, že se signál šíří v síti nekonečně rychle. Začne-li vysílat jedna stanice na začátku sítě, je ji okamžitě „slyšet“ na konci sítě. Fyzikálně to je nesmysl (každé vlnění se šíří konečnou rychlostí) a tak jsou stanoveny maximální vzdálenosti, při kterých bude CSMA/CD ještě fungovat. Pro maximální rozměr sítě se také používá termín kolizní doména. Vzdálenosti závisí na elektrických vlastnostech kabelu a rychlosti přenosu dat.

Značení Ethernetu má pevná pravidla:

- První číslice – vyjadřuje rychlost, s níž standard pracuje.
- Slovo BASE popisuje signalizační metodu, ve většině případů jde o metodu BASE.
- Písmeno na konci popisuje kabel: F = optický kabel (fiber optical cable), T = nestíněná kroucená dvojlinka (copper unshielded twisted pair).

V případě normy 10 Base jde o rychlost dnes už pomalou a nepoužívanou, proto se o tomto zastaralém standardu zmíníme pouze krátce. Existoval v těchto variantách:

- **10BASE-5 (tlustý Ethernet)** – jeho základem byl tlustý koaxiální kabel a sběrnicová topologie.
- **10BASE-2 (tenký Ethernet)** – šlo o standard velmi rozšířený, používající tenký koaxiální kabel, tedy sběrnicovou topologii. Stanice se připojovaly pomocí T členů nebo EAD zásuvek. Délka kabelového segmentu byla maximálně 185 m, celé sítě pak 910 m. V jednom segmentu mohlo být maximálně 30 uzlů (stanic, zesilovačů, můstků atd.), celkový počet uzlů v síti nesměl překročit 1024. Konce kabelového segmentu musely být opatřeny zakončovacími odpory (terminátory).
- **10BASE-T (kabeláž kroucenou dvojlinkou)** – ve své době opět hodně používaná norma. Jejím základem je kroucená dvojlinka, HUB (později switch) a topologie hvězda. V síti mohly být maximálně 4 rozbočovače, použitím mostů, však bylo možné předcházející pravidlo obejít. Maximální délka kabelu mezi PC a hubem byla 100 m.
- **10BASE-F (kabeláž optickým kabelem)** – Ethernetový předpis pro optické kabely měl tři specifikace: **10BASE-FP** (fiber passive) pro připojování stanic. **10BASE-FL** (fiber link), k propojování pracovních stanic a Hubů. Ta je pro sítě LAN nejdůležitější, délka segmentu může být až 2 km. Je možné propojit 2 Huby, což je nejčastější použití (vlastně se tak spojí dva síťové segmenty). **10BASE-FB** (fiber backbone) pro páteřní rozvody mezi budovami.

Z tabulky (na konci kapitoly) vyčteme základní vlastnosti Ethernetových provedení, nicméně chci upozornit na značnou variabilitu normy. Délku segmentu lze prodlužovat pomocí zesilovačů, transceivery převedou signál mezi kabely, u kroucené dvojlinky lze zvýšit rychlost a spolehlivost zařazením switchů.

Fast Ethernet (Ethernet pro rychlost 100 Mb/s)

100 Mb/s Ethernet je momentálně nejrozšířenější normou, proto se jejímu popisu budeme věnovat důkladněji. Je normou odpovídající doporučení IEEE 802.3. Jedná se tedy o metodu přenosu dat založenou na přístupu CSMA/CD a ostatních pravidlech Ethernetu. Na rozdíl od norem Ethernetu pro rychlost 10 Mb/s není možné použít koaxiální kabel.

100BASE-T

Rychlý Ethernet je definován ve třech variantách:

- **100BASE-TX** pracuje na kabeláži s nestíněnou kroucenou dvojlinkou kategorie 5 s využitím dvou párů (stejně jako 10Base-T, zapojení najdete v kapitole *Kroucená dvojlinka*). Je také možné použít stíněnou dvojlinku. Maximální délka segmentu může být 100 m.
- **100BASE-FX** je určena pro optické kabely. Délka segmentu může být až 412 metrů pro vícevidové kabely a poloviční duplex, nebo až 10000 m pro jednovidový kabel a duplexní režim.
- **100Base-T4** je starší normou, používající rozvody starší kroucenou dvojlinkou kategorie 3 a 4 (lze použít i kategorii 5). Maximální délka segmentu je 100 m. Pro přenos dat jsou použity všechny 4 páry. V praxi se s ní téměř nesetkáme.

Pro instalaci sítě platí

Topologická pravidla jsou velmi přísná (signál se šíří 10x rychleji než u „starého Ethernetu“), ale nejdříve si musíme říci, že Fast Ethernet rozeznává dvě kategorie koncentrátorů (Hubů, rozbočovačů):

- Class 1 (translational repeater), převádí signál do digitální formy, což způsobuje zpoždění při zpracování signálu. Proto může být v doméně pouze jeden rozbočovač, ale dovoluje kombinaci obou fyzických signálních schémat, 100Base-TX i 100Base-T4.
- Class 2 (transparent repeater), signál pouze zesiluje, a tak je nutné používat pouze jednu normu, buď 100Base-TX, nebo 100Base-T4. V jedné doméně však mohou být použity 2 rozbočovače typu Class 2, mezi nimiž smí být maximální vzdálenost 5 m.

Délky segmentů ukazuje tabulka. V prvním řádku vidíte délku spojení koncový bod – koncový bod (nejčastěji stanice-stanice, nebo stanice-rozbočovač). Druhý řádek ukazuje maximální velikost kolizní domény při použití Hubu

Class I, s kabeláží UTP, optickou, nebo kombinovanou. Totéž popisuje následující řádek, ale pro Hub Class II. Maximální velikost sítě při použití dvou Hubů Class II vidíte v posledním řádku tabulky.

Tabulka 1.12: Velikosti segmentu Fast Ethernet

	UTP	Optika	UTP + Optika(TX + FX)
stanice – stanice stanice – switch switch – switch (poloviční nebo plný duplex)	100	412	nelze použít
Hub Class I (poloviční duplex)	200	272	260,8 (100 m kabelu UTP + jeden optický spoj)
Hub Class II (poloviční duplex)	200	320	308,8 (100 m kabelu UTP + jeden optický spoj)
2 x Class II hub (poloviční duplex)	205	228	216,2 (105 m kabelu UTP + jeden optický spoj)

Gigabitový Ethernet (pro rychlost 1000 Mb/s)

Nejnovější variací Ethernetu jsou standardy pro přenosové rychlosti 1000 Mb/s, standardizované pro optické kabely a kroucenou dvoulinku.

1000Base-X (802.3z – pro optické kabely)

Je navržen především pro optické kabely. Standard existuje ve dvou variantách, lišících se použitým světelným zdrojem (jehož světlem jsou kódovány přenášené informace):

- **1000Base-SX,** používá krátkovlnný světelný zdroj 850 nm. Zdrojem může být LED dioda nebo laser. Světlo se přenáší levnými mnohovidovými optickými kabely. Použití je u kratších horizontálních vedení nebo páteřních propojení.
- **1000Base-LX,** přenáší světlo delších vln 1310 nm, generované laserovým zdrojem. Je možné použít dražší jednovidové, ale i levnější jednovidové kabely. Výhodou je překlenutí delších vzdáleností.

Tabulka 1.13: Maximální délky optických kabelů Gb Ethernetu

Standard	Typ kabelu	Vlnová délka světelného zdroje	Vzdálenost přenosu	Typické použití
1000BaseSX	Mnohovidový	850 nm	220 m (62,5 μm) 500 m (50 μm)	Krátká horizontální vedení, krátká páteřní vedení
1000BaseLX	Mnohovidový	1300 nm	550 m (62,5 μm) 550 m (50 μm)	Krátká horizontální vedení, krátká páteřní vedení
1000BaseLX	Jednovidový	1300 nm	5 km (9 μm)	Dlouhá horizontální vedení, dlouhá páteřní vedení, propojování mezi budovami

(Ve sloupečku Vzdálenost přenosu je v závorce uveden průměr vlákna optického kabelu.)

1000Base-T (Standard 802.3ab – pro kovové kabely)

Definuje použití čtyřpárové kroucené dvojlinky kategorie 5, ale testován a doporučen je pro kabeláž kategorie 5e. Výraznou změnou v kabeláži Gigabitového Ethernetu (ve srovnání s Ethernety 10 BASE-T a 100 BASE-TX) je to, že oba dva typy kabelů (kategorie 5 i 5e) používají při gigabitovém přenosu všechny 4 páry vodičů.

Důvodem zavedení nové kabeláže byly problémy způsobované nehomogenitou v kabeláži (např. konektory). Jejím vlivem dochází k odrazům signálu. Odražené vlnění pak utlumí ostatní signály. Poprvé se tento jev projevil u Ethernetu 100 Mb/s, kde se řešil přísnějšími požadavky na provedení kabeláže. Pro gigabitový Ethernet byla vyvi-nuta nová kategorie kabeláže – Category 5E. Ta samozřejmě vychází z klasické Category 5, používané pro Ethernet i Fast Ethernet, ale jsou zde přísnější podmínky jak pro konektorování, tak na provedení všech součástí kabeláže (a rozdílné je již výše zmiňované využití všech párů kabelu).

Zpočátku byl gigabitový přenos používán hlavně pro páteřní vedení spojující sítě, pro připojení serverů, všude tam, kde se přenáší velké množství dat. Vlivem poklesu cen síťových karet a switchů GB Ethenetu dochází dnes k jeho velkému rozšíření také u menších sítí.

Poznámka: *Nepříliš využívaný standard 1000BaseCX definuje použití metalických kabelů – stíněné kroucené dvojlinky (STP) nebo koaxiálu, pro propojování na krátké vzdálenosti do 25 m (např. serverů, přepínačů apod.).*

Tip: Při přechodu na vyšší rychlost sítě se může stát, že kabeláž fungující spolehlivě na 100 Mb/s nemusí dobře pracovat na rychlosti 1000 Mb/s.

Závěrem dlouhého povídání o Ethernetu uvedu krátký souhrn jeho norem. Pokud v závěrečné tabulce chybí některé údaje, nedají se jednoduše uvést a najdete je v příslušné kapitole.

Tabulka 1.14: Přehled Ethernetů

norma	kabel	konektor	délka segmentu	topologie	maximální délka sítě	přenosová rychlost[Mb/s]
10BASE-5	koaxiální (tlustý)	AUI,	500 m	sběrnice	2500 m	10
10BASE-2	koaxiální (tenký)	BNC	185 m	sběrnice	910 m	10
10BASE-T	kroucená dvojlinka	RJ-45	100 m	hvězda	Podle hubů (ty lze propojovat a tak síť „natáhnout“)	10
10BASE-FL	optický kabel	ST, SC,	2000 m		2000 m	10
Fast Ethernet						
100Base-TX	kroucená dvojlinka	RJ 45 pro UTP DB-9 pro STP	100 m	hvězda		100
100Base-FX	optický kabel	ST, SC	412 m 10000 m			100
Giga Ethernet						
1000Base-X	optický kabel	ST, SC				1000
1000Base-T	kroucená dvojlinka	RJ-45				1000

10GB Ethernet (Standard 802.3ae)

Norma nejrychlejšího Ethernetu je vyvíjena nejen pro sítě LAN, ale je použitelná také pro sítě MAN a WAN. Předurčuje ji k tomu přenosová vzdálenost, která může být při použití jednovidového kabelu až 40 km. Jak je patrné, jsou jejím přenosovým médiem optické kabely. Opět existuje několik podstandardů (některé se ještě upřesňují), lišících se použitými kabely, vlnovou délkou světelných paprsků zdroje a šířkou přenosového pásma. Protože se v nejbližší době sítě LAN 10 GB Ethernet nijak masově nerozvinou, uvedeme si stručně alespoň základní charakteristiky jednotlivých standardů:

- **10GBASE-SR** je zamýšlený pro krátké vzdálenosti od 26 do 82 m a pro mnohovidový kabel.
- **10GBASE-LX4** s mnohovidovými kabely je schopný přenášet data od 240 do 300 m, s jednovidovým kabelem až na vzdálenost 10 km.
- **10GBASE-LR** a -**ER** pracují s jednovidovými kabely, přenosová vzdálenost je 10 a 40 km.

Poznámka: Standardizační komise pracují také na vývoji metalické normy 10GB Ethernetu – pro přenos po měděných kabelech.

Token Ring

Síť založenou na kruhové topologii a přístupové metodě Token Ring zkonstruovala firma IBM, s cílem propojit počítače lokální sítě s velkými sálovými výpočetními systémy IBM (např. S/390, AS/4000 apod.). Je zapracována do standardu IEEE 802.5. Mezi základní vlastnosti patří kruhová topologie, přístupová metoda Token Ring a tzv. centrální stanice MAU (jakýsi ekvivalent ethernetového rozbočovače). Původní rychlost byla 4 Mb/s, později zvýšená na 16 Mb/s, posledním vylepšením je rychlost 100 Mb/s (IEEE 802.5t).

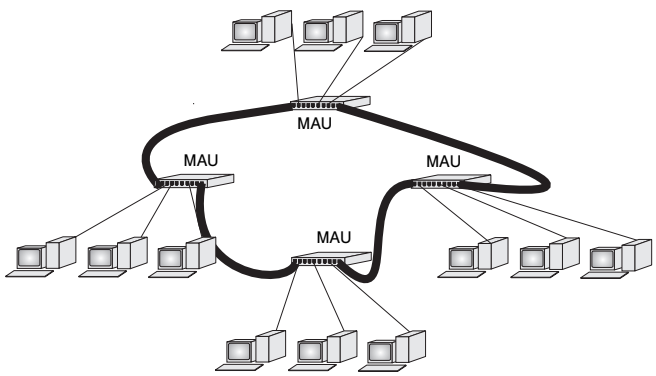
V síti je možné použít několika typů kabelů, jejich značení a základní vlastnosti ukazuje tabulka.

Tabulka 1.15: Kategorie kabelů IBM

Typ 1	Kabel tvořený dvěma kroucenými dvojlinkami (STP), které jsou opatřeny dvojitým stíněním.
Typ 2	Obdoba Typu 1, ale dvě kroucené stíněné dvojlinky jsou doplněny čtyřmi nestíněnými dvojlinkami. Ty se mohou použít pro telefonní hovory, diagnostiku sítě apod.
Typ 3	Kabel tvořený nestíněnými kroucenými dvojlinkami, parametry odpovídá telefonnímu kabelu.
Typ 5	Optický kabel se dvěma světlovodnými páry.
Typ 6	Podobný Typu 1, ale měděný vodič (drát) je nahrazen lankem. Má lepší mechanické, ale horší elektrické vlastnosti než Typ 1.
Typ 8	Vychází z Typu 1, ale je v plochém provedení, má tedy horší elektrické parametry.
Typ 9	Opět je podobný Typu 1 – dvě kroucené dvojlinky (STP). Používá se teflonová izolace, kabel je levnější, ale nevyhovuje požárním předpisům některých zemí.

Praktické provedení sítě IBM Token Ring ukazuje obrázek. Vidíme, jednotky MAU (Multistation Access Unit), které propojují kruhové vedení s jednotlivými stanicemi. Každý MAU má jednu zdířku RI (ring in) a jednu RO (ring out), sem se připojují patch kabely spojující jednotlivé MAU (ty pak tvoří kruh). Zbylé zdířky jsou určeny pro hvězdicové připojení stanic k MAU. Topologicky jde o kruh kombinovaný s hvězdou.

IBM Token Ring je konstrukčně složitější, a tím i dražší. Na druhou stranu je spolehlivější a používá bezkonfliktní metodu přístupu k vedení.



Obrázek 1.24: *IBM Token Ring*

FDDI (Fiber Distributed Data Interface)

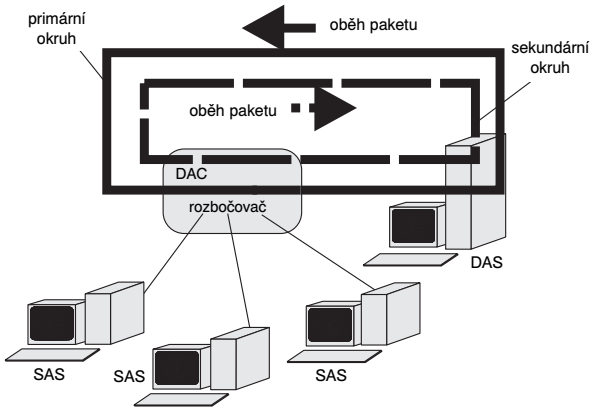
Síťový standard pro vysoce zatížené sítě se používal hlavně na začátku devadesátých let k propojování vzdálených areálů, metropolitních sítí a páteřních vedení. Mezi jeho podstatné znaky patří rychlost 100 Mb/s, dvojitá protisměrná kruhová topologie, optická kabeláž a přístupová metoda Token.

Jednotlivé uzly sítě jsou propojeny optickými kabely. Mezi stanicemi pravidelně cirkuluje token. Vysílat může jen ta stanice, která token zachytí a odstraní ze sítě.

Stanice jsou propojeny dvěma kruhy z optických kabelů. Po primárním probíhá veškerá komunikace mezi stanicemi. K dispozici je však ještě sekundární kruh, po němž putuje token v opačném směru. Pokud stanice ztratí připojení k primárnímu kruhu (např. výpadkem primárního kabelu), jsou oba kruhy propojeny a komunikace pokračuje bez přerušení dál.

U sítí FDDI rozlišujeme dva způsoby připojení stanic:

- **Dual attachment station, concentrator (DAS, DAC)** jsou připojeny k oběma optickým kruhům.
- **Single attachment station, concentrator (SAS, SAC)** jsou připojeny pouze k primárnímu kruhu.



Obrázek 1.25: *Princip připojování zařízení k síti FDDI*

K připojení se používají FDDI rozbočovače, koncová zařízení se tedy nepřipojují ke kabelům přímo.

Základní parametry sítě FDDI shrnuje tabulka, z níž je patrné, že FDDI se hodí především pro propojování metropolitních sítí, případně jako páteřní vedení pro propojování segmentů sítí LAN. Dnes se však i pro tyto účely používá levnější rychlý Ethernet.

Tabulka 1.16: Parametry sítě FDDI

kabeláž	optický kabel
rychlost	100 Mb/s
maximální vzdálenost stanic	jednovidové kabely: 10 km mnohovidové kabely: 2 km
maximální počet stanic	500 v kruhu
maximální délka kruhu	100 km

ATM (Asynchronous Transfer Mode)

Je podobně jako FDDI technologií, s níž se u běžných sítí LAN příliš nesetkáme. Používá se především pro páteřní vedení lokálních sítí či pro sítě metropolitní, v zaměření svého nasazení konkuruje sítím FDDI nebo Gigabitovému Ethernetu

Od všech technologií, s nimiž jsme se setkali se liší už svou základní koncepcí:

Je technologií **spojově** orientovanou (with connection). Před datovým přenosem mezi dvěma koncovými stanicemi musí být mezi nimi navázáno a sestaveno spojení.

Dříve uvedené technologie LAN fungují naproti tomu bez navazování spojení (connectionless), tzn. že stanice jednoduše začne vysílat data kdy potřebuje, aniž by navazovala spojení s protějším uzlem, či specifikovala cestu.

Dalším výrazným rysem ATM je **konstantní délka paketu**, který má 5bitovou hlavičku a nese 48 bitů dat. Pevná délka paketu dovoluje optimalizovat přepínače ATM a dosahovat přenosových rychlostí v řádech Gb/s. Pravidelný sled krátkých paketů zajišťuje nepřetržitý tok dat, takže ATM je možné použít kromě přenosu dat rovněž pro přenos zvuku a obrazu.

Pakety standardních technologií LAN mohou mít různou délku, navíc se přenášejí ve shlucích (burst) – to se příliš nehodí pro audio a video data. Obraz i zvuk mohou být trhané a přerušované.

Fyzická vrstva ATM není přesně definována, avšak pro správnou funkci je vyžadováno rozhraní k nějaké existující fyzické vrstvě, definované jinými síťovými standardy. Pro ATM je typická hvězdicová technologie a optické kabely.

Síťové karty (NIC – Network Interface Cards)

Už první obrázek v úvodu knihy ukazuje, že NIC je nezbytnou součástí hardwaru sítě. Teprve po zasunutí síťové karty do počítače získáme možnost připojit ho k síti. Karta zprostředkovává komunikaci mezi PC a sítí, podle pravidel daných síťovým standardem. Karta musí především vyhovět požadavku standardu na příslušný síťový protokol, přístupovou metodu a kabeláž.

Požadavek na připojení k síti je již tak běžný, že síťové karty jsou integrovány téměř ve všech základních deskách.

Parametry síťových karet

Karta je rozhraním mezi PC a sítí, její vlastnosti musí tedy korespondovat s vlastnostmi počítače na jedné straně a parametry určité sítě na straně druhé.

Z hlediska PC nás zajímá:

- Typ sběrnice základní desky PC (u integrované síťové karty samozřejmě není sběrnice potřeba), do níž budeme kartu zasunovat
- Wake-On
- Ovladač karty, který musí podporovat námi používaný operační systém

Ze strany sítě musí karta vyhovovat těmto požadavkům:

- Standardu síťového hardwaru
- Typu kabeláže
- Případnému duplexnímu provozu
- Případnému vzdálenému bootování

Sběrnice základních desek

Většina počítačů má síťovou kartu integrovánu na základní desce, ale občas potřebujeme použít dvě karty, nebo se setkáme s PC bez síťové karty. V takovém případě musíme do PC vsunout kartu novou.

Úspěch osobních počítačů spočívá (kromě mnoha jiných příčin) také v jejich snadné rozšiřitelnosti. Té je dosaženo tím, že mozek počítače – mikroprocesor komunikuje s okolím prostřednictvím standardizované sběrnice (která je součástí základní desky). Jde o soustavu vodičů, zakončenou rozšiřujícími konektory (sloty), do nichž je možné vkládat rozšiřující karty. Jednou z takových rozšiřujících karet je také karta síťová. Karty mohou být různě konstruovány, musejí však splňovat dvě podmínky: jít zasunout do rozšiřujícího slotu (mechanické rozměry, počet a tvar elektrických kontaktů) a nést informaci samy o sobě (tím řekne počítači s jakým typem karty bude spolupracovat).

U dnešních PC se můžeme setkat se dvěma typy systémové sběrnice:

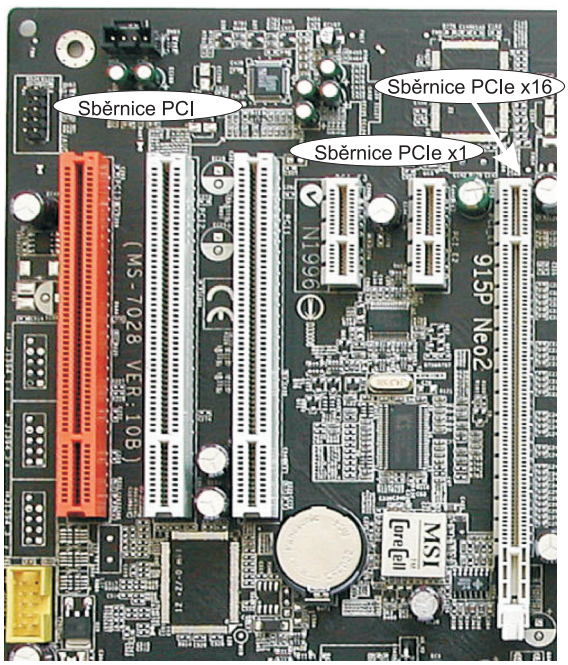
- **PCI (Peripheral Component Interconnect)** je dnešní standard. Jde o bílou zásuvku s řadou kontaktů uprostřed. Normu PCI používá převážná většina rozšiřujících karet. Sběrnice PCI (a její slot) je 32bitová a pracuje na frekvenci 33 MHz.
- **PCI Express (PCIe)** je sběrnicí relativně novou, rychlejší než PCI, která má před sebou velkou budoucnost. Na rozdíl od předešlých norem (včetně PCI) je sběrnicí sériovou, která existuje ve více variantách. Ty se od sebe liší počtem vodičů použitých pro přenos dat. Se zvyšujícím se počtem vodičů se prodlužuje také délka patice sběrnice. Přesné parametry ukazuje tabulka. Pro síťové karty se používá nejpomalejší varianta PCIe x1.

Tabulka 1.17: Propustnost sběrnice PCIe (v jednom směru)

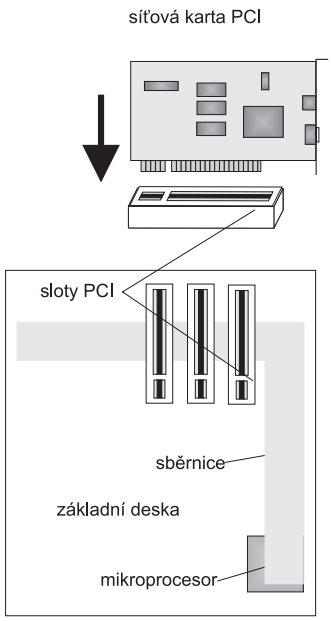
typ	propustnost	počet vodičů pro jeden směr
PCI Express x1	250 MB/s	2
PCI Express x2	500 MB/s	4
PCI Express x4	1000 MB/s	8
PCI Express x8	2000 MB/s	16
PCI Express x12	3000 MB/s	24
PCI Express x16	4000 MB/s	32
PCI Express x32	8000 MB/s	64

Pro doplnění počítače novou síťovou kartou musíme mít volný některý z rozšiřujících slotů.

Fyzickou instalaci rozšiřující karty (např. síťové karty do slotu sběrnice) naznačuje obrázek. Následujícím krokem je instalace ovladače rozšiřující karty. Ta bývá většinou automatická, ale někdy se stává velkým problémem. Proto jí je věnována samostatná kapitola.



Obrázek 1.26: *Sloty pro rozšiřující karty*



Obrázek 1.27: *Instalace síťové karty PCI do slotu PCI*

Wake-On

Vzdálené „buzení“ počítače sítí je poměrně nová vlastnost síťových karet. Díky ní je možné spustit počítač zapojený do sítě z jiného PC povelem přeneseným sítí. Téměř všechny nové 100Mb/s karty tuto vlastnost mají, k její správné funkci je ještě nutná podpora Wake-on základní deskou počítače. Ta musí být v provedení ATX, což je systém, který jednak definuje rozložení jednotlivých prvků na desce, jednak zavádí nový způsob napájení. Vypneme-li počítač, napájecí zdroj ATX bude dále napájet základní desku. Ta ve skutečnosti není vypnutá, ale pouze uspaná a čeká na signál, kterým bude probuzena. Zpravidla je impulzem pro její probuzení stisk zapínacího tlačítka, ale budící impulz může prostřednictvím síťové karty přijít také z jiného počítače.

Praktická realizace vzdáleného zapínání PC je součástí různých programů pro správu sítí – pro vzdálené zapnutí PC tedy musíme mít k dispozici takovýto softwarový síťový manažer.

Tip: V příslušenství karty s funkcí Wake-On je kablík, kterým musíme propojit zdířku označenou Wake-On na kartě se stejnou zdířkou na základní desce.

Standard síťového hardwaru

Pro vzájemnou komunikaci dvou zařízení je nutností, aby se obě zařízení „domluvila“. Výměna dat mezi nimi se tedy musí řídit určitými pravidly, která jsou obsažena v normách IEEE. Je logické, že těmto normám tedy musí vyhovovat také síťové karty. V jejich dokumentaci se vždy vyskytuje údaj o tom, pro který síťový standard je karta použita (např. Ethernet, Token Ring, či přesnou definicí např. 100Base-T).

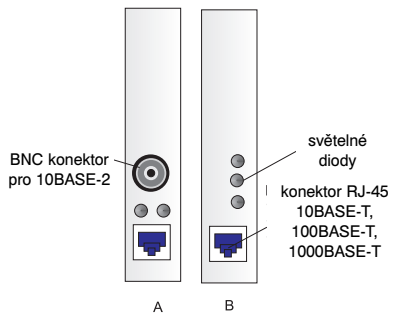
Součástí standardu je rovněž způsob adresace karet. U Ethernetu má každá síťová karta originální číslo (na světě neexistují dvě karty se stejným číslem), které je základem adresy.

Typ kabeláže

Ten navazuje na použitý síťový standard, ale z předešlých kapitol víme, že jednotlivé standardy mohou používat odlišné druhy kabeláže. Různé typy kabelů bývají zakončeny rozdílnými konektory, které musejí mít své protějšky na síťové kartě. Karty mohou být určeny pro jeden druh kabelu, ale mohou mít také několik zdířek pro různé druhy kabelů.

Nejčastěji používané zdířky síťových karet ukazuje obrázek:

- **Kombinace A**, dovoluje připojení tenkého koaxiálního kabelu (10Base-2) a kroucené dvojlinky (10Base-T). Používala se při postupném přechodu z koaxiální kabeláže na kroucenou dvojlinku. (Koaxiální kabel byl dříve velmi rozšířený, dnes se téměř nepoužívá, ani v naší knize jsem se jeho popisu již nevěnoval).
- **Kombinace B,** k ní je možné připojit pouze kroucenou dvojlinku. Vyhovuje tedy standardu 10Base-T, 100Base-T, případně 1000Base-T. Pro Fast Ethernetové a GB sítě je takovéto použití zdířek typické.



Obrázek 1.28: *Konektory síťových karet*

<u>Poznámka:</u> při popisu konektorů karty jsem použil příklady Ethernetových zdířek, u sítí nejpoužívanějších. V nabídkách výrobců síťových karet najdete také modely s koncovkami pro světelné kabely (zdířky ST, či SC), v takovém případě je karta vybavena vždy dvojicí konektorů (jeden pro vstup a druhý výstup signálu).

Novější síťové karty mívají na zadní straně kontrolky, které indikují činnost karty:

- Activity (ACT) bliká při přenosech dat mezi kartou a sítí.
- 10 LNK svítí, pracuje-li karta rychlostí 10 Mb/s.
- 100 LNK, mívají ji karty Fast Ehernetu, kontrolka svítí, pracuje-li karta rychlostí 100 Mb/s.

Označení LED diod se samozřejmě u jednotlivých výrobců liší. Při problémech s kartou je dobré prostudovat manuál a zjistit co vše mohou diody indikovat (např. blikáním, trvalým svitem …).

Tip: Pokud LNK nesvítí, je patrně chyba v kabeláži (vadný konektor, narušený kabel, špatně připojený kabel ve switchi, nespolupracující switch).

Duplexní provoz

Většina Ethernetových karet může pracovat ve dvou režimech:

- **Duplexním (Full duplex, FDX)** – schopnost současného přenosu mezi vysílající a přijímající stanicí v obou směrech.
- **Simplexním (Half duplex, HDX)** – schopnost přenosu dat mezi vysílající a přijímací stanicí v daném čase pouze v jednom směru.

Jestliže se zamyslíme nad principem přístupové metody CSMA/CD, bude se zdát duplexní provoz Ethernetové karty nemožný. Pokud v Ethernetu karta vysílá, nemá k přenosovému médiu přístup nikdo jiný. Výjimkou je však připojení síťové karty k přepínači (switch). Switch podporující duplexní režim umožní obousměrnou komunikaci point to point (z bodu do bodu) – mezi síťovou kartou a switchem. Během tohoto režimu je vypnut autodetekční obvod síťové karty, jehož úkolem je rozeznat vysílání jiné stanice v síti. Kolize v síti nenastane proto, že stanice je k síti připojována switchem. Ten dovolí průchod pouze paketům směřujícím ke konkrétní síťové kartě.

K duplexnímu provozu tedy potřebujeme duplexní síťovou kartu a duplexní switch. Oba dva musejí být do duplexního režimu přepnuty.

Vzdálené bootování

Připojení počítače k síti probíhá tak, že nejdříve počítač nastartuje (provede POST testy) a pak si z pevného disku načte do operační paměti operační systém. Jeho součástí je síťový klient, tedy software pro připojení počítače a jeho uživatele k síti.

Stanice, z níž se chceme připojit k síti, však nemusí mít pevný disk k dispozici. Pro takový případ obsahují síťové karty patici pro elektronický obvod (označovaný jako BootROM). V tomto zásuvném modulu je uložen program (v paměti ROM), jehož prostřednictvím se uživatel připojí k serveru (centrální síťové stanici). Ze serveru přenese do operační paměti bezdiskové stanice operační systém a síťového klienta (ti se jinak načítají z pevného disku PC). Stanice se tak může připojit k serveru a pracovat s jeho programy.

V dnešním prostředí osobních počítačů, založeném na operačních systémech Windows, se bezdiskové stanice téměř nepoužívají. Přesunování rozměrných programů Windows po síti je velmi pomalé a ceny pevných disků nejsou nijak vysoké.

Instalace ovladače

Pro správnou činnost je kromě fyzické instalace rozšiřující desky (tj. jejího zasunutí do slotu) nutné nahrání ovladačů nové karty do operačního systému. Tím doplníme operační systém počítače o programy nutné k jeho „domluvě“ s novou rozšiřující deskou.

Všechny síťové karty v provedení PCI a PCIe splňují normu *PnP. Plug and Play* (PnP, P&P) se dá volně přeložit jako „zastrč a hraj“. Posláním této metody je maximálně usnadnit rozšíření počítače novou deskou. Po zasunutí karty do slotu a zapnutí počítače proběhne automaticky „softwarové přidání karty“ (tj. nahrání nových ovladačů). Mohou nastat tři varianty:

1. Ovladač karty je Windows známý.
2. Ovladač karty Windows neznají a je nutné jej doinstalovat prostřednictvím *Průvodce nově rozpoznaným hardwarem*.
3. Ovladač karty (a zpravidla také další software) instalujeme pomocí instalačního programu.

V **prvním** případě budeme pouze informováni o průběhu instalace. Informační okénko se objeví v pravém dolním rohu *Hlavního panelu* – viz obrázek *Informace o instalaci nové síťové karty*.

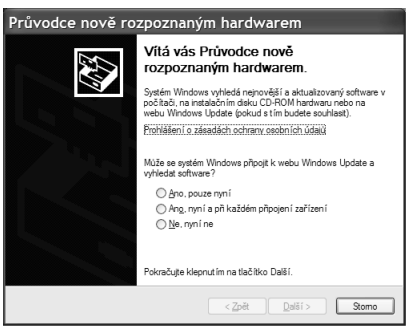
Obrázek 1.29: *Informace o instalaci nové síťové karty*

V **druhém** případě – když Windows ovladač k dispozici nemají, je nutné jej doplnit. K tomu slouží *Průvodce nově rozpoznaným hardwarem*. Jeho okno se objeví na obrazovce v okamžiku, kdy operační systém najde hardware, jehož ovladače nezná. Po vložení nové síťové karty do počítače (a jeho zapnutí) rozpozná PnP nový hardware a spustí *Průvodce:*

V jeho první obrazovce rozhodujeme o tom, zda ovladače budou hledány na webu Windows Update. Jde o web Microsoftu určený především k distribuci aktualizací Windows (a jiných *programů* Microsoftu, např. Office). Jsou zde uloženy také nové verze některých hardwarových ovladačů, ale rozhodně zde nenajdeme všechny ovladače. Proto se můžeme rozhodnout zda:

- vyhledání ovladačů zkusíme pouze nyní (*Ano, pouze nyní*),
- nebo se budou ovladače na Windows Update hledat vždy (*Ano, pouze nyní a při každém připojení zařízení*),
- Windows Update vůbec nepoužijeme *(Ne, nyní ne)*.

Poznámka: *Dotaz na Windows Update upravíme stiskem tlačítka Windows Update na kartě Hardware obrazovky Vlastnosti hardware (pravým tlačítkem myši klepneme na ikonce Tento počítač a vybereme Vlastnosti, pak přejdeme na záložku Hardware). Možnosti volby ukazuje obrázek Připojit k webu Windows Update.*



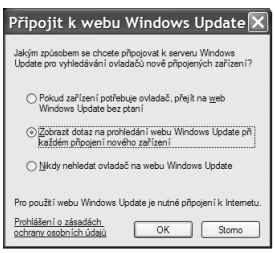
Obrázek 1.30: *Start Průvodce přidáním nového hardwaru*

Jestliže instalaci Windows Update nepoužijeme (nebo se nezdaří), přejdeme do druhé obrazovky *Průvodce*. Zde vybíráme:

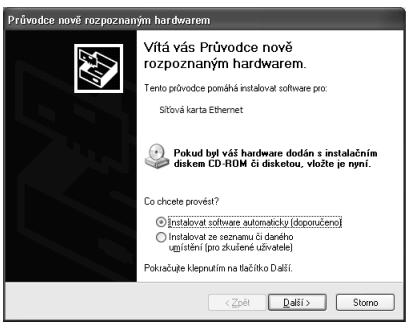
- *Instalovat software automaticky* – je to doporučená varianta. Máme-li instalační CD (nebo disketu s ovladačem), vložíme ji do mechaniky a systém zde ovladač najde a nainstaluje.
- *Instalovat ze seznamu či daného umístění...* – pokud víme kde je ovladač umístěný (např. jsme ho stáhli z Internetu), je výhodnější ope-rační systém o tom informovat (a ušetřit tak čas při prohledávání datových médií).

Budeme-li *Instalovat ze seznamu*, přejdeme do třetí obrazovky průvodce. Zde již blíže volíme umístění ovladače:

- *Vyhledat nejlepší ovladač v těchto umístěních* je základní volbou. Po jejím zaškrtnutí se nám zpřístupní další možnosti:

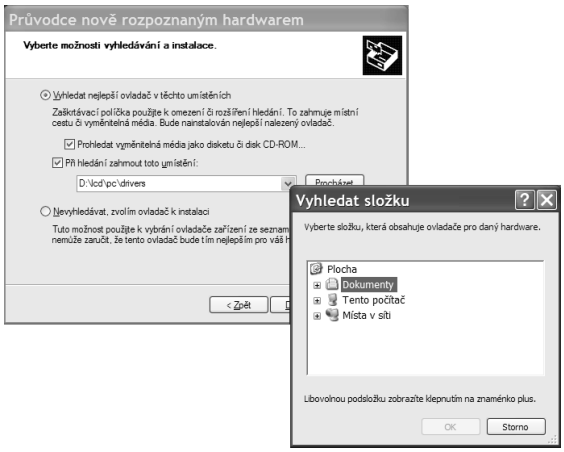


Obrázek 1.31: *Připojit k webu Windows Update*



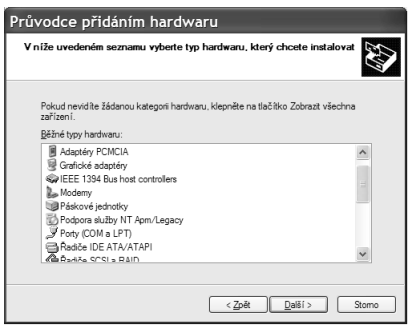
Obrázek 1.32: *Druhá obrazovka Průvodce*

- *Prohledat vyměnitelná média …* ovladač bude hledán na vyměnitelných médiích (kde bývá umístěn nejčastěji).
- *Při hledání zahrnout toto umístění* – do řádky můžeme napsat přesnou polohu ovladače, což nejsnadněji provedeme stiskem tlačítka *Procházet*. Následně pak umístění ovladače určíme v grafickém režimu.
- Opakem předešlých možností je *Nevyhledávat, zvolím ovladač k instalaci,* v tomto případě musíme konkrétní ovladač vybrat z databáze ovladačů zařízení Windows.



Obrázek 1.33: *Třetí obrazovka Průvodce.*

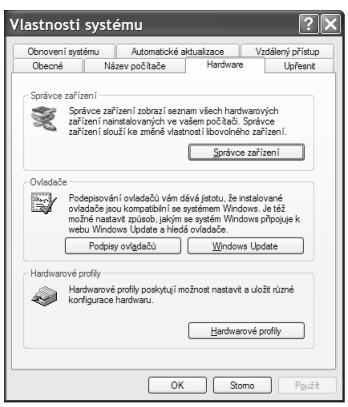
Ve **třetím** případě (kdy se ovladač nahrává instalačním programem) si musíme v manuálu síťové karty přečíst, jakým programem se instalace začíná (nejčastěji to je program s názvem Setup) a pak postupovat podle jeho pokynů.



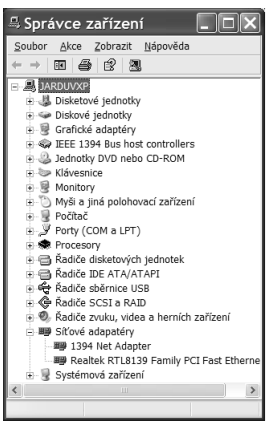
Obrázek 1.34: *Výběr ovladače z databáze Windows*

Informace o síťové kartě

Po instalaci karty doporučuji zkontrolovat její vlastnosti. Zjistíme tak, zda instalace byla úspěšná. Pravým tlačítkem myši klepneme na ikonce *Tento počítač* a vybereme *Vlastnosti*. Přejdeme na záložku *Hardware*, kde stiskneme tlačítko *Správce zařízení*. V obrazovce *Správce* vidíme všechna instalovaná hardwarová zařízení. Klepneme-li na položku *Síťové adaptéry,* zobrazíme informaci o všech instalovaných síťových kartách. Příklad správně instalovaných adaptérů vidíme na obrázku. Pokud by se instalace nezdařila, přidávané zařízení (v našem případě síťovou kartu) neuvidíme, nebo bude uvedena jako neznámé zařízení.



Obrázek 1.35: *Karta Hardware Vlastností systému*



Obrázek 1.36: *Instalované karty*

Shrnutí

Práce se síťovou kartu je velmi častá a tak na závěr kapitoly ještě jednou shrnu, co vše musíme vědět před nákupem a instalací síťové karty:

- Pokud nám nestačí integrovaná karta, zjistíme jaké sloty jsou na počítači k dispozici (PCI, PCIe).
- Musíme vědět na jaký typ sítě budeme počítač připojovat (nejčastěji to bude Ethernet), k jaké kabeláži bude karta připojena (kroucená dvojlinka či optika?), zda chceme kartu pro rychlost 100 Mb/s, 10/100 Mb/s, 1000 Mb/s nebo 100/1000 Mb/s.
- Musíme mít k dispozici ovladače, které pak budeme nahrávat do operačního systému počítače.
- Budeme požadovat další vlastnosti (Wake-On, vzdálené bootování)?

Strukturovaná kabeláž

Nyní již víme, že pro stavbu sítě můžeme použít různé typy kabelů, jejichž propojením vytvoříme topologii sítě. Provoz v síti se bude řídit pravidly stanovenými síťovým standardem (přístupová metoda, tvar paketu, možné kombinace kabelů a topologií…). Optimálním řešením pro hardwarové uspořádání sítě je strukturovaná kabeláž, jejíž zjednodušený příklad vidíme na obrázku.

Základem kabeláže je hvězdicová topologie (každá zásuvka je připojena svým kabelem), realizovaná kroucenou dvojlinkou. Zásuvky mívají nejčastěji dvě zdířky (pak do ní vedou dva kabely). Lze k nim připojovat různá zařízení (nejčastěji počítač a telefon). Všechny kabely jsou svedeny do propojovacího panelu (patch panelu) v rozvaděčové skříni. Ve skříni je kromě patch panelu ještě switch a telefonní ústředna. Zásuvkové kabely (ukončené v patch kabelu) pak můžeme propojovat buď se switchem (pak bude zdířka zásuvky určená pro PC), nebo telefonní ústřednou (konektor zásuvky slouží k připojení telefonu).

Nejčastěji bývá na každém patře jeden rozvaděč a v každé místnosti je alespoň jedna zásuvka. Celé řešení je velmi výhodné a má tyto přednosti:

- Možnost využití zásuvek jak pro datové, tak i telefonní přenosy. Systém má značnou variabilitu, k jedné zásuvce je možné připojovat různá zařízení (PC + telefon, 2 PC, 2 telefony) – stačí pouze přepojit propojovací (patch) kabely ve skříni.
- Hvězdicovou topologii, což usnadňuje údržbu a identifikaci poruch.
- Univerzálnost, je možné provozovat různé typy sítí, např. Ethernet, Token Ring. Kabeláž vyhovuje většině standardů, liší se aktivní prvky ve skříních (switch, MAU).
- Ochrana investic – vyšší pořizovací náklady jsou díky modularitě a flexibilitě systému kompenzovány minimálními náklady na další změny vyvolané konfigurací nebo rozšiřováním sítě, předpokládá se morální životnost 15–20 let.
- Možnost snadného přechodu na jiné komunikační prvky bez nutnosti rozsáhlých investic do nových rozvodů.

Důležitým konstrukčním prvkem strukturované kabeláže je rovněž rozvodná skříň, do níž se musí vejít všechny prvky (propojovací kabel, rozbočovače, ústředna…), ale měla by zabírat co nejméně místa.

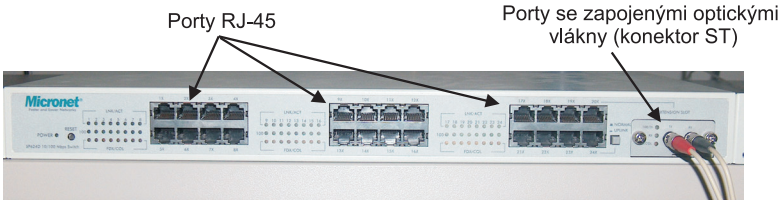
Poznámka: *Pro malé sítě, např. v jedné místnosti se strukturovanou kabeláží se nevyplatí zřizovat HUB, tam stačí switch propojený s počítači.*

Switche

Dalším důležitým prvkem praktického provedení sítě jsou aktivní prvky. U hvězdicové topologie jsou to především switche. Při jejich volbě nás zajímají tyto vlastnosti:

Počet portů

Kolik kabelů je možné připojit, nejmenší hodnota bývá 5, maximální počet 24. Vždy volíme určitou rezervu, ale pokud se zaplní všechny zdířky, nedojde k žádné tragédii, protože je možné připojit další switch.



Obrázek 1.37: *Přední strana switche*

Typ portů

- Vlastně definuje typy kabelů, které k prvku připojíme. Běžně to jsou RJ-45 pro kroucenou dvojlinku. Ty mohou být doplněny:
- BNC konektorem, který se používal hlavně u HUBů s rychlostí 10 Mb/s – bylo tak možné propojit segment koaxiálního kabelu s hvězdicovou strukturou kroucené dvojlinky. Osazení BNC konektorem bylo časté při postupném přechodu ze sběrnicové topologie založené na koaxiálním kabelu na topologii hvězdicovou (s kroucenou dvojlinkou). Dnes toto řešení již většinou nepotřebujeme.
- Konektorem (a na něj navazujícím převodníkem) pro připojení optického kabelu. Tím můžeme propojit optický kabel se zbytkem sítě, většinou s hvězdicovou topologií (kroucenou dvojlinkou).

Když budeme spojovat dva switche, musíme k tomu použít křížené zapojení dvojlinky (viz kapitola *Kroucená dvojlinka*). U starších HUBů a switchů jsme skutečně překřížené kabely museli používat. Novější switche mají jedním portem RJ-45 označen *Uplink*. Ten slouží k propojování koncentrátorů. V uplinkové zásuvce je již překřížení vodičů provedeno – pro propojování koncentrátorů tak stačí obyčejný patch kabel. Zdířka *Uplink* bývá zpravidla krajní (první nebo poslední) a navíc se její křížení zapíná přepínačem (můžeme ji použít k připojení PC v normálním zapojení, nebo k propojení koncentrátorů v kříženém – Uplink zapojení). Konkrétní ovládání uplinku si musíme najít v dokumentaci. Nové switche mají automatickou detekci překřížení označovanou jako *AutoMDI*. Detekce je aktivní zpravidla na všech portech, takže Uplink port vytvoříme z libovolné zdířky (automatika sama rozezná, zda protějškem je další switch nebo PC a křížený kabel není nutné používat).

Rychlost

Může být 10 Mb/s, 100 Mb/s, 10/100 Mb/s a nejrychlejší GB/s. Při volbě rychlosti musíme zohlednit použité síťové karty. Máme-li v síti různé síťové karty: pomalé 10 Mb/s, rychlé 100 Mb/s a nejrychlejší 1000 MB/s, mohou nastat varianty, které ukazuje tabulka (ano = spolupracují, ne = nespolupracují):

Tabulka 1.18: Spolupráce síťových prvků

Rychlost koncentrátoru	NIC 10 Mb/s	NIC 100 Mb/s	NIC 10/100 Mb/s	NIC 1000 Mb/s	NIC 10/100/1000 Mb/s
10 Mb/s	ano	ne	ano	ne	ano
100 Mb/s	ne	ano	ano	ne	ano
10/100 Mb/s	ano	ano	ano	ne	ano
1000 Mb/s	ne	ne	ne	ano	ano
10/100/1000 Mb/s	ano	ano	ano	ano	ano

Funkce

- **Huby** jsou „prosté“ **rozbočovače**, které pouze opakují signál a šíří jej do všech připojených kabelů, dnes pouze dožívají ve starých kabelážích.

- **Switche (přepínače)** jsme si již popsali, pouze shrneme: čtou procházející pakety a propouštějí je pouze do té větve, kde se nachází adresa určení. Pokud si uvědomíme, že u hvězdicové topologie je samostatnou větví vždy jeden kabel vedoucí k PC, pochopíme v čem spočívá přepínání. Switch vlastně propouští pakety pouze mezi vysílající a přijímající stanicí – přepíná pakety mezi dvěma porty (zdířkami). Současně pak může probíhat komunikace mezi několika dvojicemi portů. U přístupové metody CSMA/CD (typické pro Ethernet) je tak možné minimalizovat konflikty a podstatně zrychlit přenos dat. Běžnou vlastností switchů je podpora plně duplexního provozu. Dnes jde o standardní řešení ve všech kabelážích.

Provedení

Switche se vyrábějí ve dvou provedeních:

- **Desktop** – určené na položení na stůl, poličku, vhodné pro nestrukturovanou kabeláž.
- **Rack** – pro zamontování do rozvaděčových skříní strukturované kabeláže.

Světelné indikátory

Na přední straně koncentrátoru najdeme pro každou zdířku sadu světelných diod. Ty indikují činnost portu. Zpravidla ukazuje jedna světelná dioda připojení zdířky k síťové kartě. Většinou můžeme připojit více typů karet a pak je indikace doplněna ještě barvou, např.:

- Zelená indikuje úspěšně připojenou kartu rychlosti GB Ethernetu
- Žlutá informuje o připojené kartě 100 Mb/s
- Podsvětlení upozorňuje na kartu 10 Mb/s

Na switchi najdeme ještě kontrolku oznamující připojení k elektrické síti, případně další světelné diody jejichž význam se liší podle výrobce a typu switche. Často to je kontrolka (označená např. *Collision*), která svítí při kolizích v síti (tj. současném vysílání více stanic – viz CSMA/CD), dále zde bývá kontrolka *Duplex* upozorňující na duplexní provoz.

Tip: Pokud LED dioda nesvítí, přestože je do konektoru připojený kabel, musíme hledat závadu v kabeláži nebo síťové kartě.

Bezdrátové sítě LAN (Wireless LAN), WiFi (Wireless Fidelity)

Dalším dosud nepopsaným přenosovým médiem jsou bezdrátové sítě. Signál se přenáší elektromagnetickým vlněním, které nahrazuje metalické kabely. Elektromagnetické vlny se liší vlnovou délkou (a frekvencí) a jsou široce užívaným přenosovým médiem (např. pro televizní, rozhlasové, telekomunikační signály). Chceme-li od sebe oddělit jednotlivé přenosové linky, musíme pro každou z nich použít jinou frekvenci. Bohužel volných frekvencí je velmi málo, a tak na bezdrátové sítě zbyla nelicencovaná frekvence 2,4 GHz a frekvence 5 GHz. V pásmu 2,4 GHz můžeme sítě provozovat bez obav (jde o volně použitelné pásmo), ale toto pásmo používají také jiné technologie (mikrovlnné trouby, jiné WiFi sítě, Bluetooth, některé bezdrátové telefony či počítačové periferie), což způsobuje rušení přenosu. Provoz v pásmu 5 GHz je regulován pravidly Českého telekomunikačního úřadu (ČTÚ).

V úvodu kapitoly ještě zkonstatujeme to, co bude dále vysvětlováno: Výhodou bezdrátových sítí je to, že k provozu není potřeba kabeláž. Řešení má přirozeně také mnoho nevýhod: bezdrátové prvky jsou stále ještě mírně dražší než tomu je u sítí „klasických“, nedaří se dosáhnout vyšších přenosových rychlostí a zajištění bezpečnosti dat je také podstatně náročnější.

Standard

Vývoj bezdrátových sítí probíhal podobně jako u sítí kabelových. Nejdříve živelně, posléze bylo nutné přijmout normu, která zajistí vzájemnou spolupráci sítí. Hlavní výrobci bezdrátové technologie založili alianci WECA (Wireless Ethernet Compatibility Alliance – sdružení pro kompatibilitu bezdrátového Ethernetu), která stanovila požadavky na zařízení a zajistila tak vzájemnou kompatibilitu. Při splnění podmínek obdrží výrobek certifikát Wi-Fi, který potvrzuje kompatibilitu s výrobky ostatních výrobců. Samotná wireless norma byla odvozena z Ethernetu, proto s ním má některé podobné znaky – přístupovou metodu CSMA/CD a obdobné složení paketu. Pro bezdrátové sítě LAN existuje několik standardů, jejichž základní vlastnosti vidíte v tabulce. Standard 801.11g je zpětně kompatibilní se starším a pomalejším 802.11b (mohou spolupracovat, samozřejmě na nižší rychlosti). Ze standardu 802.11g byla odvozena norma 802.11i, používající bezpečnější autentizační a šifrovací algoritmus.

Tabulka 1.19: Základní vlastnosti bezdrátových standardů

	802.11a	**802.11b**	**802 11g**
Rychlost přenosu [Mb/s]	54	11	54
Frekvence [GHz]	5	2,4	2,4
Dosah [m]	viz poznámka	25 až 100	25 až 100

Poznámka: *ČTÚ definoval pravidla pro použití normy 802.11a. Existují tři varianty lišící se (mimo jiné) také povoleným výkonem vysílačů. Vzdálenost, na kterou mohou komunikovat zařízení normy 802.11a, se pak logicky liší. Maximum může být okolo 15 km.*

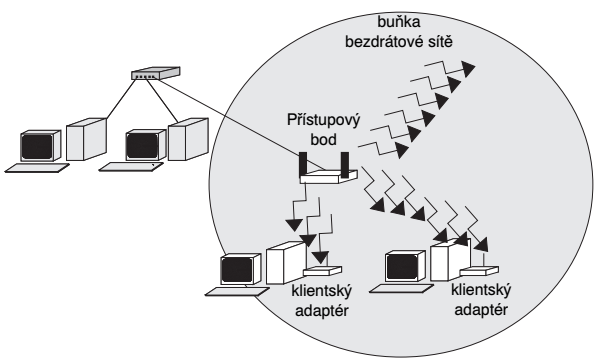
Provedení prvků

Bezdrátové prvky spolu mohou komunikovat dvěma způsoby:

• **ad hoc**, kdy se jedná vlastně o přímé propojení několika počítačů – od dvou do pěti. Každý počítač komunikuje s jiným na stejné úrovni, jsou si rovni (organizace je podobná síti peer to peer). Podstatnou výhodou je rychlá instalace a velmi nízká cena (kromě klientských síťových adaptérů nepotřebujeme žádný další hardware). Umožňuje sdílení souborů a Internetu, tisk přes síť a ostatní věci, které jsou běžné u klasických sítí LAN. Nevýhodou je fakt, že všechna připojená zařízení musí být v dosahu – každý musí vidět každého. Dalším nedostatkem je to, že spojení vzniká až nebezpečně snadno a je obtížné je zabezpečit (spojit se s námi může i ten, o koho nestojíme).

• **infrastrukturní mód** založený na přístupovém bodu – Access Pointu (AP). Ten pracuje jako prostředník (server), přes nějž proudí všechny datové toky mezi klienty sítě (organizace je podobná síti klient/server). Jeho použití má především výhodu v možnosti filtrovat či kontrolovat provoz, včetně zpřístupnění sítě různým klientům. To zaručuje eliminaci náhodných pokusů o sestavení *ad hoc* spojení, veškerý tok musí směřovat na AP, což umožňuje síť ochránit.

Přístupový bod není rozhodně nutný, pokud provádíme bezdrátové spojení příležitostně, mezi několika zařízeními. Budujete-li však malou domácí síť s více účastníky, či hodláte sdílet třeba Internet v domácnosti či malé kanceláři, bez přístupového bodu se většinou neobejdete (také kvůli podstatně vyššímu zabezpečení sítě).

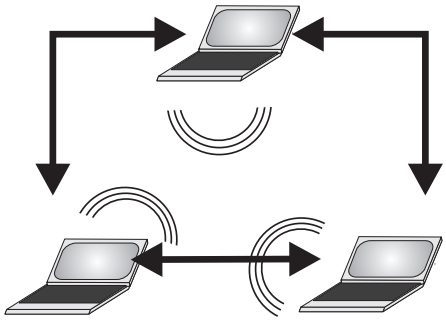


Obrázek 1.38: *Propojení přes Access Point*

Přístupový bod – AP

Je základem bezdrátové sítě. Zprostředkovává spojení mezi bezdrátovými koncovými body a serverem, většinou umístěným v metalické síti LAN. AP tedy obsahuje radiovou část – vysílač/přijímač a část kabelovou – zdířky RJ-45 pro připojení kroucené dvojlinky.

V podstatě jsou AP huby, z nichž se rozvádí signál. Vlastní provedení se liší u jednotlivých výrobců, do hubů mohou být integrovány funkce mostu nebo routeru (nejčastěji pro sdílené připojení Internetu). Mnoho výrobců nabízí napájení AP bodu pomocí kroucené dvojlinky, jíž je bod připojen k pevné síti. K přístupovému bodu (na obtížně dostupném místě) se tak nemusí táhnout dvě vedení.



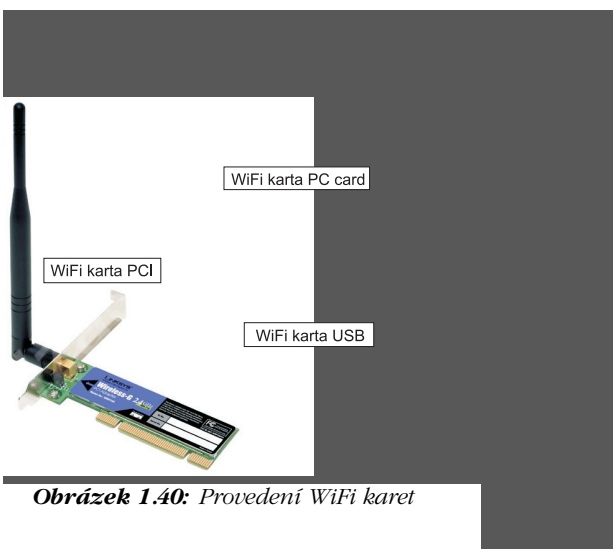
Obrázek 1.39: *Propojení ad hoc*

Přístupový bod a jeho protějšky – klientské adaptéry pracují pouze tehdy, pokud mezi nimi není žádná překážka – mezi AP a počítači umístěnými v bezdrátové síti musí být přímá viditelnost. Proto najdeme přístupové body v nejvyšších částech místností. Při jejich umístění musíme brát do úvahy možné zdroje rušení rádiového signálu, kovové konstrukce (i ve zdi), elektrická rušení (v pásmu 2,4 GHz pracují např. mikrovlnné trouby, bezšňůrové telefony, bezdrátové reproduktory).

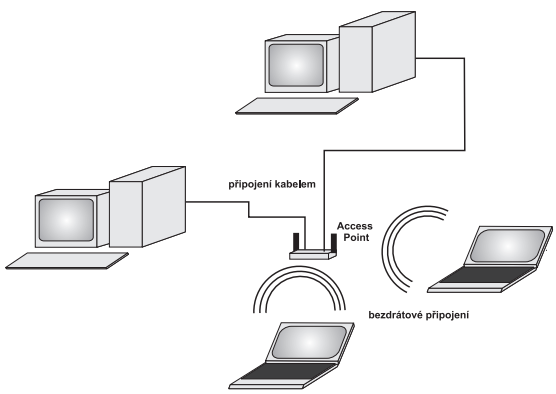
Pokud je potřeba propojit bezdrátové sítě mezi sebou, je možné použít Wireless Bridge (WB) – přístupové body s funkcí mostů, pro filtrování paketů mezi sítěmi.

Klientský adaptér

Jde o jednotku, jíž je „připojeno" PC k přístupovému bodu. V podstatě to tedy je síťová karta (s anténkou). Její provedení bývá pro sloty PCI či USB. Do notebooků lze použít síťovou wireless kartu normy PC Card, ale mnoho notebooků má bezdrátové síťové rozhraní již integrováno (což dále zjednodušuje a zlevňuje budování bezdrátové sítě). Druhým krokem instalace je načtení ovladačů, které je téměř totožné s instalací síťové karty.



Obrázek 1.40: *Provedení WiFi karet*



Obrázek 1.41: *Příklad sítě WiFi*

Provozní vlastnosti

Rychlost

Je ve srovnání s metalickými sítěmi podstatně nižší. V tabulce, popisující základní normy, jsou uvedeny maximální teoreticky dosažitelné rychlosti. Ty jsou ve skutečnosti těžko dosažitelné, protože:

- V případě horší dostupnosti signálu mezi rádiovými stanicemi dojde k přeskoku na nižší přenosovou rychlost. V praxi to znamená, že při větší vzdálenosti (třeba přes 20 m) či při zastínění (stačí kvalitní kovová zárubeň) okamžitě rychlost v klesá, a to dosti rapidně, třeba o polovinu či čtvrtinu.
- Pokud je skupina příjemců připojena na stejný přístupový bod a nacházejí se tak fyzicky na jednom síťovém segmentu (což je typický případ), musejí se o kapacitu linky podělit. (Stejně jako u metalické sítě propojené rozbočovačem – hubem). Dochází tak ke kolizím (znak CSMA/CD). Maximálních rychlostí lze tak dosahovat pouze při bezprostředním přiblížení bezdrátových síťových karet a při komunikaci „jeden na jednoho"!
- Dalším činitelem snižujícím reálnou rychlost je nutná režie protokolů vyšších vrstev. Jednoduše řečeno, když posíláte dopisy, i obálka něco váží. Skutečná šíře pásma, určená pro čistá data, tak opět povážlivě klesá.

Počítejme v praxi s tím, že za velmi dobrých podmínek se maximální šířka pásma pro užitečný datový náklad pohybuje někde kolem poloviny nominálních hodnot, tedy asi 5 Mb/s u „béčka" a 25 Mb/s u „géčka".

Bezpečnost

Oproti metalickým sítím je bezpečnost hůře zajistitelná. Základním nebezpečím při provozu je to, že se rádiový signál šíří do všech stran a náš provoz může kdokoliv odposlouchávat, či se do naší bezdrátové sítě zapojit. Proto je tato problematika velmi důležitá a při praktické práci ji nesmíme zanedbávat. Bezpečnostní opatření jsou v zásadě dvě:

- Autentizace, kdy se kontroluje oprávněnost přiřazení nové stanice do bezdrátové sítě (aby se do sítě nevetřel „cizinec").
- Kódování, jímž jsou přenášená data šifrována (aby se nedala vyluštit ani po jejich zachycení).

K dispozici je několik ochranných metod, které se postupně zdokonalují a zapracovávají do standardů WiFi. Zabudované bezpečnostní metody jsou dalším důležitým kritériem posuzování kvality hardwaru WiFi.

- **SSID:** *(Service Set ID)* – je názvem Access Pointu, pod nímž jej uvidí všichni klienti, kteří se dostanou do jeho dosahu. SSID je tak logickým identifikátorem určité bezdrátové podsítě. Může být nastaven manuálně na stanici, nebo informaci o SSID přístupový bod pravidelně vysílá, či může být vysílání SSID vypnuto a klient se na SSID sám dotáže (probe).
- **WEP:** Byl volitelně integrován do všech Wi-Fi zařízení už od protokolu 802.11b. Přesto je překvapivé, že jej ani dnes řada sítí nepoužívá. Jeho princip spočívá v tom, že se odesílaná zpráva na vysílači zašifruje nějakým klíčem, a přijímač ji stejným klíčem rozšifruje. Tento klíč musí být znám jak vysílající stanici, tak přijímací (ve standardu se jedná o 40bitový klíč). Pracuje tedy na symetrickém principu, kdy se pro šifrování i dešifrování používá stejný klíč. WEP však neověřuje uživatele samotného, ale pouze fyzickou adresu (MAC) jeho síťové karty. Později byl tento klíč obohacen o 24bitový, pravidelně se měnící pseudonáhodný sled znaků, který se na straně vysílače přidá k tajnému klíči (tím vzniká 64bitová „šifra", se kterou se pak zašifruje zpráva) a také se pošle přijímači (posílá se nezakódovaný! – to patří mezi jednu z hlavních nevýhod WEPu). Přijímač ho přidá ke svému tajnému klíči a tento složený klíč pak použije pro dešifrování. Dalším nedostatkem WEP je fakt, že klíč (přesněji námi zvolená fráze) zůstává po zadání neměnný (do doby, než ho sami změníme – což musíme udělat na obou stranách zabezpečeného kanálu). Dlouhodobé používání stejného klíče znamená smrt pro každou šifru, WEP nevyjímaje. Pokud si zvyknete jednou za dva až tři dny klíč k šifře WEP měnit, nesmírně tím zvýšíte své šance na ochranu síťového přenosu. Kdyby se útočníkovi přece jen podařilo klíč odhalit, bude mu po několika hodinách či málo dnech k ničemu. Největší bolestí WEP je skutečnost, že klíče není možné automaticky obměňovat během komunikace. Uživatelé to

musí provádět ručním nastavením, a to na obou stranách sítě. Většina výrobců implementuje do hardwarových prvků (AP, karet) vyšší úrovně zabezpečení ve formě 128bitového šifrování (sdílený klíč má délku 104 bitů, inicializační vektor poté 24 bitů). Přestože má WEP mnoho nedostatků, poskytuje alespoň minimální úroveň zabezpečení a určitě bychom ho měli používat (nemáme-li k dispozici lepší metody).

- **802.1x:** Velmi brzo si výrobci a i samotní uživatelé začali uvědomovat veliké nedostatky, které protokol WEP přinášel. Začalo se tedy pracovat na nové normě, jež měla umožnit lepší úroveň přihlašování uživatelů na základě šifrování a distribuce klíčů. Vznikl tedy protokol **EAP** (Extensible Authentication Protocol), jenž blokuje přístup k síti neoprávněným uživatelům. Samotné ověřování pak provádí protokol **RADIUS**, který identifikuje uživatele podle seznamu povolených klientů a těm také povolí přístup k samotné síti. Podstatnou výhodou je také dynamičnost šifrovacích klíčů TKIP (Temporal Key Integrity Protocol), jež jsou známy vždy jen stanici, ke které se uživatel připojuje a po odhlášení se mažou. Avšak ani toto opatření nezabránilo v průniku, i při této metodě ochrany existují způsoby průlomu hesla.
- **802.11i:** Pro získání co nejvyšší bezpečnosti byla časem zavedena nová robustnější norma. Jejím základem bylo navržení protokolu **WPA** (Wi-Fi Protected Access), mezi jehož hlavní znaky patří: Průběžná a automatická výměna dynamicky vytvářených klíčů pro šifrovací procedury (což řeší zásadní slabinu technologie WEP), potenciálnímu útočníkovi tak chybí to nejdůležitější – dostatečné množství dat šifrovaných stejným způsobem. Druhým vylepšením, je zvětšení délky klíče pro šifrování na hodnotu až 256 bitů. Dalším vylepšením je **MAC filter**, umožňující povolit přístup do sítě pouze vybraným uživatelům na základě vypsání fyzické adresy jejich Wi-Fi zařízení. Ta je pro každé zařízení zcela jedinečná, a tudíž umožní přesně vymezit okruh povolených uživatelů. (Tato funkce není žádnou novinkou, v některých přístupových bodech byla obsažena ještě před zavedením standardu 802.11i).

Konfigurace bezdrátové sítě

Nastavení bezdrátové sítě si ukážeme na příkladu sítě s přístupovým bodem (AP), tedy sítě pracující v infrastrukturním módu. Konfigurace probíhá ve dvou krocích:

- nejdříve musíme zadat parametry přístupového bodu
- pak zapsat nastavení do jednotlivých stanic

Konfigurace přístupového bodu (Access Pointu)

Přístupové body vyrábí mnoho výrobců, a tak je přirozené, že se jejich konfigurační obrazovky odlišují. Přesto se zde nastavují stejné veličiny, a tak náš příklad určitě pomůže při pochopení postupu.

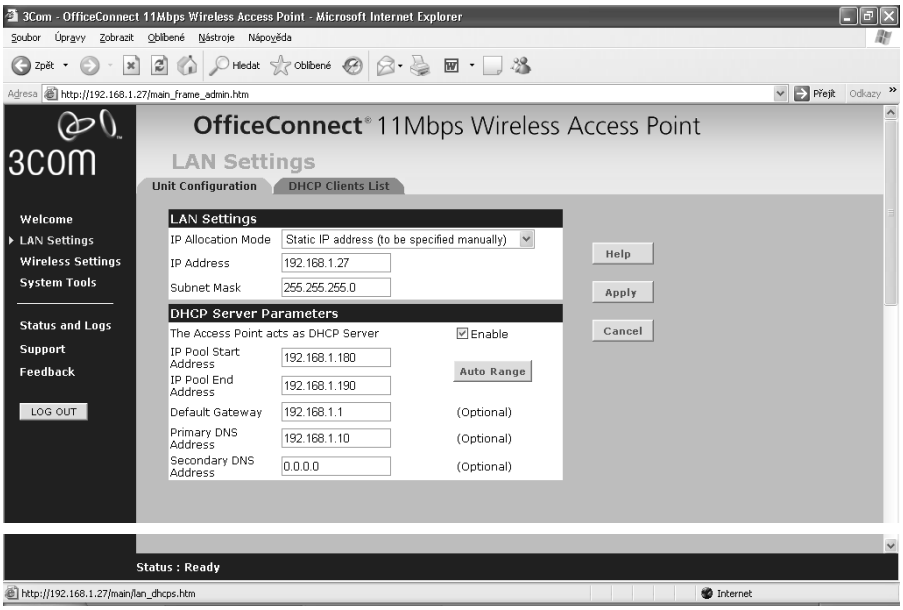
Každý Acces Point má vstupní porty RJ-45 pro připojení do metalické sítě (spojí se tak bezdrátová síť s metalickou). Access Point připojíme k stávající metalické síti (pokud ji provozovat nebudeme – počítače budeme spojovat pouze prostřednictvím WiFi sítě, spojíme Access Point kroucenou dvojlinkou s počítačem). Vstup do konfiguračních obrazovek se totiž provádí prostřednictvím internetového prohlížeče. Po zadání IP adresy Access Pointu, vyplnění přihlašovacího jména a hesla, otevřeme konfigurační obrazovky (adresu, jméno a heslo najdeme v manuálu a můžeme je později změnit).

Obrazovka AP má v levé části menu a v pravé jednotlivé obrazovky, organizované do záložek.

První konfigurační zastávkou je volba ***LAN Settings***. Na kartě *Unit Configuration* zadáváme IP adresy, nutné k činnosti AP (IP adresaci je věnována kapitola *Adresace v sítích TCP/IP*).

- V horní části obrazovky – *LAN Settings* zapisujeme vše, co souvisí s adresou samotného AP, IP adresu a její masku.
- Dolní část – *DHCP Server Parameters* použijeme tehdy, když budeme chtít, aby AP pracoval také jako DHCP server (ten automaticky přiděluje IP adresy počítačům v síti). Z bezpečnostního hlediska to není nejlepší řešení (případnému vetřelci sami přidělíme IP adresu), ale pokud se pro DHCP rozhodneme, musíme zaškrtnout políčko *Enable* a dále nastavit:
  - *IP Pool Start Address* počáteční adresa rozsahu, z něhož budou IP adresy přidělovány

- *IP Pool End Address* koncová adresa rozsahu, z něhož budou IP adresy přidělovány
- *Default Gateway* adresa brány, která bude počítačům DHCP serverem přidělovaná
- *Primary DNS Address* adresa primárního DNS serveru, která bude počítačům DHCP serverem přidělovaná. Pokud budeme chtít, aby DHCP server přiděloval i záložní adresu DNS, vyplníme řádek *Secondary DNS Address*.

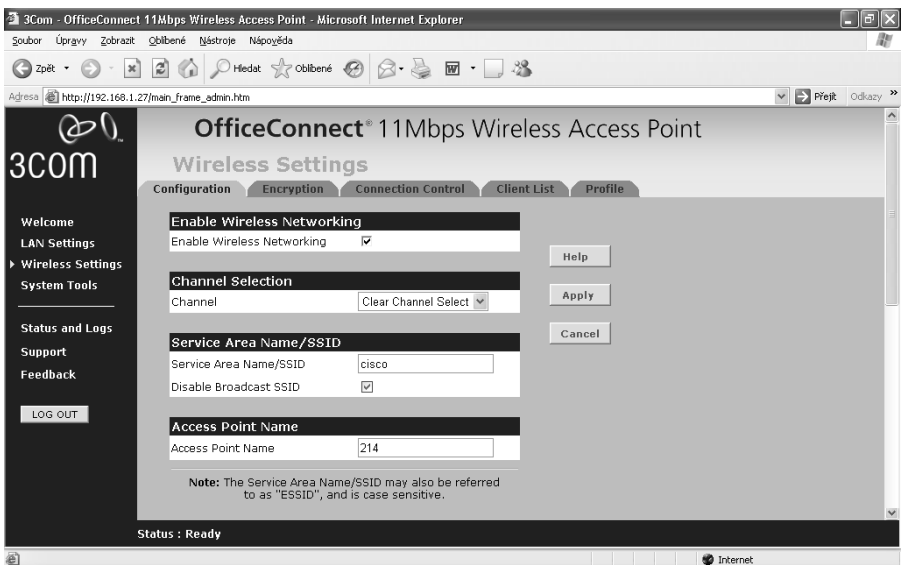


Obrázek 1.42: *Nastavení LAN*

Seznam momentálně přidělených adres získáme na kartě *DHCP Clients List*.

Následujícím konfiguračním bodem je volba *Wireless Settings*, při jejím popisu se omezím pouze na nejdůležitější údaje.

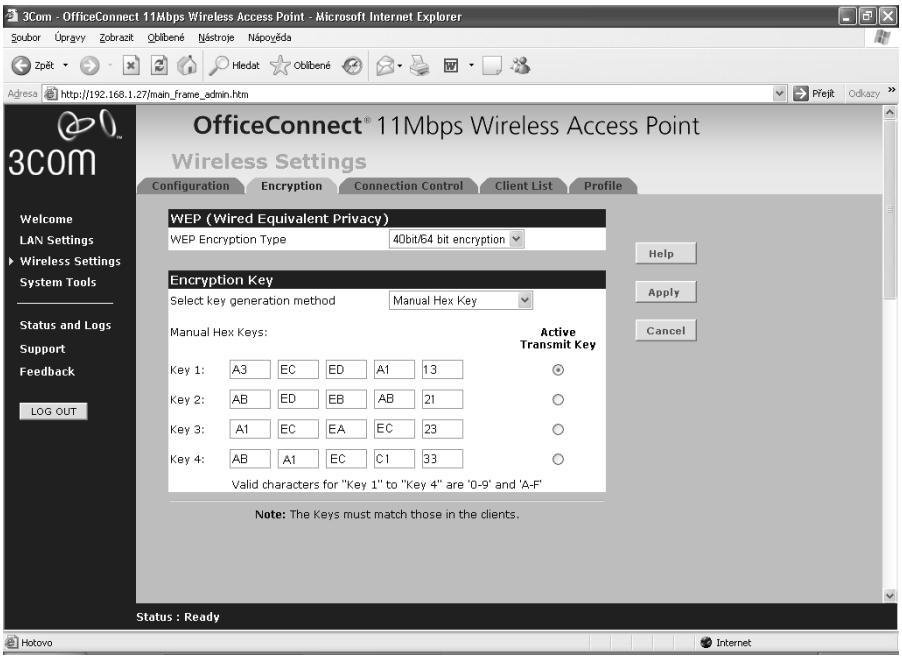
- Opět začneme na první kartě – *Configuration*. Zde zaškrtnutím *Enable Wireless Networking* povolíme bezdrátový přenos. Dále je důležitá volba *Service Area Name/SSID* (viz předešlý odstavec *Bezpečnost*). Zatržením *Disable Bro-*



Obrázek 1.43: *Nastavení WiFi – karta Configuration*

adcast SSID zamezíme vysílání identifikátoru AP a zvýšíme bezpečnost sítě. Také sem zapíšeme jméno AP (v našem příkladu jím je *cisco*).

- Druhá karta *Encryption* se týká nejdůležitějšího bezpečnostního nastavení – definice klíče, jímž se kódují přenášená data. Náš AP používá pro kódování metodu WEP (viz předešlá kapitola). Tvar a parametry klíče WEP určujeme právě v této volbě.
  - V horní řádce *WEP Encryption Type* zadáváme délku klíče. K dispozici bývají dvě možnosti: kratší (a méně bezpečný) 64bitový klíč a delší klíč 128bitový. My máme nastaven klíč 64bitový.
  - V rámečku *Encryption Key* zapíšeme čtyři hodnoty klíče a tu momentálně platnou vybereme ve sloupečku. Máme tedy předdefinovány čtyři hodnoty, které můžeme měnit (stejný klíč používaný delší dobu je dalším bezpečnostním rizikem). Poznámka dole: *The keys must match those in the clients* upozorňuje na to, že stejná hodnota klíče jako na Access Pointu musí být i na klientských stanicích.

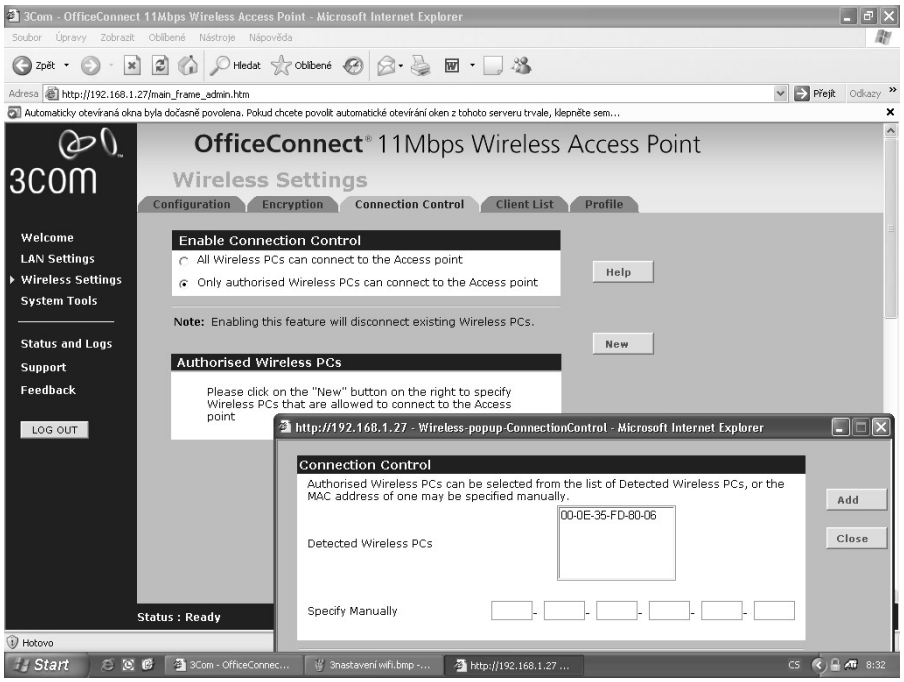


Obrázek 1.44: *Nastavení WiFi – karta Encryption*

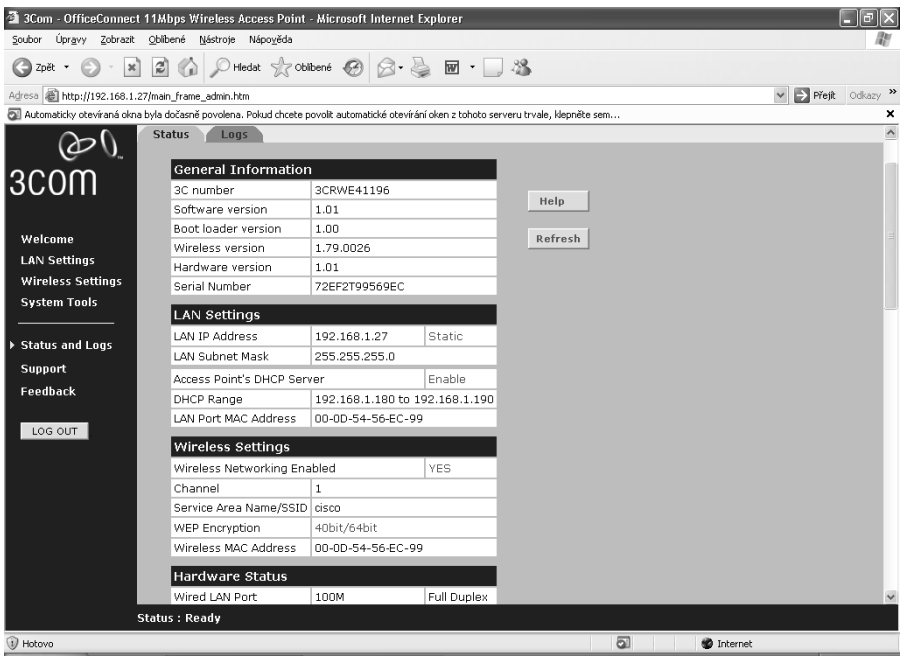
- Karta *Connection Control* slouží k dalšímu zvýšení bezpečnosti bezdrátové sítě. Stanovujeme zde zda do sítě budou moci vstupovat libovolné stanice (*All Wireless PCs can connect to the Access Point*), nebo bude síť přístupná pouze autorizovaným počítačům (*Only authorised Wireless PCs can connect to the Access Point*). V případě druhé volby opět zvýšíme bezpečnost sítě. Autorizace spočívá v tom, že vytvoříme seznam MAC adres síťových karet, jimž je dovoleno s AP spolupracovat. Zatržením druhé možnosti (autorizace) se zpřístupní okno *Connection control*, v němž budeme MAC adresy zadávat. K dispozici je okénko *Detected Wireless PCs,* kde vidíme MAC adresy momentálně připojených PC. Tlačítkem *ADD* pak můžeme MAC adresy přidat do seznamu povolených MAC adres. Případně můžeme MAC adresu vložit ručně *Specify Manually.*

Posledním zastavením je volba *Status and Logs.* Zde získáme momentální provozní informace. K dispozici jsou dvě karty:

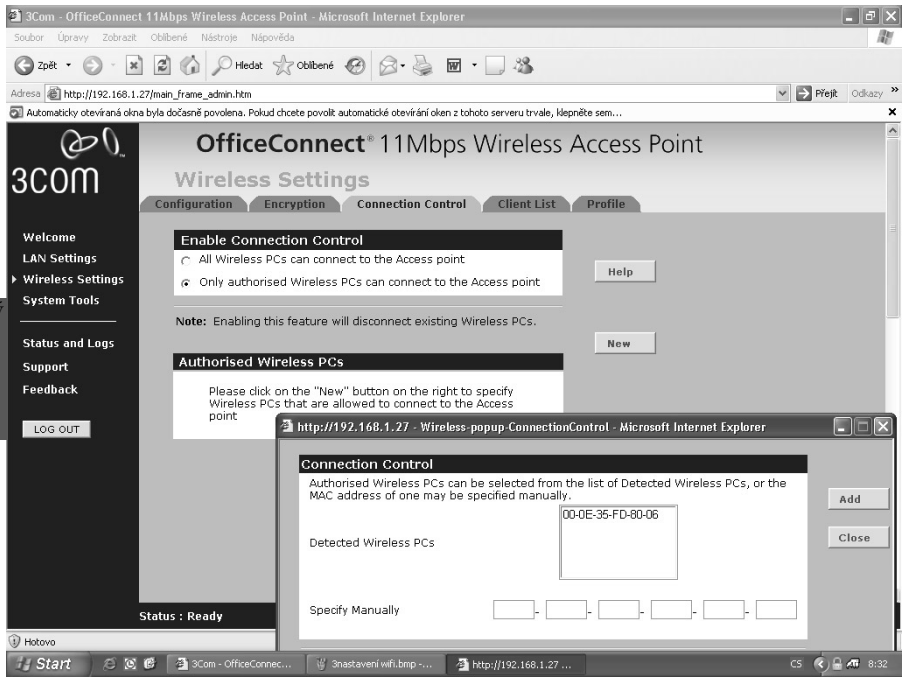
- *Status* ukazuje momentální nastavení Access Pointu (jeho IP adresu, MAC adresy a informace o DHCP serveru).
- *Logs* zobrazuje logovací výpisy, v nichž jsou informace o činnosti apod. Najdeme zde hlavně kdo a kdy se k AP připojil.



Obrázek 1.45: *Nastavení WiFi – karta Connection Control*



Obrázek 1.46: *Nastavení WiFi – karta Status*



Obrázek 1.47: *Nastavení WiFi – karta Logs*

špatný obrázek

Závěrem si stručně shrneme několik zásad, které pomohou udržovat síť maximálně bezpečnou a které uplatníme při nastavování AP:

1. Zakažte SSID Broadcast – vysílání identifikačního jména AP všem opravdu bezpečnost nezvýší.
2. Nastavte vlastní SSID, nepoužívejte přednastavený firemní tvar. Ten je známý a dá se odhadnout.
3. Nepovolujte DHCP a adresy přidělujte ručně – vetřelec tak automaticky neobdrží adresu z vaší sítě.
4. Používáte-li WEP zapněte 128bitový klíč a pravidelně měňte klíče WEP.
5. V Access Pointu zaveďte tabulku povolených MAC adres – tj. adres hardwarových zařízení, která se mohou připojit.
6. Pokud je to možné, nastavte také tabulku povolených IP adres.
7. Pravidelně kontroluje síť i logy z AP.
8. Omezte výkon tak, aby signál vysílačů ve vaší síti zbytečně nepřesahoval půdu vaší firmy.
9. Znemožněte fyzický přístup uživatelů k AP.

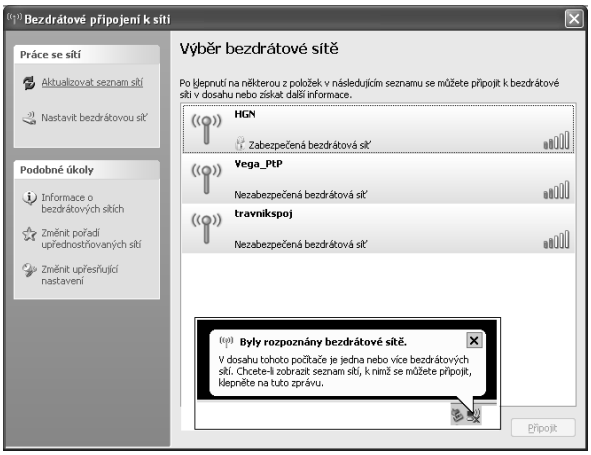
Konfigurace klientské stanice

Když je přístupový bod (AP) nastaven, musíme ještě nastavit klientské stanice. Síťový software k WiFi připojení je součástí Windows XP, jeho vlastnosti byly podstatně vylepšeny Service Packem 2 a právě konfiguraci Windows XP SP2 si ukážeme.

Prvním krokem je připojení bezdrátové síťové karty. Víme, že karta může být ve formě klasické rozšiřující karty (nejčastěji PCI), USB adaptéru nebo karty PC Card. V principu je instalace vždy stejná, jde o nahrání správných ovladačů prostřednictvím *Průvodce přidáním nového hardwaru*. Tato činnost je popsána v kapitole *Síťové karty*.

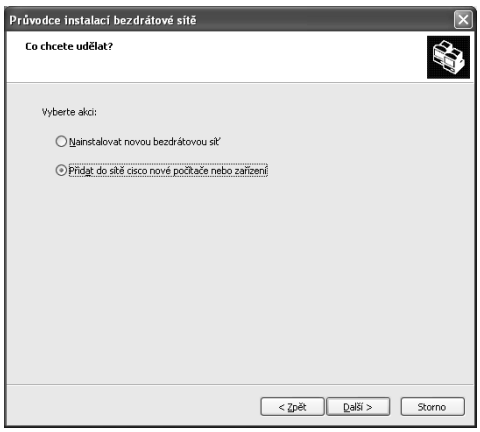
Po správné instalaci adaptéru WiFi se v pravém dolním rohu obrazovky objeví informace o tom, že adaptér našel bezdrátové sítě. Pokud na informační bublinu klepneme levým tlačítkem myši, detekované bezdrátové sítě spatříme.

V obrazovce *Bezdrátové připojení k síti* klepneme na možnost *Změnit upřesňující nastavení* a spustíme tak *Průvodce instalací bezdrátové sítě*. Ten nám pomůže vše nastavit. Při konfiguraci bezdrátové sítě musíme nejdříve připravit Access Point a pak až stanice. Máme-li AP aktivní, měla by se vždy nějaká síť najít. Pokud tomu tak nebude, můžeme *Průvodce* spustíte také z *Ovládacích panelů* (*Start / Ovládací panely / Bezdrátová síť*). A nyní již k samotnému *Průvodci instalací bezdrátové sítě*.

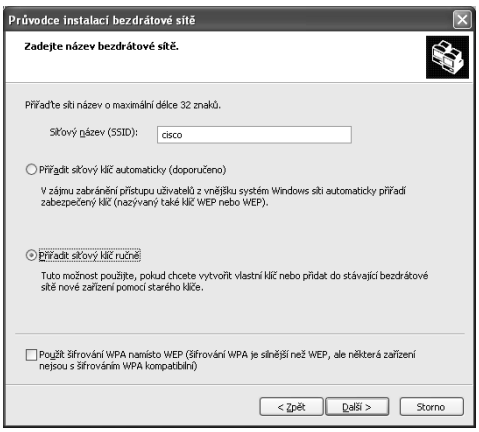


Obrázek 1.48: *Detekce sítě a nalezené sítě.*

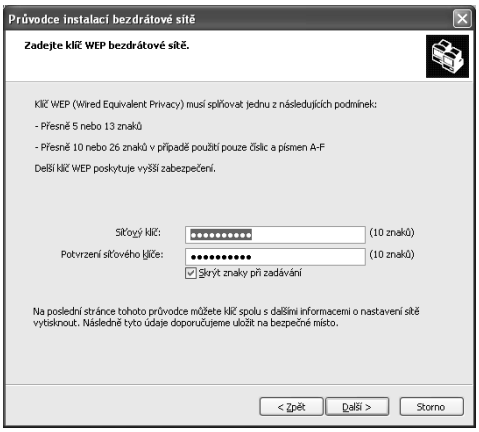
- Jeho první obrazovka je tradičně uvítací.
- Ve druhé obrazovce jsme dotázáni na to, zda budeme připojovat stanici do nové sítě, nebo sítě detekované. My si ukážeme instalaci nové sítě (*Nainstalovat novou bezdrátovou síť*).
- Třetí a čtvrtá obrazovka jsou nejdůležitější. Ve třetí vkládáme informace o Access Pointu:
  - *Síťový název (SSID)* – je údajem zadaným již při konfiguraci AP (*Service Area Name/SSID).* Stejné přístupové jméno musíme zapsat i sem.
  - Poté zadáme, zda budeme používat šifrování WPA nebo WEP (volba dole *Použít šifrování WPA místo WEP*). Problematika již byla rozebrána v kapitole *Bezpečnost,* takže jen stručně. Šifrování WPA přinesla norma 802.11i, je kvalitnější než WEP, ale naše volba musí odpovídat možnostem Access Pointu.
  - Síťový klíč, jímž jsou šifrována přenášená data, může být přidělen automaticky, nebo ručně. Opět vybereme nám vyhovující variantu. Rozhodneme-li se pro ruční přidělení klíče (opět jde o bezpečnější metodu), přejdeme do obrazovky č. 4.
  - Ve čtvrté obrazovce zadáme hodnotu klíče.
  - V páté obrazovce nám je nabídnuta možnost uložit nastavení na Flash disk. Uložená data pak můžeme použít při konfiguraci jiných počítačů.



Obrázek 1.49: *Druhá obrazovka Průvodce*



Obrázek 1.50: *Třetí obrazovka Průvodce*



Obrázek 1.51: *Čtvrtá obrazovka Průvodce*

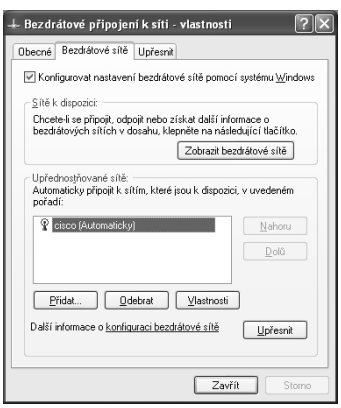
Obrázek 1.52: *Pátá obrazovka Průvodce*

Obrázek 1.53: *Šestá obrazovka Průvodce*

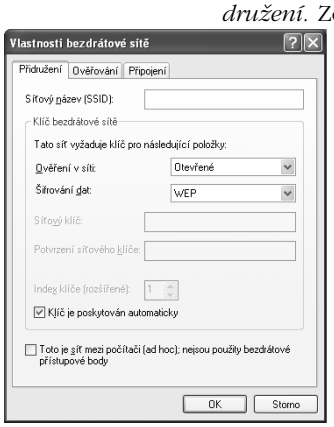
- Poslední, šestá obrazovka nabídne možnost vytištění konfigurace WiFi. O úspěšném připojení k bezdrátové síti (které by po konfiguraci mělo následovat, nás informuje bublina v pravém spodním rohu obrazovky.

Po instalaci bezdrátové síťové karty se ve Windows XP vytvoří síťové připojení patřící bezdrátovému adaptéru. (Ovládací panel *Síťová připojení* zobrazíme např. klepnutím pravého tlačítka myši na ikonu *Místa v síti* a následnou volbou *Vlastnosti*.) Klepneme-li na zástupce bezdrátového připojení pravým tlačítkem myši a v menu vybereme *Vlastnosti*, dostaneme se ještě k dalším nastavením sítě WiFi. Dvě nejdůležitější obrazovky ukazují obrázky:

- Na kartě *Bezdrátové sítě* určíme k jakým sítím se má náš počítač automaticky připojovat.
  - Stiskem tlačítka *Vlastnosti* se dostaneme na kartu *Přidružení*. Zde vložíme údaje potřebné ke vstupu do sítě (šifrovací protokol, klíč atd.). Důležitou volbu najdeme ve spodním řádku okna – *Toto je síť mezi počítači (ad hoc)...* Tady můžeme nastavit spojení ad hoc!



Obrázek 1.54: *Karta Bezdrátové sítě*



Obrázek 1.55: *Karta Přidružení*

Kapitola 2

Základní pojmy síťového softwaru

Kromě síťového hardwaru, jímž jsme se zabývali v předešlé kapitole, je dalším stavebním kamenem sítí software. Tím je hardware oživen a vznikne provozuschopná síť. Trh se softwarem počítačových sítí je ve srovnání s hardwarem podstatně užší. Setkáme se se sítěmi Microsoftu, Novellu a Linuxem. Každému produktu bude věnována zvláštní kapitola. Než se pustíme do detailního popisu jednotlivých síťových systémů, vysvětlíme si některé obecné pojmy, které potřebujeme při práci se síťovým softwarem znát.

Typy síťového softwaru

Základním kritériem, podle něhož rozdělujeme síťový software je použití (či nepoužití) serveru. Z tohoto hlediska rozeznáváme sítě peer-to-peer a client – server.

Síť peer to peer (rovný s rovným)

Tato síť je tvořena jednotlivými síťovým stanicemi (počítači), které si jsou navzájem rovné. Znamená to, že počítače si mezi sebou nabízí své služby. Například mohou být na počítači zpřístupněny určité složky, do nichž je povolen přístup jiným uživatelům, nebo můžeme dovolit tisk na jedné tiskárně více stanicím. Jako vše má takovéto řešení své přednosti a nedostatky:

- **Výhody**: Pro správu sítě nejsou třeba žádné velké znalosti. Jde o řešení levné, není nutné kupovat server ani žádné síťové operační systémy (peer to peer síť je obsažena ve Windows).
- **Nevýhody** Při větším počtu počítačů je velmi obtížné udržet přehled o datech (na kterém počítači je to uloženo?). Data jsou jen málo chráněna proti zneužití. Konfigurace přístupových práv (kdo může co číst) je u peer to peer jednoduchá (a méně bezpečná), navíc se musí aplikovat (a dodržovat) na všech stanicích, což bývá téměř neuskutečnitelné.

Celkově lze říci, že síť peer to peer je vhodná pro propojení několika počítačů v malé firmě. Horní hranice provozuschopnosti sítě je někde u 10 stanic.

Síť klient – server

Filozofie tohoto řešení je jednoduchá. Soustředit vše (data, služby, údaje o uživatelích…) do jednoho bodu v síti. Ten důkladně zabezpečit a odsud nabízet služby všem síťovým stanicím. Počítač kam údaje soustřeďujeme nazýváme server (sluha). Protože musí obsluhovat mnoho požadavků v krátkém čase, je zde ukládáno mnoho dat, je nutné, aby to byl počítač kvalitní a rychlý. Navíc na něm musí být nahrán speciální program – síťový operační systém, který bude organizovat ukládání dat, přidělovat přístupová práva k složkám a souborům, vést evidenci o tom kdo se může k serveru přihlásit a co bude moci na serveru dělat… Celkově lze síť klient – server charakterizovat takto:

- **Výhody:** vysoká bezpečnost dat, přehlednost, snadná konfigurovatelnost.
- **Nevýhody:** spočívají v nákladech na nákup serveru a síťového operačního systému, v nutnosti mít vysoce kvalifikovaného pracovníka, který bude umět obsluhovat síťový operační systém.

Pro většinu sítí je toto řešení nevyhnutelné, a proto je také značná část knihy věnována popisu nejpoužívanějších síťových operačních systémů. Nejrozšířenější síťové operační systémy pracující na serveru jsou pro sítě LAN tři:

- Od firmy **Microsoft** to je Microsoft Windows Server 2003 a jeho předchůdce Microsoft Windows 2000 Server.
- Dalším síťovým systémem je NetWare firmy **Novell**. I ten existuje ve více verzích. Tou poslední je Novell NetWare 6,5, jeho předky byly verze 6 a 5, můžeme se setkat s dožívajícími verzemi 4 (hlavně 4.11).
- Různé distribuce **Linuxu**. (Linuxovým serverům se v poslední době věnuje také firma Novell).

Server

To nejdůležitější a nejdražší v celé síti není žádný počítač, ale data (kvůli nimž síť budujeme). Nicméně je server tím místem, kde jsou data uložena, a proto se na něj podíváme blíže. Serverem může být teoreticky jakýkoliv počítač, na nějž nahrajeme síťový operační systém. Víme však, že server je jádrem počítačové sítě, musí současně obsluhovat mnoho požadavků od síťových stanic, zaručit bezpečnost zde uložených dat a tak na hardware serveru klademe daleko vyšší nároky než na obyčejnou stanici.

Hardwarové požadavky na server

Mikroprocesor

Ten samozřejmě požadujeme vždy co nejlepší. U levných serverů se používají špičkové desktopové procesory (Intel Pentium, AMD Athlon 64). Daleko častější je však použití mikroprocesorů vyvinutých speciálně pro servery – Intel Xeon a AMD Opteron. U serverů určených do velkých sítí se používá multiprocessoring – spolupráce několika mikroprocesorů na jedné základní desce.

Operační paměť

Musí být dostatečně veliká pro soubory síťového operačního systému a ještě musí poskytnout prostor pro další aplikace vyžadované uživateli. Navíc je potřeba místo pro kešování pevných disků. Velikost paměti je tedy závislá na použitém operačním systému, počtu stanic v síti a na programech, které budeme ze serveru spouštět. U menších serverů je její spodní hranice 1 GB, ale často se používají paměti podstatně větší. Většinou se používají operační paměti v provedení *registered* a *ECC*.

Při charakteristikách paměti jsme se setkali s několika novými pojmy, které nemusí každý znát:

- **Kešování (cache)** – server musí velmi často číst data z disku, což je ve srovnání s čtením dat z operační paměti pomalá operace. Proto jsou dříve čtená data stále uchovávána v operační paměti. Pokud přijde požadavek na čtení dat, hledají se nejdříve v rychlé operační paměti a až když tam nejsou nalezena, jsou přečtena z pomalejšího pevného disku. Protože většina uživatelů sítě používá stejný program (uložený na serveru), je pravděpodobnost nalezení dat v operační paměti vysoká – podstatně se tak zrychlí práce serveru.
- **ECC (Error Checking and Correcting)** je samoopravný kód, který dokáže nejen zjistit, ale i opravit jednobitovou (nové systémy i dvoubitovou) chybu v paměti. ECC musí být podporován základní deskou i paměťovým modulem. ECC paměti jsou samozřejmě dražší, proto se používají převážně v serverech.
- **Registered** moduly se liší použitím speciálních vstupně výstupních bufferů, které zvyšují stabilitu a spolehlivost přenosu dat. Také registrované moduly musejí být podporovány chipsetem základní desky a také ony jsou dražší než častěji používané moduly bez bufferů **(unbuffered)**.

Pevné disky

Pevné disky, na něž se ukládají data z celé sítě, jsou další veledůležitou součástkou serverů. Musejí mít dostatečnou kapacitu, která závisí na použitém programu a velikosti sítě. Spodní hranice velikosti disků je okolo 100 GB, většinou se však používají disky podstatně větší. Dalším požadavkem, uplatňovaným u serverů, jsou zvýšené požadavky na bezpečnost uložených dat – z tohoto důvodu se serverové disky sdružují do diskových polí *RAID*.

Dalším typickým znakem serverových disků je rozhraní *SCSI* (*Small Computer System Interface*). Jde o způsob komunikace mezi základní deskou a diskem, který je rychlý a dovoluje připojit 7 nebo 15 SCSI zařízení (např. disků). Další výhodou SCSI je to, že komunikaci mezi jednotlivými SCSI zařízeními obstarává řadič SCSI, bez účasti mikroprocesoru. Řadič bývá instalován na rozšiřující desce zasazené do slotu PCI. Vysoká komunikační rychlost SCSI je vhodná pro disková pole.

U levnějších serverů se také nabízí možnost použití disků SATA. Tato relativně nová technologie přenosu dat mezi pevným diskem a základní deskou je rovněž rychlá a je možné ji použít při sestavování disků do polí. Ve srovnání s SCSI je znatelně levnější.

Disková pole

Jako velké sklady dat se v dražších serverech nepoužívají jednotlivé disky, ale disková pole. Jde o skupinu disků, která se navenek „tváří" jako disk jeden. Server sem posílá požadavky na čtení a zápisy dat a pole si samo organizuje na který disk se data uloží (či odkud se přečtou). Pole mohou být umístěna ve skříni serveru i mimo ni. Účelem diskových polí je především zvýšení bezpečnosti dat. K organizaci dat používají některou z metod *RAID* (*Redundant Array of Inexpensive Disks*). Vlastní problematika RAID je velmi složitá, pro naše účely postačí vysvětlit základní vlastnosti diskových polí. Vyšší bezpečnosti diskových polí je dosaženo díky nadbytečnosti (redundanci) dat. V principu jde o to, že se stejná data zapisují na více disků. Při havárii se pak z nadbytečných dat doplní chybějící údaje. Vyšší bezpečnost je vykoupena snížením použitelného prostoru disku. RAID se dělí do několika skupin, které používají různé úrovně redundance dat. Podstatné znaky metod RAID používaných u serverů PC ukazuje tabulka:

typ	princip	výhody	nevýhody
RAID 0, striping	Data se rozdělují mezi několik disků.	Zvýšení kapacity, snížení přístupové doby při čtecích i zapisovacích operacích.	Nezvyšuje bezpečnost, pokud jeden disk zhavaruje, ztratíme všechna data.
RAID 1, mirroring	Data se současně zapisují na více disků (většinou dva). Jeden disk je úplnou kopií druhého.	Data jsou 100% redundantní. Vysoká bezpečnost, při poruše primárního disku, přebírá jeho funkci sekundární disk. Dochází ke zrychlení čtecích operací díky současnému čtení ze dvou disků.	Kapacita jednoho disku je zrcadlena na disk další. K uložení dat je tak potřebná dvojnásobná kapacita (2 disky).
RAID 5, striping s redundancí	Data jsou rozdělována mezi více disků. „Nadbytečná" paritní data jsou rozprostřena na všechny disky. Zhavarovaný disk je možné vyměnit. Jeho data jsou pak zrekonstruována pomocí paritních redundantních údajů.	Zvýšení výkonu při čtecích operacích. Redundantní data zaberou jen část kapacity disků (není třeba zdvojnásobovat kapacitu disků). Havarovaný disk je možné vyměnit a pole dopočítá a zrekonstruuje chybějící data.	Potřeba minimálně tří disků.

- *RAID 0* – zvýší pouze rychlost sekvenčního čtení a sekvenčního zápisu. Najde proto využití pouze v případech, kdy je třeba rychlého zápisu či čtení velkých bloků dat – například při editaci filmů, fotografií, audio nahrávek atp. Pro běžnou práci se síťovým operačním systémem je jeho použití nevýhodné.
- RAID 1 a 5 – jsou v serverech nejpoužívanější. Nevýhodou RAID 1 je vysoká potřeba diskového prostoru, obsah jednoho disku se zrcadlí na druhý – výsledná kapacita je tedy pouze 50%, ale na vytvoření pole stačí pouze 2 disky. RAID 5 potřebuje minimálně disky 3 (ale může být složeno z více disků), s kapacitou hospodaří podstatně

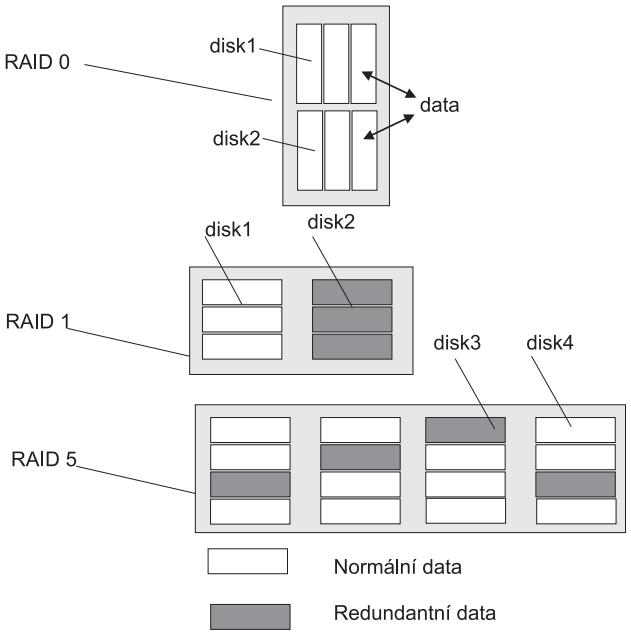
lépe, na redundanci spotřebuje kapacitu jednoho disku, v případě 3 disků přijdeme o 33 % kapacity. Protože na vytvoření RAID 5 potřebujeme více disků, je pole dražší. Z výše uvedených důvodů se RAID 1 používá u levnějších serverů, dražší servery pak mívají instalováno diskové pole RAID 5.

- Je také možné kombinovat RAID 0 se zbylými technologiemi. Pak se takové pole označuje např. RAID 50.

Vytvoření RAID

Rozhraní RAID může být realizováno dvěma způsoby:

- Softwarově, kdy je RAID vytvářen operačním systémem. Metodu RAID umějí výhradně síťové operační systémy.
- Hardwarově, kdy je RAID vytvářen řadičem pevných disků.



Obrázek 2.1: *Princip RAID*

CD-ROM

Tou musí být vybaven každý server, protože síťové operační systémy se dodávají na několika CD discích. Instalace operačního systému bez mechaniky CD-ROM tedy není možná. Je vhodné, aby mechanika splňovala co nejnovější normu, dnes by měla alespoň umět číst disky DVD – odkud se mohou instalovat některé rozsáhlejší varianty síťových operačních systémů.

Někdy může být výhodná také zapisovací mechanika, především zapisovací mechaniky DVD mají slušné kapacity a mohou se použít pro zálohování dat. Ve srovnání s páskovými jednotkami jsou však jejich velikosti stále malé a je potřeba zvážit, zda pro případné zálohování budou použitelné.

Pásková jednotka

Jak již bylo řečeno – nejdražší jsou data. Pásková jednotka se používá pro jejich zálohování. Přestože jsou data chráněna (před havárií serveru) nějakým systémem RAID, je dobré zapsat je ještě na pásku. Páska se pak ukládá odděleně od serveru. Data jsou tak chráněna proti krádeži, požáru serveru nebo celé budovy. Navíc je možné z páskové zálohy data obnovovat – vrátit se k jejich starší verzi.

Síťové operační systémy umějí zapisovat na pásku vybraná data v určitém čase (např. v noci) – tím se eliminuje nízká rychlost pásky. Při pořizování pásky nesmíme zapomenout na její kapacitu – ta musí odpovídat předpokládané velikosti zálohovaných dat.

Ostatní hardwarové prvky

Z předešlého výkladu je jasné, že pro server musíme použít speciální základní desku, která dovolí multiprocessoring a bude mít dostatečnou kapacitu pro operační paměť.

Dnes se do nových serverů standardně vkládají síťové karty o rychlosti 1 GB/s.

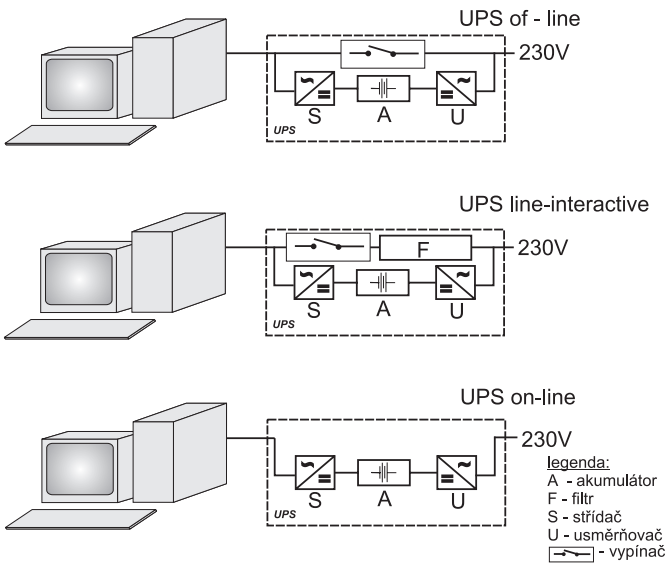
Dalším podstatným znakem serverů jsou velké skříně, do nichž se musí vejít několik disků a pásková jednotka. Důležité je také propracované chlazení (server se nevypíná). Často jsou prvky ve skříni v modulárním provedení dovolujícím výměnu jednotlivých modulů za chodu serveru. Je takto možné měnit disky, ventilátory atd.

Záložní zdroje UPS (Uninterruptible Power Supply)

Přerušení napájecího napětí serveru může způsobit velké problémy. Pro mnoho aplikačních programů i samotný síťový operační systém představuje náhlé ukončení práce (bez uložení dat) nedefinovaný stav, jehož následkem může být nutnost nové instalace systému nebo programu (nemluvě o ztrátě dat aplikačních programů).

Problematika UPS je široká a přesahuje rámec knihy, přesto si alespoň základní informace o napájecích zdrojích řekneme. Nejdříve k tomu, co náhradní zdroj obsahuje. Základem je samozřejmě akumulátor, ten musí být hermetizovaný, aby z něho nevycházely jedovaté výpary (určitě nemůžeme použít autobaterii). Akumulátor musíme dobíjet, dalším obvodem je tedy usměrňovač, který mění střídavý proud z elektrorozvodné sítě na stejnosměrný. Výstupní napětí z UPS však musí být střídavé, mezi akumulátorem a výstupem z UPS je střídač (měnící stejnosměrný signál na střídavý). Právě kvalita střídače od sebe jednotlivé UPS odlišuje. Vyrobit ze stejnosměrného proudu dokonalou sinusoidu s frekvencí 50 Hz není tak jednoduché. Technicky to samozřejmě možné je, ale stojí to peníze, takže se se skutečně sinusovým výstupem při napájení z akumulátoru setkáte pouze u kvalitnějších UPS (line-interactive či on-line). Základní obvody UPS mohou být různě zapojeny, což je asi základním kritériem při hodnocení UPS:

- **UPS off-line** jsou nejnižší a nejlevnější třídou záložních zdrojů. Mají jen jednoduchý nabíjecí obvod s usměrňovačem pro nabíjení akumulátorů a jednoduchý střídač s většinou nekvalitním lichoběžníkovým výstupem. Pokud je v elektrorozvodné síti dostatečně vysoké napětí, tak se počítač napájí přímo z ní, bez účasti jakýchkoliv filtrů či elektroniky v UPS. Jestliže hodnota napájecího napětí poklesne, přichází na řadu napájení z akumulátoru, které bohužel nemívá sinusový průběh (ale počítačům to zas tak nevadí).
- **UPS on-line** jsou naopak třídou nejvyšší, nejkvalitnější a nejdražší. Pracují tak, že výstup z UPS je vždy tvořen střídačem napájeným z akumulátorů a akumulátor je stále dobíjen z elektrorozvodné sítě. Počítač není vlastně nikdy připojen přímo k napájecí síti. Je tedy oddělen od všech poruch a nepravidelností v napájecí síti.
- **UPS line interactive** jsou jakýmsi mezi-článkem mezi oběma předešlými variantami. V základním režimu je spotřebič napájen přímo z elektrorozvodné sítě, ale napájecí napětí je v UPS upravováno. Jsou odfiltrovány šumy, někdy si elektronické obvody poradí bez účasti akumulátorů s mírným podpětím či přepětím.



Obrázek 2.2: *Principy UPS*

Poznámka: Na obrázku Principy UPS je přepínání mezi přímou napájecí větví a napájením přes baterie symbolizováno vypínačem.

K zálohování napájecího napětí počítačů jsou asi nejvhodnější UPS line interactive. Máme-li přísné požadavky na kvalitu napájecího napětí (tvar, odrušení...), budeme muset sáhnout hlouběji do kapsy a pořídit si UPS on-line.

Při výběru UPS musíme také zohlednit jejich technické parametry:

- **Výkon** UPS se udává ve VA (voltampérech) a musí být o něco větší než výkon napájecího zdroje serveru. Výkon napájecího zdroje serveru se vyjadřuje ve W (watt). Vztah mezi zdánlivým výkonem (voltampéry) a činným výkonem (watty) je pro napájecí zdroje serveru 0,7. (Činný výkon záložního zdroje by měl být 0,7 krát větší než zdánlivý výkon napájecího zdroje serveru.)

- **Čas napájení z UPS,** jde o dobu během níž je UPS schopná napájet server z baterií. UPS slouží k překlenutí krátkodobých výpadků napájení a ukončení systému, proto je horní hranice této doby zhruba dvacetiminutová. Platí přímá úměra mezi dobou zálohy a výkonem UPS. Při vyšším výkonu UPS (ve vztahu k výkonu zdroje serveru) se prodlužuje doba napájení z baterií. (Podívejme se na třetí řádek tabulky: kdybychom použili zálohovací zdroj 1000 VA pro napájení serveru 450 W, vzroste doba napájení z baterií na cca 60 min.)
- **Softwarové vybavení** je především pro servery životně důležité. Ve výbavě UPS bývá program (ten nahrajeme k síťovému operačnímu systému), který plní několik funkcí: podává informace o stavu baterií, o tom kdy UPS napájela PC z baterií, posílá zprávy o výpadcích napájecího napětí na e-mailovou adresu... Hlavní funkcí softwaru UPS je však legální ukončení operačního systému po určité době (kdy již hrozí nebezpečí, že se vybijí akumulátory v UPS). Pro komunikaci mezi UPS a serverem se používá sériový port nebo USB.
- **Stav baterií** je také velmi důležitý. Z vybitých baterií není napájení možné. Většina UPS má na čelním panelu kontrolní diody, z nichž je možné stav baterií vyčíst. Informaci zjistíme většinou také softwarově. Životnost baterií bývá 3 až 4 roky.

Pro představu uvádím tabulku výkonové řady jednotek UPS určených pro servery. Doba napájení je ještě závislá na momentální zátěži serveru (a také stavu baterií), a tak v tabulce udávám její mezní hodnoty.

Tabulka 2.1: Typické parametry záložních zdrojů

Výkon UPS	Výkon zdroje serveru	Doba napájení
620 [VA]	390 [W]	6–14 [min.]
700 [VA]	450 [W]	5–17 [min.]
1000 [VA]	650 [W]	6–18 [min.]
1400 [VA]	950 [W]	7–18 [min.]
2200 [VA]	1600 [W]	8–24 [min.]
3000 [VA]	2250 [W]	5–15 [min.]

Dedikace (vyčlenění) serveru

Server může být dedikovaný (vyčleněný). V takovém případě na něm běží pouze síťový operační systém a k běžné práci jej vůbec nepoužíváme. Opakem je server nededikovaný, na němž můžeme provádět běžnou práci a ještě na něm běží síťový operační systém. Takovouto práci dovolují například síťové operační systémy Windows Server. Uvědomíme-li si však, že na server jsou koncentrována data sítě, je běžná práce na něm nevhodná (už fyzický přístup ke konzole serveru je nebezpečný) a především u větších sítí se používá jen zřídka.

Softwarové požadavky na server

Základní služby, které budeme od serveru vyžadovat (bude je zajišťovat síťový operační systém) jsou následující:

File server

Je prvotní funkcí každého síťového operačního systému, která zabezpečuje:

- víceuživatelský přístup k souborům – s jedním souborem může současně pracovat více uživatelů,
- vede evidenci uživatelů, kteří se mohou k serveru přihlásit a má přehled o tom, co mohou a nemohou dělat na discích, adresářích (složkách) či s konkrétním souborem (např. někdo může soubory jen číst, jiný je vůbec nevidí, další má k souborům přidělena vyšší práva – zapisovat do nich, mazat je).

Print server

Síťový operační systém zprostředkuje přístup k jedné tiskárně více uživatelům. Opět se definuje, co může uživatel s tiskárnou provádět (jen tisknout, konfigurovat, mazat tiskové úlohy atd.).

Aplikační server

Servery neslouží pouze jako sklady dat, ale často jsou na nich spuštěny programy (aplikace) společné všem uživatelům sítí. Aplikací je celá řada, jsou určeny pro různé obory: Jde o různé ekonomické informační systémy zajišťující účetnictví, skladové evidence, kontakty na zákazníky, ekonomické rozbory. Dále se používají např. výrobní programy, sledující a řídící průběh výroby.

Mnoho aplikačních programů dodávají výrobci softwaru společně se síťovým operačním systémem. Ty jsou určeny pro doplnění základních serverových funkcí. Mezi nejčastěji dodávané patří:

- DHCP server
- DNS server (oba produkty se týkají práce s protokolem TCP/IP a jsou vysvětleny v kapitole Protokol TCP/IP. Dnes jsou součástí síťového operačního systému).
- Program pro připojení sítě k Internetu. Ten mívá minimálně dvě složky: Proxy server (ukládá prohlížená internetová data. Pokud si uživatelé sítě prohlížejí stejná data, čtou se z proxy, a ne z Internetu). Firewall – ten nepustí do naší sítě nikoho z Internetu.
- Program pro elektronickou poštu
- Programy pro správu velkých databází

Pro začátečníka bývá orientace ve spleti názvů jednotlivých aplikačních serverů velmi složitá. Výrobci síťových operačních systémů nabízejí také softwarové balíky. Jejich základem je operační systém, který je doplněn o jednotlivé aplikace. V následující tabulce jsou uvedeny takové programové balíky, jejich přehled je doplněn i o vysvětlení významu jednotlivých aplikací.

Tabulka 2.2: Balíky síťových operačních systémů

produkt	Microsoft Small Business Server 2003	Novell Small Business Suite 6.6	Linux
Operační systém	Microsoft Windows Server 2003	Novell NetWare 6.5	Linux
Připojení k Internetu	Microsoft ISA 2000	BorderManager	Proxy cache Squid
Elektronická pošta	Exchange 2000 Server	GroupWise	Sendmail, IMAP a LDAP servery
Správa databází	Microsoft SQL Server		PostgreeSQL, MySQL

Poznámka: *Cílem tabulky je vysvětlení terminologie nejpoužívanějších aplikačních serverů, není tedy úplným popisem produktů (a zde integrovaných služeb) a nezabývá se licenční politikou.*

Umístění serveru

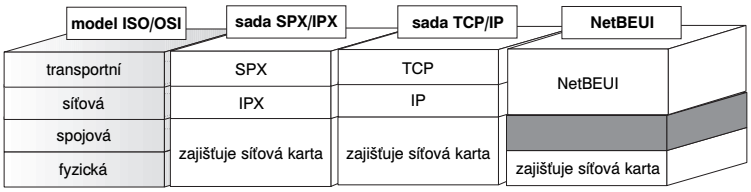
Z předešlých řádků to nemusí být na první pohled zřejmé, ale síťový hardware (ani software) nekladou žádné požadavky na umístění serveru. Ten tedy může být umístěn na libovolném místě sítě. Praktické umístění serveru je dáno spíše požadavky organizačními. Umísťuje se tak, aby nerušil svým hlukem okolí, aby byl dobře zabezpečen před krádeží a neodbornou obsluhou.

Síťové protokoly

Další nedílnou součástí síťového softwaru jsou síťové protokoly. Protokol definuje komunikační pravidla, jimiž se řídí výměna dat v síti. Pro správnou funkci sítě je tedy nutné, aby všechny síťové stanice používaly stejný protokol. V praxi se vždy setkáme se sadou protokolů, které navzájem spolupracují. U sítí LAN se fakticky používají tři druhy protokolů:

NetBEUI

Je protokolem poměrně starým. Vyvinula jej IBM v době, kdy na sítě nebyly kladeny takové požadavky jako dnes. NetBEUI proto nepodporuje směrování (není možné vytvořit síťové segmenty). Je vhodný pouze pro malé sítě peer to peer a dnešní operační systémy jej podporují pouze kvůli zpětné kompatibilitě. Celkově lze říci, že se používá velmi málo.



Obrázek 2.3: *Protokoly v modelu ISO/OSI*

IPX/SPX

Je sadou protokolů, vyvinutou firmou Novell pro její síťový operační systém NetWare. Setkáme se s ním především u NetWare 3.x a 4.x. Novější verze 5 a především 6 s ním samozřejmě umí také pracovat, ale jako prvotní používají protokoly sady TCP/IP. Především ve starších sítích a na starších serverech se ještě s protokoly IPX/SPX setkáme, proto bude následovat jejich popis. Na novějších systémech však dáváme přednost rodině protokolů TCP/IP.

Ve specifikaci IPX/SPX je obsaženo mnoho protokolů se speciálními úkoly. Pro naše účely postačí vysvětlit si činnost obou základních protokolů.

IPX (Internet Packet Exchange)

Je prvním ze sady protokolů IPX/SPX. Pracuje na úrovni síťové vrstvy ISO/OSI. Zajišťuje přenos paketů vyšších protokolů a přenos dat mezi stanicemi, ale nekontroluje správnost přenosu (to má na starosti vyšší protokol SPX). Jde o protokol nespojově orientovaný.

SPX (Sequenced Packet Exchange)

Je vyšším (nadřízeným) protokolem IPX. Jde o protokol spojově orientovaný, pracující na úrovni transportní vrstvy ISO/OSI. Kontroluje správnost přenesených paketů, při zjištění chyby vyžaduje opakování přenosu.

Adresace v sítích IPX/SPX

Při konfiguraci sítě se často setkáme s problémem adresace – přidělení originální adresy jedné stanici. Jednotlivé protokoly se s tím vyrovnávají odlišně. U sítí IPX/SPX se adresování řídí následujícími pravidly:

- Každý kabelový segment sítě má své vlastní číslo externí sítě IPX (external network number). Využívají je především směrovače. Číslo je osmimístné, vyjádřené hexadecimálně (šestnáctkově).
- Pak následuje číslo uzlu (node number), též udávané jako MAC adresa (Media Access Control address). Jde o unikátní adresu síťové karty. U karet Ethernet a Token Ring je údaj zadán již ve výrobě. Jde o dvanáctimístné hexadecimální číslo.

• Posledním je **číslo interní sítě** (IPX internal network number), tím je identifikován server. Číslo je hexadecimální a čtyřmístné.

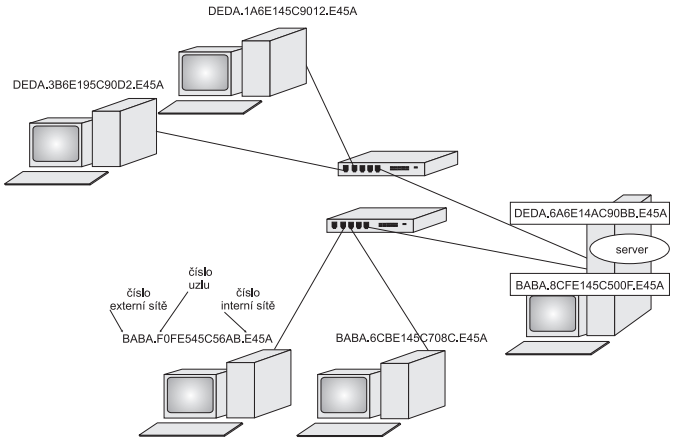
Pro adresaci v síti pak platí tyto zásady:

• každý server musí být unikátní, má tedy jedinečnou adresu definovanou interním číslem sítě

• unikátní jsou i čísla kabelových segmentů (externí čísla sítě), ale v rámci jednoho segmentu je externí číslo sítě stejné

• každá síťová karta (tj. počítač) má originální číslo uzlu

Výhodou tohoto uspořádání je to, že číslo interní i externí sítě se generuje automaticky (i když ho lze upravit) a rovněž číslo uzlu je generováno při výrobě. Uživatel tedy do adresování nemusí (ale může) zasahovat.



Obrázek 2.4: *Příklad adres IPX/SPX*

Na obrázku vidíme síť s dvěma segmenty – čísly externí sítě BABA a DEDA (vše to jsou hexadecimální číslice), každá karta má originální dvanáctimístné číslo uzlu a číslo interní sítě (serveru) je E45A. V serveru jsou dvě karty, každá s příslušným číslem segmentu.

Poznámka: S hexadecimálními (šestnáctkovými) adresami se setkáme při adresaci protokolů TCP/IP, bližší popis je v následující kapitole.

Protokol TCP/IP

Tato skupina protokolů je dnes určitě nejrozšířenější. Původně byla navržena pro síť, z níž se vyvinul Internet. Dnes je rodina protokolů TCP/IP používána v sítích Novellu i Microsoftu, kde se stala standardem a své předchůdce zcela vytlačila.

Z funkčního hlediska můžeme TCP/IP rozdělit na tři vrstvy (reprezentované samostatnými protokoly):

• *aplikační vrstvu* (spolupracující s konkrétními programy)

• *transportní vrstvu* (protokoly TCP a UDP)

• *síťovou vrstvu* (protokoly IP)

Spolupráce vrstev probíhá asi takto: Program (tj. aplikace) potřebuje navázat spojení se svým protějškem na jiném počítači. Použije k tomu aplikační vrstvu, od níž putuje požadavek na spojení do transportní vrstvy. Ta zorganizuje dopravu dat (data rozdělí na segmenty, naváže spojení, zkontroluje, zda byla data doručena). Vlastní přenos zajišťuje nižší – síťová vrstva. Segmenty, které obdržela od nadřazené vrstvy, „zabalí“ do datagramů a doručí vzdálenému počítači.

Aplikační vrstva

Je tvořena množinou protokolů spolupracujících s jednotlivými aplikačními programy. Jejich funkci se pokusím vysvětlit na jednoduchém příkladu:

Při prohlížení webových stránek používáme prohlížeč (nejčastěji asi *Internet Explorer*, ale existují i jiné programy, např. *Netscape Navigator, Mozilla* atd.). Prohlížeče spolupracují s internetovými servery, na nichž jsou webové stránky uloženy a uživatelům nabízeny (opět různými speciálními programy pro publikaci www, nakonec webové stránky můžeme nabízet i prostřednictvím Windows). Vidíme, že při brouzdání Internetem spolupracují různé programy

různých výrobců. Jejich spolupráce je zajištěna aplikačním protokolem – vlastně soustavou norem, které musí tyto programy respektovat. (Při prohlížení www stránek jím je protokol *http*.)

Aplikačních protokolů je mnoho, některé z nich (ty nejznámější) ukazuje tabulka.

Tabulka 2.3: Nejznámější aplikační protokoly

služba	funkce
FTP – File Transfer Protocol (datový kanál)	Používá se pro přenos souborů mezi vzdálenými PC
Telnet	Pro jednoduché terminálové relace (v podstatě ovládáme obrazovku vzdáleného PC)
Server DNS – Domain Name System	Organizuje jména počítačů v Internetu a jejich vazby na IP adresy
WWW – protocol HTTP (Hypertext Transfer Protocol)	Protokol používaný k uspořádání www stránek a pohybu mezi nimi
SMTP – Simple Mail Transfer Protocol	Protokol zajišťující přenos zpráv mezi servery Internetu (používaný hlavně pro elektronickou poštu)
POP3 – Post Office Protocol	Jeho posláním je dopravit poštu z elektronické schránky na náš počítač

Transportní vrstva

Je jakýmsi jádrem celé soustavy TCP/IP, tvořeným pouze dvěma protokoly: TCP a UDP.

Protokol TCP (Transmission Control Protocol)

Od aplikační vrstvy (prostřednictvím některého protokolu) přebere data, která rozdělí na segmenty, očísluje a seřadí podle toho, jak mají být postupně odeslány. Před začátkem výměny dat zahájí relaci s transportní vrstvou protějšího počítače. Poté začne s vysíláním a potvrzováním jednotlivých datových segmentů.

Vlastní odesílání je již věcí síťové vrstvy, což je popsáno dále. (Vše funguje také opačně: Od síťové vrstvy jsou přebrány datové segmenty, které TCP setřídí. Pokud některý chybí, tak si jej znovu vyžádá. Ze segmentů složí data a předá je prostřednictvím aplikačního protokolu některému z programů).

Protokol UDP (User Datagram Protocol)

UDP má stejné poslání jako TCP: převezme data od aplikace, sestaví z nich segmenty a předá je k odeslání síťové vrstvě. Na rozdíl od TCP nepotřebuje vytvářet před přenosem dat relaci s protějškem a nekontroluje zda byly datagramy protějškem přijaty.

Protokol UDP je jednodušší, ale méně spolehlivý. Některé programy jej využívají namísto protokolu TCP pro rychlý a nenáročný přenos dat (bez zajištění spolehlivosti).

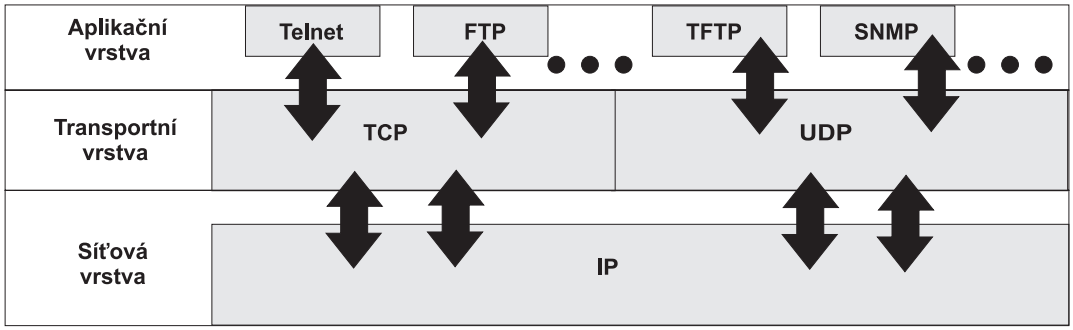
Protokol IP (Internet Protocol)

Pracuje v síťové vrstvě soustavy TCP/IP. Od nadřazených protokolů transportní vrstvy obdrží datové segmenty s požadavkem na odeslání. K segmentům připojí vlastní hlavičku a vytvoří IP datagram. V IP hlavičce je především IP adresa příjemce a odesílatele, což předznamenává hlavní poslání protokolu: doručení jednotlivých datagramů k příjemci – provádí tedy adresování a směrování datagramů mezi počítači.

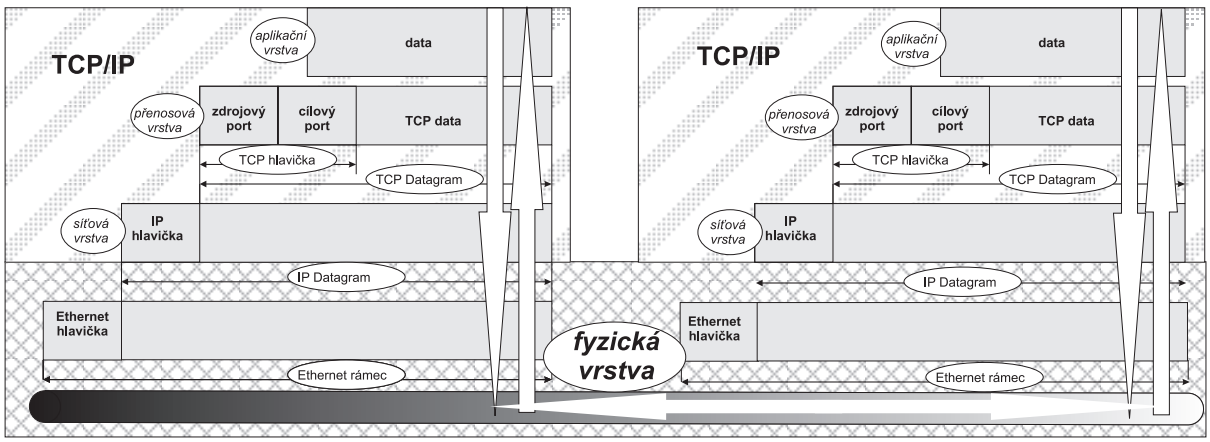
IP protokol je nespojovaný (před zahájením výměny dat nevytváří relaci) a nespolehlivý (předání paketů na místo určení není kontrolováno). Paket IP se tedy může ztratit, být doručen mimo pořadí, zdvojen nebo zpožděn. Protokol IP neobsahuje prostředky pro zotavení z chyb tohoto typu. To vše má zajistit nadřízená transportní vrstva – protokol TCP.

Uspořádání protokolů TCP/IP ukazuje obrázek *Rodina protokolů TCP/IP*. Komunikace mezi jednotlivými protokoly probíhá bránami, anglicky porty. Černé šipky na obrázku porty znázorňují. V soustavě TCP/IP odpovídá každému protokolu jedna brána.

Na druhém obrázku *Spolupráce v TCP/IP* je naznačena vzájemná výměna dat mezi jednotlivými vrstvami protokolů TCP/IP. Vlastní přenos provádí zařízení fyzické vrstvy – síťová karta, kabeláž a aktivní prvky kabeláže.



Obrázek 2.5: *Rodina protokolů TCP/IP*



Obrázek 2.6: *Spolupráce v TCP/IP*

Adresace v sítích TCP/IP

Při zprovozňování sítě založené na protokolu TCP/IP je pro nás z praktického hlediska nejdůležitější práce s adresami. V sítích IPX/SPX probíhá adresace a konfigurace sítě automaticky, ale v sítích TCP/IP je většinou nutný zásah uživatele. (Není to úplná pravda, existuje služba DHCP, která adresaci podle zadaných pravidel provede automaticky, ale tato služba není k dispozici vždy).

Základní a nejobecnější pravidlo adresace je jednoduché – každá stanice musí mít originální číslo, navíc je potřebné, aby z čísla bylo zřejmé umístění stanice v síti či síťovém segmentu. Každá stanice má tedy svoji IP adresu reprezentovanou čtveřicí čísel, oddělených tečkou. Obecně je ve výpočetní technice výchozím formátem čísel dvojková abeceda. Pokud vyjádříme IP adresu dvojkově, bude adresa tvořena čtyřmi osmibitovými čísly. (Osm bitů představuje jeden bajt.

Je možné také říci, že adresa IP je tvořena čtyřmi bajty). Celá adresa může například vypadat takto: 11000000.10101000.00000001.00001011. Vyjadřování ve dvojkové soustavě není každému srozumitelné, a proto se pro zápis čísel IP adresy mohou použít ještě jiné číselné soustavy: šestnáctková a nám nejpřirozenější desítková. Velice stručně uvedu několik poznámek.

- **dvojková (binární) –** má pouze dvě číslice 0 a 1 a jak již bylo řečeno, je soustavou, s níž pracují hardwarové prvky PC.
- **šestnáctková (hexadecimální)** – jejím základem je šestnáct znaků: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, A, B, C, D, E, F. Občas se s ní v adresaci IP také setkáme. V šestnáctkovém vyjádření by výše uvedená dvojková adresa vypadala takto: C0.A8.01.11.
- **desítková (dekadická) –** je tou soustavou, v níž jsme zvyklí pracovat, a proto ji budeme dále používat. Naše příkladová adresa vypadá v desítkové soustavě takto: 192.168.1.11.

Tip: Pro převody mezi soustavami existují přesná pravidla, také význam a váha jednotlivých číslic soustav je přísně definována. Popis obou skutečností přesahuje rámec knihy, přesto se zmíním alespoň o snadném způsobu převodu mezi soustavami, který je v praxi nejdůležitější. Můžeme využít program Kalkulačka, který najdeme v Příslušenství Windows. Přepneme-li její obrazovku do vědeckého rozhraní (v menu Zobrazit), můžeme jednoduše provádět převody. Zvolíme soustavu, z níž chceme převádět (tlačítko Hex je pro šestnáctkovou, Dec pro desítkovou, Bin pro binární soustavu) a pak přepneme kalkulačku do cílové číselné soustavy. Na displeji vidíme výsledek převodu.

V praxi mezi sebou spolupracují různé sítě, jednotlivé sítě mohou být navíc rozděleny na části – segmenty. V IP adrese počítačů spojených do sítě nestačí uvést pouze číslo konkrétního počítače, ale potřebujeme znát ještě číslo sítě (nebo jejího segmentu), v níž je počítač zařazen. Část IP adresy pak vyjadřuje číslo sítě a zbytek popisuje adresu počítače v této síti. Podle toho, jaká část adresy je věnována síti a jaká číslu PC, jsou IP adresy rozděleny do tříd. Třídy sítí vidíme v tabulce, která ukazuje kolik čísel ze čtveřice je vyhrazeno pro určitý typ adresy (čím více bajtů je věnováno adrese sítě, tím více sítí můžeme adresovat, ale tím méně číslic zbude na adresy počítačů v síti a naopak). Vše ještě přibližuje obrázek.

Obrázek 2.7: *Program Kalkulačka*

Tabulka 2.4: Třídy sítí IP

	Rozsah adres prvního čísla	Počet čísel vyhrazených pro adresu sítě	Počet čísel vyhrazených pro adresu uzlu	Použití
Třída A	0–127	1 (adresuje 126 sítí)	3 (adresuje asi 17 mil. uzlů = PC)	Pro rozsáhlé sítě
Třída B	128–191	2 (adresuje 16 tis. sítí)	2 (adresuje asi 65 tis. uzlů)	Středně velké sítě
Třída C	192–223	3 (adresuje 2 mil. sítí)	1 (adresuje asi 254 uzlů)	Menší sítě

IP adresy byly poprvé použity v Internetu a až později se začaly používat v lokálních sítích. Aby nedocházelo ke konfliktům adres (mezi IP adresami lokálních sítí a adresami internetovými), byly v každé třídě IP adres vymezeny pro lokální sítě adresové rozsahy. Jsou to:

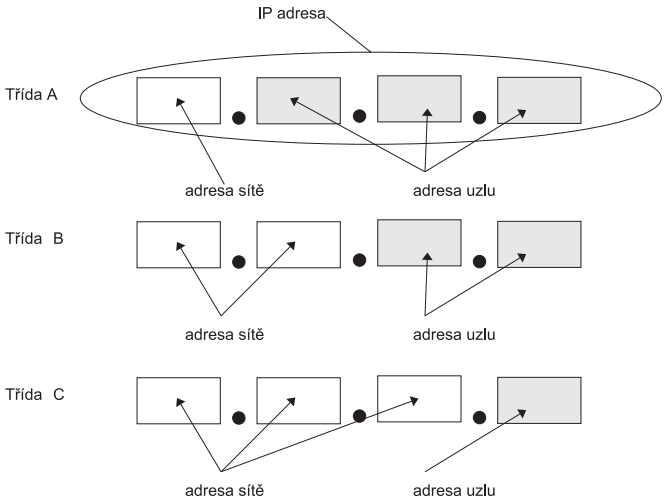
- **Třída A:** 10.0.0.0 až 10.255.255.255
- **Třída B:** 172.16.0.0 až 172.31.255.255
- **Třída C:** 192.168.0.0 až 192.168.255.255

Jak vidíme v tabulce, je IP adresa navržena variabilně, adrese sítě je možné vyhradit 1 až tři číslice (neboli bajty). Abychom poznali, která část adresy je síťová, je nedílnou součástí IP adresy také **síťová maska**. Maska je opět čtyř-

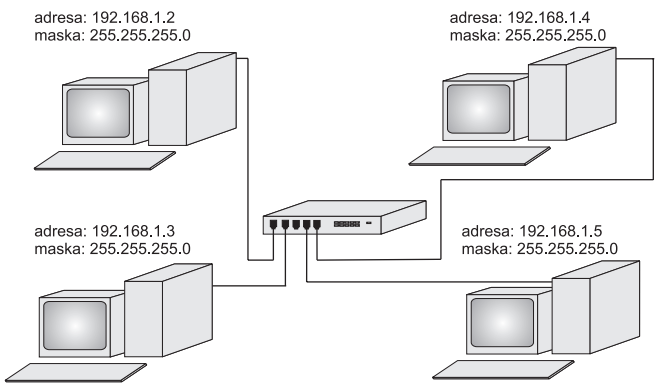
bajtové číslo, vycházející přirozeně ze dvojkové soustavy. V masce jsou na místě síťové adresy vždy zapsány jedničky (vyjadřujeme se dvojkově).

Pro IP adresy vyhrazené lokálním sítím se používají standardní síťové masky:

- pro **třídu A,** kde je adrese sítě určen první bajt (první číslo), je binární tvar masky 11111111.00000000.00000000.00000000, hexadecimální FF.00.00.00 a dekadický 255.0.0.0
- pro **třídu B,** kde jsou adrese sítě určeny první dva bajty (první dvě čísla), je binární tvar masky 11111111.11111111.00000000.00000000, hexadecimální FF.FF.00.00 a dekadický 255.255.0.0
- pro **třídu C,** kde jsou adrese sítě určeny první tři bajty (první tři čísla), je binární tvar masky 11111111.11111111.1111111.00000000, hexadecimální FF.FF.FF.00 a dekadický 255.255.255.0



Obrázek 2.8: *Třídy TCP/IP*

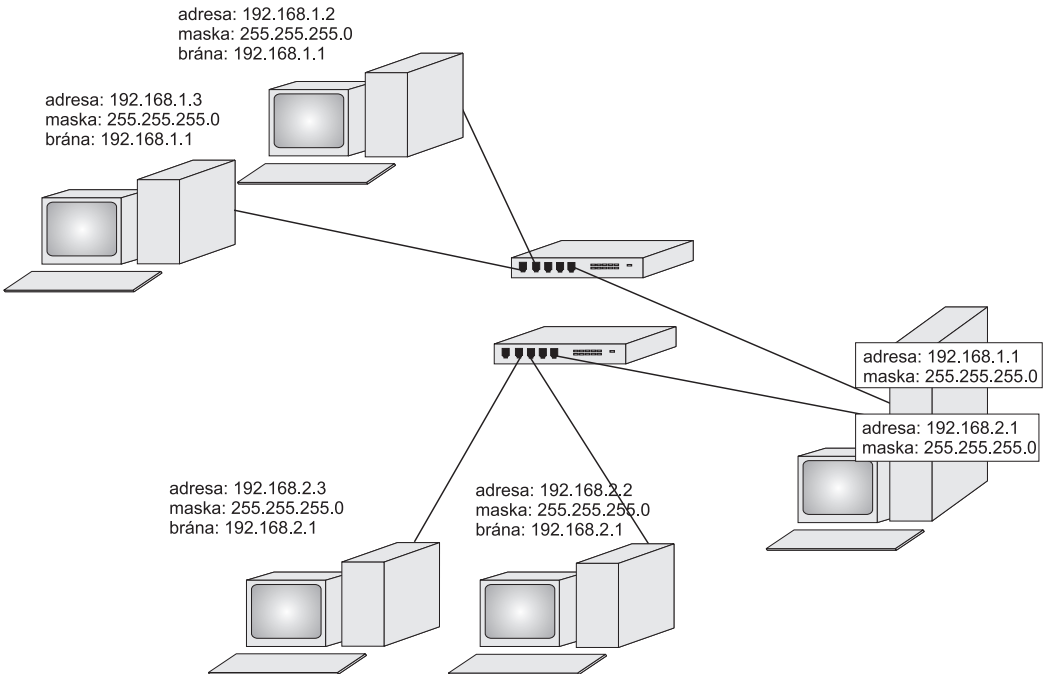


Obrázek 2.9: *Adresace v síti TCP/IP*

Na obrázku je vidět malou síť a její konfiguraci protokolem TCP/IP. Síť je složena z adres třídy C, každý počítač má svoji originální adresu a ke každé adrese samozřejmě patří síťová maska.

Propojování sítí TCP/IP

Již jsem se několikrát zmínil o tom, že počítače zapojené v síti nekomunikují pouze v rámci vlastní sítě, ale je také možná výměna dat s počítači umístěnými v jiné síti. Kvůli mezisíťové komunikaci obsahuje IP adresa další údaj – **bránu (gateway)**. Brána je nepovinnou částí adresy, kterou potřebujeme pouze při výměně dat mezi dvěma sítěmi. Jde opět o číselný údaj stejného formátu jako IP adresa (můžeme ji vyjádřit dvojkově, šestnáctkově i desítkově). Brána je IP adresou, na níž budou směrovány pakety v případě, že jejich adresa bude mimo rozsah vlastní sítě – budou-li posílány na adresu jiné sítě než té, z níž jsou vysílány. Vše nejlépe pochopíme z obrázku. Jsou zde dvě sítě TCP/IP: první s rozsahem adres 192.168.1.x a druhá má rozsah 192.168.2.x. Součástí každé sítě je ještě jedna síťová karta počítače, kterým jsou obě sítě spojeny. Tento počítač pak plní funkci brány spojující obě sítě. Na síťových stanicích je zadána brána – číslo síťové karty, kam budou mířit datové pakety v případě, že jejich cílová adresa není obsažena v síti, z níž byly vyslány. Software počítače – brány pak zajistí převod mezi oběma kartami.



Obrázek 2.10: *Propojování sítí TCP/IP*

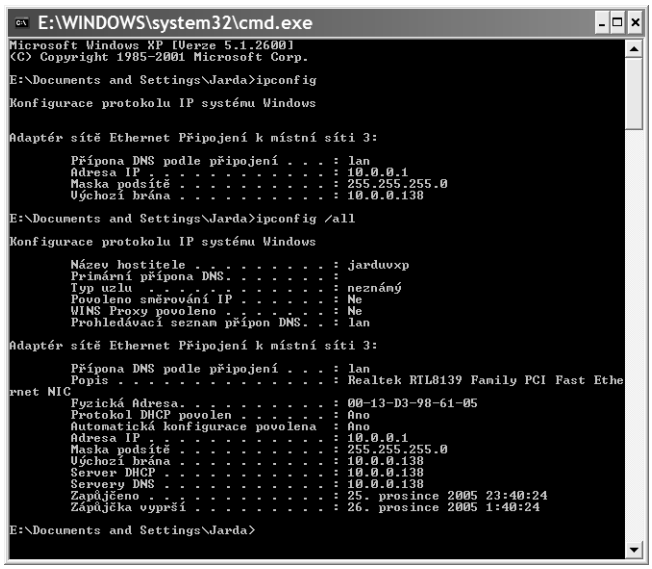
DHCP a DNS

Závěrem se ještě zmíním o dvou pojmech, které s adresací TCP/IP úzce souvisejí. Nepoužívají se však vždy a při konfiguraci malých sítí LAN se s nimi setkáme pouze okrajově:

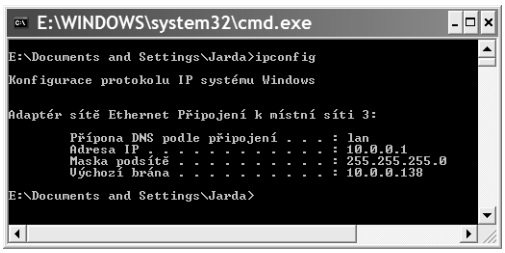
- **DHCP (Dynamic Host Configuration Protocol)** automaticky přiděluje IP adresy. Bývá nabízen jako služba síťového operačního systému – je to tedy program spuštěný na serveru (tzv. DHCP server). Po připojení stanice do sítě jí je serverem přidělena IP adresa.
- **DNS (Domain Name System)** Tato služba byla vyvinuta pro Internet, v němž má každý počítač svoji IP adresu, ale počítačů je mnoho a bylo by nemožné zapamatovat si, pod jakým číslem jsou skryty hledané údaje. Proto existuje DNS, která převádí čísla na lépe zapamatovatelná jména. DNS rozděluje počítače do zón, nazývaných domény. (Například všechny počítače v ČR jsou zařazeny do domény .cz). Domény se dále řadí do stromové struktury. DNS zadáváme tehdy, když počítač připojujeme k Internetu a musíme zadat IP adresu alespoň jednoho serveru, který DNS převod provede.

Informace o nastavení protokolu TCP/IP

Pro zjištění základních informací o nastavení TCP/IP je ve Windows XP k dispozici příkaz *IPCONFIG.* Ten pracuje v příkazovém režimu, do něhož se dostaneme poklepáním na tlačítko *Start/Spustit,* v okně Spustit zadáme příkaz *cmd.* (Okno Spustit vyvoláme také rychlou volbou – současným stiskem kláves *Windows* a *R). P*o zadání *cmd* již máme okno příkazové řádky k dispozici. Po napsání příkazu *ipconfig* vidíme základní údaje o TCP/IP. Chceme-li získat informace detailní, přidáme ještě parametr all, příkaz bude mít tvar *ipconfig/all.*



Obrázek 2.11: *Příkaz ipconfig/all*



Obrázek 2.12: *Příkaz ipconfig*

Ethernetové rámce

Data si jednotlivé protokoly (pracující ve vrstvě ISO/OSI) mezi sebou vyměňují prostřednictvím datagramů. Datagram je množina dat zpracovaná podle pravidel protokolu.

Před přenosem je datagram rozdělen na menší části – pakety – vhodné pro přenos mezi síťovými PC. Přeprava paketu probíhá v linkové a fyzické vrstvě, podle pravidel Ethernetu. Před faktickým odesláním je paket „zabalen" do ethernetové obálky – rámce (je zde adresa příjemce, odesílatele, vlastní data, kontrolní součet). Pro přepravu dat existuje několik Ethernetových norem (obálek), které ukazuje tabulka. Typ rámce je vlastností síťové karty, staré karty umějí jen rámec 802.3, novější znají rámce všechny.

Tabulka 2.5: Ethernetové rámce

Název rámce	Charakteristika
Ethernet 802.2	novější standard firmy Novell, umí přepravovat pouze IPX/SPX
Ethernet 802.3	původní standard firmy Novell, umí přepravovat pouze IPX/SPX
Ethernet II	umí přepravovat IPX/SPX i TCP/IP, nejrozšířenější, nejjednodušší
Ethernet SNAP	umí přepravovat IPX/SPX i TCP/IP

Pozorný čtenář si jistě všiml rozporu v terminologii. V dřívějším textu jsem často pojem paket používal, ale měl jsem spíše použít termín rámec. V praxi se však často oba dva termíny zaměňují. Pro upřesnění tedy shrnu: paket je produktem síťového softwaru, zpracovaný podle pravidel určitého protokolu. Rámec produkuje síťová karta (a její ovladač), podle pravidel síťového hardwaru.

Tip: Pokud je to možné, vždy používejte v síti jen jeden rámec!

Kapitola 3

Síť peer to peer

Základní charakteristiky této sítě již známe: je to síť sestavená z počítačů, jež si navzájem nabízejí své služby. Každý počítač je tedy klientem a zároveň serverem. Víme, že toto uspořádání se hodí pro několik PC – zhruba do 10, že pro síť peer to peer nepotřebujeme mít žádný speciální software – stačí operační systém Windows. My si ukážeme konfiguraci Windows XP.

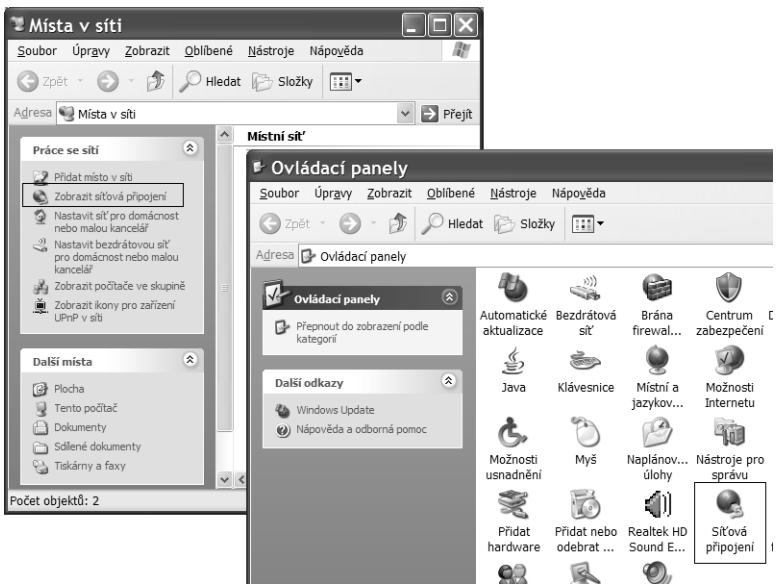
K vytvoření sítě musíme provést několik kroků:

- Instalovat kabeláž.
- Zasunout síťové karty do počítačů a načíst jejich ovladače.
- Instalovat klienta sítě, nakonfigurovat síťové protokoly a vytvořit pracovní skupiny.
- Nastavit sdílení (složek a adresářů), definovat případná přístupová práva.

První dva kroky jsme si již podrobně popsali. Patrně použijeme kroucenou dvojlinku kategorie 5, dnes spíše 5e, switch a síťové karty Fast nebo Gigabitového Ethernetu. Další kroky si vysvětlíme podrobně v následujících řádcích.

Práci se síťovými klienty a protokoly (jejich instalaci a nastavování) je ve Windows XP věnována obrazovka *Síťová připojení*. Vstoupit do ní můžeme více způsoby, například:

- poklepem na ikonu *Místa v síti* a v pravé části okna *Místa v síti* klepneme na *Zobrazit síťová připojení*,
- na ikonu *Místa v síti klepneme* pravým tlačítkem myši a pak zvolíme *Vlastnosti*,
- *Síťová připojení* najdeme také v *Ovládacích panelech*.

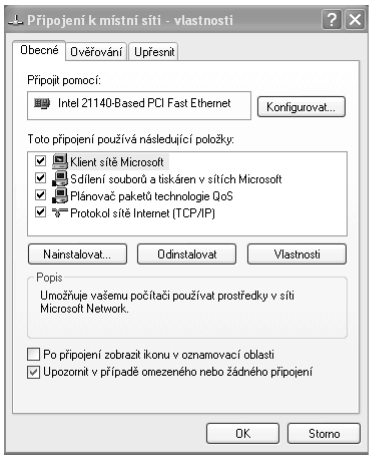


Obrázek 3.1: *Otevření okna Síťová připojení*

A nyní se již budeme věnovat oknu *Síťová připojení*. Po jeho otevření spatříme ikony reprezentující jednotlivá síťová připojení. Počet ikon a jejich názvy vycházejí z konkrétní konfigurace počítače, typický příklad ukazuje obrázek:

- *Připojení k Internetu* zastupuje připojení k Internetu modemem ADSL.
- *1394 připojení* je zástupcem rozhraní 1394 (FireWire), které je integrováno na základní desce mého PC.
- *Připojení k místní síti* informuje o připojení počítače k síti LAN, je pro naše potřeby nejdůležitější a jeho vlastnostem se budeme věnovat.

Obrázek 3.2: *Okno Síťová připojení*



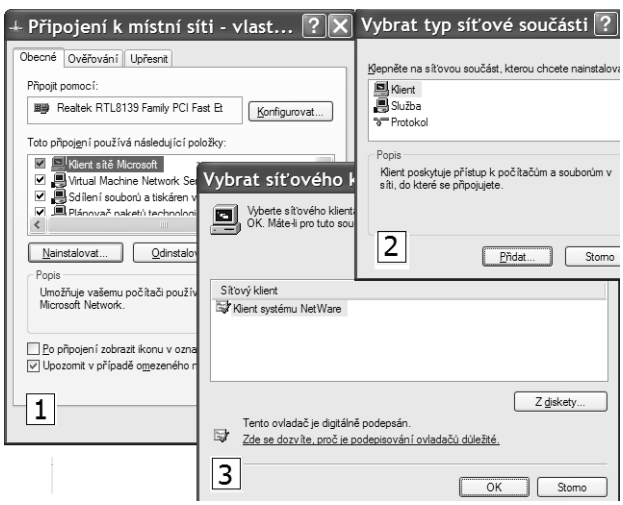
Obrázek 3.3: *Okno Připojení k místní síti – vlastnosti*

Na našem PC vidíme jedno *Připojení k místní síti,* ale pokud by bylo v PC nainstalováno více síťových karet, bylo by síťových připojení také více – pro každou síťovou kartu jedno. Vlastnosti konkrétního připojení jsou dostupné v okně *Připojení k místní síti – vlastnosti.* Otevřeme ho klepnutím pravého tlačítka myši na ikoně síťového připojení a volbou *Vlastnosti.* Okno má tři záložky, my se budeme věnovat především záložce *Obecné.* Zde jsou k dispozici všechny součásti potřebné ke konfiguraci sítě. Při instalaci síťové karty je sem doplní Windows XP. To samozřejmě můžeme měnit, součásti odebírat i přidávat, ale ke zprovoznění sítě peer to peer již většinou jiné součásti potřebovat nebudeme. Najdeme zde *Klienta sítě Microsoft, Sdílení souborů a tiskáren v sítích Microsoft* a *Protokol TCP/IP.*

Práce s klientem

Pro práci v síti peer to peer je potřebný *Klient sítě Microsoft,* který se instaluje automaticky spolu s ovladačem síťové karty. Ve Windows je k dispozici také *Klient systému NetWare,* ale jeho posláním je spojení síťového PC se serverem NetWare, v síti peer to peer se tedy nepoužívá. Obecně je možné každého klienta přidat a odebrat. I když to patrně nebudeme potřebovat, uvedu alespoň stručný popis toho jak to udělat (budeme pracovat v okně *Připojení k místní síti – vlastnosti)*:

- Odebrání klienta je velmi snadné, myší ťukneme na klienta (umístíme tak na něj kurzor) a stiskem tlačítka *Odinstalovat* jej odebereme.
- Instalaci zahájíme tlačítkem *Nainstalovat,* v okně *Vybrat typ síťové součásti* vybereme *Klient* a stiskneme tlačítko *Přidat,* přejdeme tak do okna *Vybrat síťového klienta*, kde klienta vybereme a stiskem tlačítka *OK* instalaci dokončíme. V praxi



Obrázek 3.4: *Přidání klienta*

je jiný klient potřeba především u sítí Novell (k připojení k serveru NetWare). Jeho instalaci si v kapitole Síť Novell NetWare ještě ukážeme.

Síťové protokoly

Jak již víme, jsou k dispozici protokoly NetBEUI, IPX/SPX a TCP/IP. Pro malou síť peer to peer můžeme použít kterýkoliv z nich. Pro jejich volbu platí tato kritéria:

- na všech počítačích musí být nahrán stejný protokol
- v jedné síti bychom měli používat co nejméně protokolů

První podmínka je jasná, ale u druhé se pozastavím. Jestliže bude naše malá síť izolovaná, můžeme zvolit jakýkoliv protokol. Shrňme si jejich vlastnosti:

- NetBEUI je jednoduchý, ale nesměrovatelný (není možná práce mezi sítěmi) a dnes se téměř nepoužívá. Do Windows XP jej musíme instalovat nestandardním postupem (který je dále popsán).
- IPX/SPX je sice určen pro sítě firmy Novell, ale v síti peer to peer bude také pracovat. Navíc se nemusí konfigurovat.
- TCP/IP je dnes nejrozšířenější, u Windows XP (ale i u starých 98 a 2000) se nainstaluje automaticky s *Klientem sítě Microsoft*. Protokol se musí ručně donastavit – nesmíme zapomenout zadat každému PC jedinečnou IP adresu. Dnes je většina sítí připojena k Internetu, k čemuž je protokol TCP/IP nutný, a tak je ve většině sítí právě protokol TCP/IP tím základním (a zpravidla také jediným).

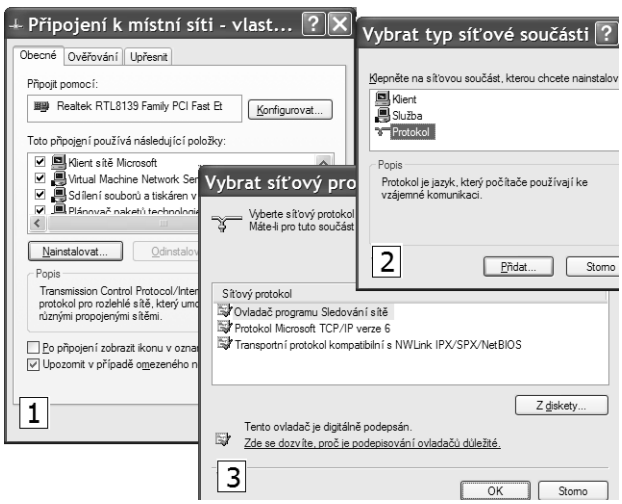
Z dosavadního výkladu to není patrné, ale pracujeme-li na síti klient server (tzn. naše stanice se připojuje k serveru), je zároveň možné vytvořit na stejné kabeláži síť peer to peer. Jednoduše ke klientovi serverové sítě dohrajeme klienta sítě peer to peer. V takovém případě je nutné pamatovat na to, abychom v síti používali co nejméně protokolů. Připojujeme-li se k serverům Novell NetWare verze 4.x, použijeme také pro síť peer to peer protokol IPX/SPX (pokud se však bude tato síť připojovat k Internetu, bude nutné použít ještě protokol TCP/IP). U sítí Novell NetWare verzí 5 a 6.x. a Microsoft Windows 2000 či 2003 je doporučeno používat protokol TCP/IP. V dalším si proto popíšeme konfiguraci sítě peer to peer prostřednictvím protokolu TCP/IP.

Tip: Při volbě protokolu může být rozhodující podmínkou software, který budeme používat. Pokud program vyžaduje určitý protokol, budeme ho muset v naší síti nainstalovat.

Instalace a odebrání protokolu

Jak již bylo řečeno, protokol TCP/IP se instaluje automaticky. Pokud bychom jej chtěli odebrat (či přidat jiný protokol), použijeme analogický postup jako při práci se síťovými klienty:

- použijeme tlačítko *Odinstalovat* (před tím na protokol myší umístíme kurzor)
- také k přidání protokolu použijeme téměř stejný postup jako při přidávání klienta: Začneme tlačítkem *Nainstalovat,* v obrazovce *Vybrat síťového kli-*



Obrázek 3.5: *Přidání protokolu*

enta zvolíme *Protokol* a po stisku tlačítka *Přidat* se ocitneme v poslední obrazovce *Vybrat síťový protokol,* kde vybereme protokol a stiskem *OK* instalaci ukončíme.

NetBEUI ve Windows XP

NetBEUI je již protokolem velice starým a zřídka používaným, Windows XP nepočítají s jeho použitím, a proto jej výše popsaným způsobem nelze nainstalovat. Některé starší programy, určené pro práci v síti, však komunikují mezi sebou pouze tímto protokolem. Do Windows XP můžeme NetBEUI doinstalovat, ale poněkud složitějším způsobem. Je třeba mít k dispozici instalační médium (CD disk) systému Windows XP.

- Na instalačním CD disku Windows XP otevřete složku *\VALUEADD\MSFT\NET\NETBEUI.*
- Odsud zkopírujte soubor *NBF.SYS* do složky *WINDOWS\SYSTEM32\DRIVERS.*
- Dále zkopírujte soubor *NETNBF.INF* do složky *WINDOWS\INF* (najdete ho také ve *\VALUEADD\MSFT\NET\NETBEUI).*
- Otevřete ikonku *Místa v síti*, v levém okně menu klepněte na řádek *Zobrazit síťová připojení.*
- Klepněte pravým tlačítkem myši na ikoně *Připojení k místní síti* a zvolte *Vlastnosti.*
- Klepněte na tlačítko *Nainstalovat*, zvolte *Protokol* a klepněte na tlačítko *Přidat*, zvolte *Protokol NetBEUI* a klepněte na tlačítko *OK*. (To že NetBEUI je k dispozici, způsobilo předešlých 5 kroků).
- V seznamu protokolů se zobrazí položka *Protokol NetBEUI.*
- Nakonec musíme počítač restartovat.

Konfigurace protokolu TCP/IP

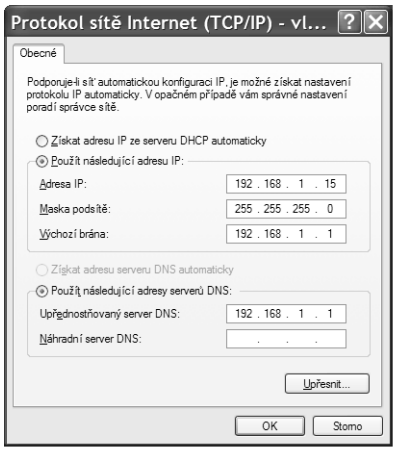
TCP/IP je v sítích nejrozšířenějším protokolem, ale většinou je nutné jej konfigurovat. Východiskem k jeho nastavení je obrazovka *Připojení k místní síti – vlastnosti*. Poklepeme-li na její (většinou poslední) řádek *Protokol sítě Internet (TCP/IP),* otevřeme okno *Protokol sítě Internet – vlastnosti,* kde jsou již k dispozici jednotlivá nastavení TCP/IP. Obrazovka karty *Obecné* obsahuje dva skupinové rámečky, horní věnovaný adrese IP a spodní, určený k zadávání serverů DHCP. Oba skupinové rámečky začínají variantou automatické konfigurace (*Získat adresu IP ze serveru DHCP automaticky, Získat adresu serveru DNS automaticky*). Je to varianta velmi příjemná, rychlá a nenáročná, aby však fungovala, musí v síti pracovat DHCP server, který automatické přidělování adres zabezpečí. Tato služba je obsažena v serverových operačních systémech, často ji obsahují také hardwarové prvky (např. ADSL modemy či routery, jimiž připojujeme sítě k Internetu. DHCP server pracuje také ve *Sdíleném připojení k Internetu* – součást Windows XP). Pokud je DHCP k dispozici, není důvod jej nepoužít. V konfiguračním okně ponecháme obě automatické volby zaškrtnuté, odpadne nám pracné ruční nastavování a konfigurace TCP/IP je hotova (nepotřebujete pak číst další řádky, popisující ruční nastavování).

Ve většině sítí peer to peer však DHCP k dispozici nemáme, musíme tedy parametry TCP/IP nastavit. Nejdříve se budeme věnovat adrese IP (horní skupinový rámeček). Zaškrtneme možnost *Použít následující adresu IP,* čímž si zpřístupníme řádky:

- **Adresa IP** je nejdůležitější volbou, sem zapisujeme IP adresu. Připomínám že, v jedné síti nesmějí být dvě adresy stejné. Adresy vybíráme z rozsahu nepřidělovaného v Internetu: pro adresy třídy A to je rozsah 10.0.0.0 až 10.255.255.255, pro třídu B 172.16.0.0 až 172.31.255.255 a třída C používá adresy 192.168.0.0 až 192.168.255.255.
- **Maska podsítě** bývá v sítích LAN standardní, pro adresy třídy A to je 255.0.0.0, třídu B 255.255.0.0 a třídu C 255.255.255.0. Budeme-li používat standardní masky, Windows jejich hodnotu doplní automaticky.
- **Výchozí brána** – tuto záložku použijeme, pokud chceme propojit naši síť TCP/IP s jinou sítí TCP/IP. Vkládáme sem IP adresu počítače, přes nějž se k jiné síti připojujeme. Obyčejně jsou v tomto PC dvě síťové karty, pro každou síť jedna. Brána je typickým parametrem při připojování sítí k Internetu (často je pak branou IP adresa hardwarového prvku, jenž nás s Internetem spojuje).

Tip: Pro síťový provoz postačuje pouze jeden protokol. Pokud se vám s některým klientem nainstaluje ještě další protokol, nebojte se jej smazat (tlačítkem Odebrat v ovládacím panelu Sítě).

Pokud nebude DNS server (DNS služba převádí číselné IP adresy počítačů na lépe srozumitelná jména) zadáván automaticky, musíme ručně vyplnit jeho hodnotu. Po zaškrtnutí volby *Použít následující adresy serverů DNS* můžeme zapsat adresy pro: **Upřednostňovaný server DNS** a **Náhradní server DNS.** Obě adresy potřebujeme především pro připojování k Internetu a většinou nám je sdělí firma, která nás k Internetu připojí. Je dobré zadávat obě adresy. Pokud totiž dojde k poruše upřednostňovaného serveru, máme k dispozici další server, který převod mezi jmény PC a jejich IP adresami provede. Někdy může běžet DNS služba na prvku, kterým je síť připojena k Internetu. Pak přirozeně zadáváme IP adresu tohoto prvku.



Obrázek 3.6: *Konfigurace TCP/IP*

Vytvoření pracovních skupin a pojmenování počítačů

V síti peer to peer je nesmírně důležitá identifikace počítače. Každý počítač musíme pojmenovat a přiřadit do určité pracovní skupiny. V síti může být jedna nebo více pracovních skupin. Rozdělení počítačů do několika pracovních skupin usnadní orientaci v síti. Pokud je skupin více, je samozřejmě možné se mezi nimi přepínat. Zda budeme pracovat v jedné nebo několika skupinách je vyloženě individuální záležitostí, vyplývá to z potřeb konkrétní sítě a především z potřeb uživatelů a rozhodující je názor správce sítě.

Pojmenování PC je ve Windows XP poměrně snadné. Klepneme pravým tlačítkem myši na ikonce *Tento počítač,* menu *Vlastnosti* a otevřeme okno *Vlastnosti systému.* (Další alternativou je *Start/Ovládací panely/Systém.*) Přejdeme na záložku *Název počítače* a zde již můžeme pracovat. K identifikaci PC se používají dva pojmy:

- Popis počítače: je údajem spíše pomocným, upřesňuje informace o PC.
- Úplný název počítače: je hlavním identifikačním údajem, pod ním je počítač veden v síti.

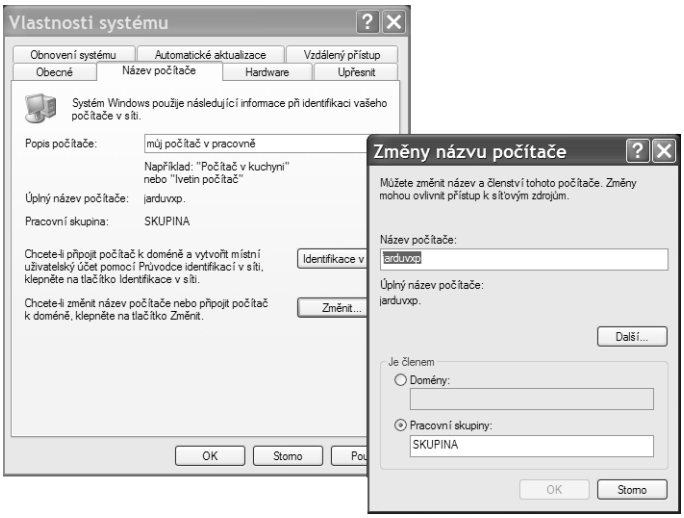
Na obrázku *Počítače v síti* vidíte příklad malé sítě a především to, jak se různě pojmenované počítače zobrazují v síti. Jsou zde dva počítače zařazené do pracovní skupiny *Skupina.* První počítač se jmenuje Jarduvxp a nemá definován žádný *Popis počítače,* druhý počítač je pojmenován *U_deti,* a jeho *Popis počítače* zní *u Honzíka a Báry.*

Obrázek 3.7: *Počítače v síti*

A nyní již ke kartě *Název počítače:*

- V prvním řádku *Popis počítače* zadáme příslušný popis (je to volitelná nepovinná položka).
- Dále vidíme dva základní údaje *Úplný název počítače* a *Pracovní skupinu*, v níž je PC zařazeno. Oba dva údaje můžeme měnit stiskem tlačítka *Změnit,* čímž přejdeme do okna *Změny názvu počítače.* Práce zde je intuitivní a není ji třeba blíže popisovat. Snad jen jedna poznámka – při práci v síti peer-to-per pracujeme v *Pracovní sku-*

pině, práci v *Doméně* je věnována zvláštní kapitola knihy (*Síť Windows Server 2003*). Při přiřazování PC do sítě musíme dodržet určitá pravidla: název pracovní skupiny se nesmí shodovat s názvem počítače. Název pracovní skupiny i počítače se může skládat z max. 15 znaků, ale nesmí obsahovat: ; : " < > * + = \ | ? ,. Rovněž v názvu počítače jsou zakázané znaky ~ ! @ # $ ^ & * () = + [] {} \ | ; ’ “ , < > / ?



Obrázek 3.8: *Pojmenování počítače a přiřazení do skupiny*

Průvodce instalací sítě

Všechna síťová nastavení jsou ve Windows XP integrována do *Průvodce instalací sítě*. Nastavíme zde způsoby připojení k Internetu, pojmenujeme počítač a zařadíme jej do pracovní skupiny, nastavíme sdílení a konečně můžeme vytvořit *Síťovou instalační disketu*. Některým nastavením jsme se věnovali v předešlých kapitolách – šlo o ty konfigurace, které se občas mění a je zbytečné kvůli nim procházet celého *Průvodce instalací sítě*.

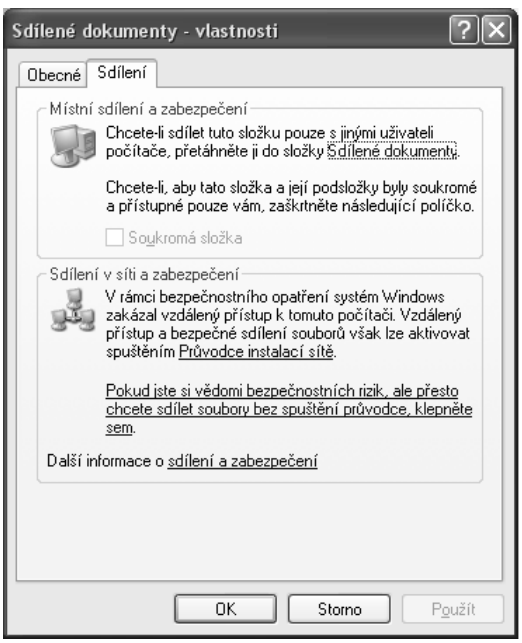
Ještě než se k *Průvodci* dostaneme, zmíním se o pojmu sdílení. Budeme se s ním setkávat velmi často, sdílení je věnována následující kapitola, ale setkáme se s ním již nyní. Sdílením rozumíme nabízení prostředků jednoho počítače ostatním PC v síti. Sdílený prostředek je tedy ten, s nímž mohou pracovat jiní uživatelé a přistupují k němu ze sítě. Sdílení je vlastně to, proč síť budujeme.

A nyní již k *Průvodci instalací sítě*. Spustit jej můžeme dvěma způsoby:

- První vidíme na obrázku *Počítače v síti*. Jde o řádek *Nastavit síť pro domácnost nebo malou kancelář* v okně *Místa v síti*.
- Druhý způsob se nám nabídne v případě, že chceme nastavit sdílení složky. Uděláme to tak, že klepneme pravým tlačítkem myši na ikonce složky a v menu vybereme *Sdílení a zabezpečení* (můžeme také zvolit *Vlastnosti* a přejít na záložku *Sdílení*). Zde vidíme dva skupinové rámečky: vrchní věnovaný *Místnímu sdílení* (opět více v následující kapitole) a spodní pro *Sdílení a zabezpečení v síti*. Pokud není síťové sdílení povoleno (po instalaci Windows XP je zakázáno), jsme na to ve spodním skupinovém rámečku upozorněni a je nám nabídnuta možnost sdílení aktivovat prostřednictvím *Průvodce instalací sítě*.

Samotný *Průvodce* má několik obrazovek:

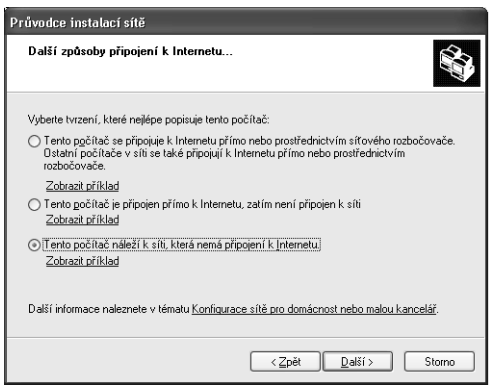
- první nás informuje o možnostech *Průvodce,* co vše můžeme jeho prostřednictvím ovlivnit,
- druhá upozorňuje na to, že před spuštěním *Průvodce* máme připojit PC k síti hardwarově (připojit síťový kabel, zapnout tiskárnu...),



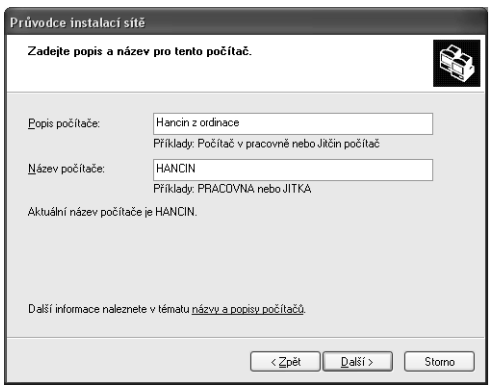
Obrázek 3.9: *Karta Sdílení*

- ve třetí obrazovce vybíráme způsob připojení k Internetu,
- čtvrtá obrazovka slouží k pojmenování počítače (a případnému zadání jeho popisu),
- na páté obrazovce zařazujeme počítač do pracovní skupiny,
- v šesté zatrhneme druhy sdílení, které chceme nabídnout ostatním v síti,
- sedmá obrazovka je souhrnem všech nastavení,
- osmá obrazovka pouze graficky znázorňuje průběh konfigurace,
- devátá slouží k vytvoření *Síťové instalační diskety* (o té blíže v Poznámce),
- poslední obrazovka slouží k ukončení průvodce.

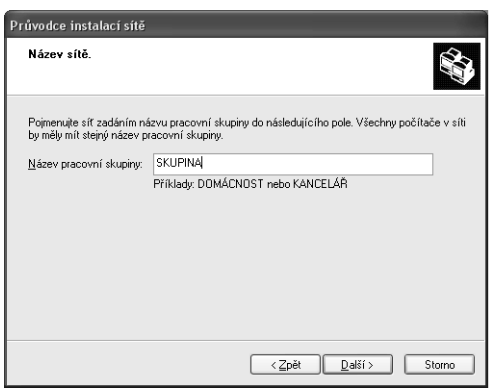
Poznámka: *Průvodce instalací sítě bychom měli spustit na každém počítači v síti. Můžeme to udělat přímo z Windows XP, nebo z jejich instalačního CD a poslední možností je právě Síťová instalační disketa. Tu můžeme spustit pouze z Windows 98, Windows 98 SE, Windows Millennium a Windows XP. Pokud budeme disketu používat (nutnost to není, konfiguraci můžeme provádět individuálně na každém PC), je nutné spustit Průvodce nejdříve na PC, kterým je síť připojena k Internetu.*



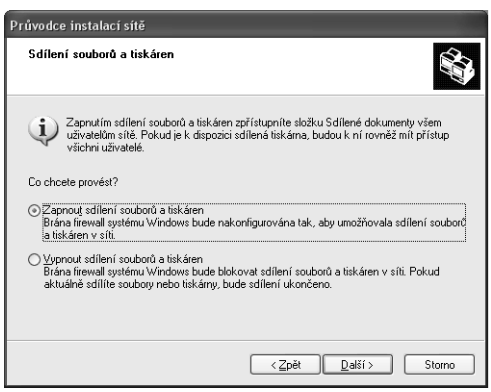
Obrázek 3.10: *Možnosti připojení k Internetu*



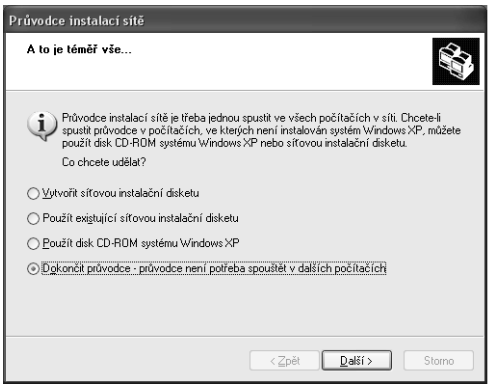
Obrázek 3.11: *Pojmenování PC*



Obrázek 3.12: *Přiřazení do pracovní skupiny*



Obrázek 3.13: *Povolení sdílení*



Obrázek 3.14: *Vytvoření Síťové instalační diskety*

Nastavení sdílení

Nyní již máme síť vytvořenou. Zbývá udělat to hlavní, určit které složky a tiskárny bude možné v síti sdílet a stanovit podmínky jejich sdílení. (Sdílené prostředky jsou, ty které budou k dispozici pro uživatele sítě.)

Pravidla sdílení složek vycházejí z použitého souborového systému. Úkolem souborového systému je organizovat ukládání souborů na disk (musí vědět kde je volné místo na disku, kde na disku najít soubor atd.). Současně si u každého souboru zaznamenává další informace: délku souboru, datum vzniku atd., mezi těmito údaji mohou být také informace o přidělování přístupových práv. V zásadě rozeznáváme dva souborové systémy:

- **FAT (File Allocation Table)** – je použita u Windows 98. Pro sdílení je důležité, že neumožňuje použití rozsáhlých oprávnění (kdo co může a nemůže). Ve Windows XP ji můžeme také použít, ale druhý systém NTFS je kvalitnější, a tak je lepší jej používat.
- **NTFS (New Technology System)** – řídí správu souborů ve Windows XP (a také v dřívějších Windows 2000). Mezi jeho hlavní přednosti patří práce s oprávněními. Ve Windows XP je tedy možné přesně definovat, kdo bude moci se složkou pracovat a co mu povolíme. Protože NTFS je výchozím souborovým systémem ve Windows XP, budeme se nadále věnovat konfiguraci sdílení založeného na NTFS.

V úvodu kapitoly se musíme ještě seznámit s edicemi Windows XP. Existují dvě, lišící se především z hlediska práce v síti:

- **Windows XP Home: je navržena** do domácností a malých sítí. Pracuje ve zjednodušeném režimu sdílení, méně náročném na správu (ale také méně bezpečném). Pracují-li Windows XP Home v síti peer to peer, může k jejich sdíleným složkám přistupovat kdokoliv ze sítě. Windows XP Home nemohou být začleněny do domény.
- **Windows XP Professional:** v síti peer to peer pracují také ve zjednodušeném režimu, ale lze je začlenit do domény, což s sebou přináší vyšší zabezpečení (povinné používání uživatelských účtů při práci s operačním systémem, větší škálu oprávnění, úplná práce se skupinami, možnost centrální správy v doméně atd.). Při práci v síti peer to peer lze navíc ověřovat přístupy ze sítě (vnější uživatel zde musí mít vlastní účet, nebo vstupovat prostřednictvím účtu Guest). Tato edice je určena především pro firmy, v nichž se předpokládá provoz v sítích.

Windows XP tedy mohou pracovat v síti peer to peer (obě edice) nebo klient server (ale zařazen do domény může být pouze počítač s operačním systémem Windows XP Professional). My si nejdříve ukážeme právě práci v síti peer to peer, neboli zjednodušené sdílení souborů.

Uživatel, skupina a uživatelský účet

Windows XP jsou víceuživatelským systémem, u jednoho počítače se může střídat několik uživatelů. Každému z těchto uživatelů operační systém zajišťuje určité soukromí: má vlastní nastavení pracovního prostředí (souborů, plochy atd.), má vlastní složku pro ukládání dat, navíc je možné definovat k jakým složkám bude mít uživatel přístup a co zde bude mít povoleno. Aby Windows XP jednotlivé uživatele od sebe oddělily, jsou zde zřizovány uživatelské účty. Každý, kdo chce s operačním systémem pracovat, musí mít ve Windows XP k dispozici vlastní uživatelský účet. Navíc se k PC mohou připojovat uživatelé ze sítě, do níž je počítač připojen. Některé prostředky počítače (především složky a tiskárny) mohou uživatelé používat společně – sdílet je . Sdílení rozeznáváme dvojí:

- Sdílení ***místní*** – pro uživatele střídající se u počítače. Ke sdíleným prostředkům přistupují ze stejného počítače.
- Sdílení ***v síti*** – pro uživatele, kteří využívají prostředků PC ze sítě. Ke sdíleným prostředkům přistupují z jiných počítačů – ze sítě.

Oba dva způsoby sdílení si jsou velmi podobné, my se logicky zaměříme především na sdílení ze sítě. Než se k popisu sdílení dostaneme, musíme se ještě seznámit s uživatelskými účty a profily, protože práce s nimi je základním předpokladem nastavování sdílení.

Uživatelský účet

Je záznamem v systémové databázi Windows XP, který je věnován jednomu uživateli (k účtu je vztažen také uživatelský profil). Bez uživatelského účtu není možné se k Windows XP přihlásit a začít s počítačem pracovat. Součástí účtu je uživatelské jméno a heslo, jimiž se do Windows XP přihlašujeme.

Ve Windows XP rozeznáváme tři základní druhy účtů:

- ***Účet správce počítače*** je nejvyšším typem účtu. Osoby přihlášené pod tímto účtem mohou instalovat software a přistupovat ke všem souborům a složkám v počítači (pokud správce přístup ke složce nemá, může převzít její vlastnictví). Dále mohou zřizovat, upravovat a mazat ostatní účty.
- ***Omezený účet*** je určen pro běžné uživatele. Ti mají přístup k programům, které již jsou v počítači nainstalovány, ale nemohou nainstalovat software ani hardware.
- ***Guest*** je určen pro uživatele, který nemá v daném počítači žádný uživatelský účet. Používá se především pro přístup ke sdíleným prostředkům počítače ze sítě. Budeme se mu ještě věnovat, ale předesílám, že je účtem nebezpečným a po instalaci Windows XP je zakázaný.

Poznámka: Třídy účtů jsou v podstatě skupinami, s kterými se ještě mnohokrát setkáme.

Uživatelský profil

Ke každému uživatelskému účtu patří jeden uživatelský profil, vytvořený při prvním přihlášení uživatele k počítači. Je uložen na místním pevném disku počítače ve složce *Documents and Settings*. Tady má každý profil kořenovou složku, v níž jsou uloženy další složky, určené k záznamu osobních údajů uživatele. Důležité je, že složky profilu jsou nepřístupné ostatním uživatelům PC (s výjimkou uživatele s oprávněním *Správce počítače*). Každý profil začíná složkou, která se jmenuje stejně jako uživatelský účet. Uvedeme alespoň základní přehled složek profilu.

- ***Uživatel – Dokumenty*:** vyhrazena pro ukládání dat uživatele. Ukládání sem mají přednastaveno všechny programy. Při práci se sdílením nás tato složka zajímá nejvíce.
- ***Nabídka Start*:** pro uložení programů v nabídce *Start*. Nabídka *Start* má dvě části: osobní a společnou. (Konfiguraci společné složky Start najdeme v *Documents and Settings\All Users\ Nabídka Start*).
- ***Oblíbené položky*:** sem se zapisuje nastavení oblíbených položek, které si uživatel zvolil.
- ***Plocha*:** k ukládání nastavení plochy uživatele (každý má tedy svoji plochu).

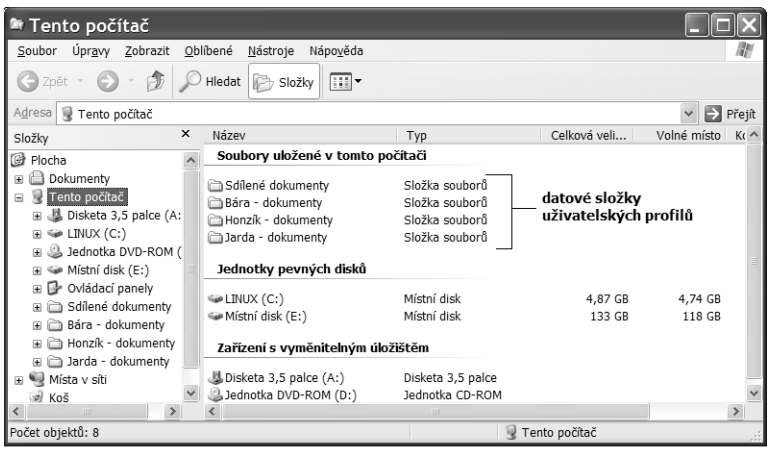
Obrázek 3.15: *Uživatelský profil uživatele Jarda*

Složek v uživatelském profilu je samozřejmě podstatně více, ukládají se sem dočasné soubory, nastavení aplikačních programů, záznamy potřebné pro práci s Internetem atd. Většinu složek používá operační systém, sdílení přidělujeme většinou pouze složkám datovým (hlavně složce *Dokumenty*).

Ve Windows XP navíc existuje speciální uživatelský profil *All Users*. Zde jsou uloženy záznamy společné všem uživatelům. Jde například o složku *Nabídka Start*, v níž najdeme ty programy, které se mají zobrazit všem uživatelům, je zde také složka *Plocha* s ikonami zobrazovanými pro všechny. Z hlediska sdílení dat je pro nás velmi zajímavá složka *Sdílené dokumenty*. Ta je připravená pro sdílení dat. Pokud chceme nabídnout nějakou složku pro ostatní uživatele, měli bychom použít právě *Sdílené dokumenty*.

Poznámka:

Poklepeme-li na ikonku Tento počítač, máme v pravé části okna k dispozici datové složky všech uživatelských profilů (včetně Sdílených dokumentů).



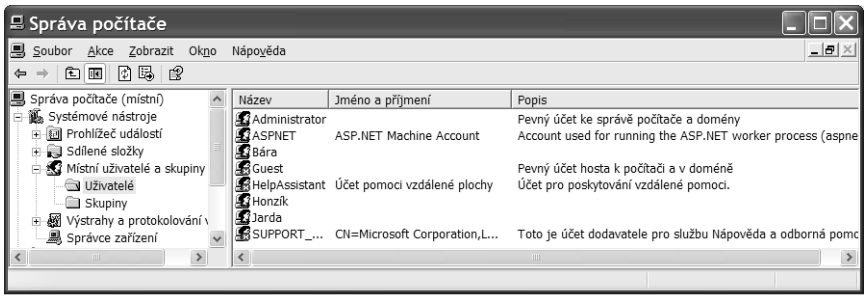
Obrázek 3.16: *Datové složky profilů*

Práce s uživateli

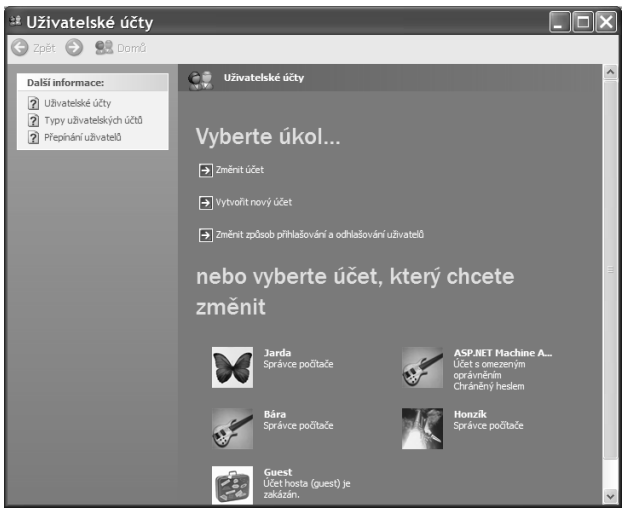
Ještě než začneme s popisem sdílení, shrneme si základní činnosti při práci s účty. Můžeme použít dvě metody:

- Práci s ovládacím panelem *Uživatelské účty* (*Start / Ovládací panely / Uživatelské účty*).
- Práci s konzolou MMC *Správa počítače*. (Pravé tlačítko myši na ikoně *Tento počítač / Spravovat / Místní uživatelé a skupiny / Uživatelé*). Jde o konzolu, která není přístupná ve Windows XP Home.

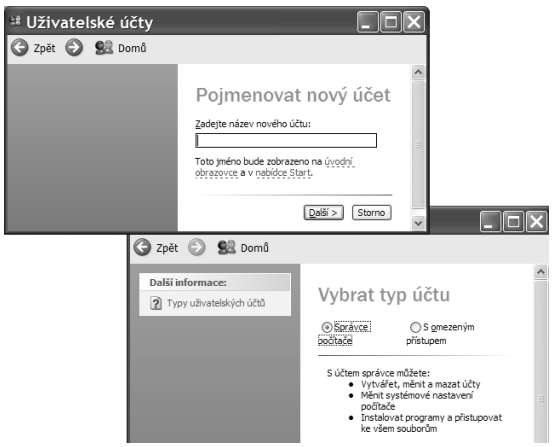
  Práce s ovládacím panelem *Uživatelské účty* je jednodušší, MMC konzola slouží k pokročilejší správě PC.



Obrázek 3.17: *MMC konzola Správa počítače*



Obrázek 3.18: *Ovládací panel Uživatelské účty*

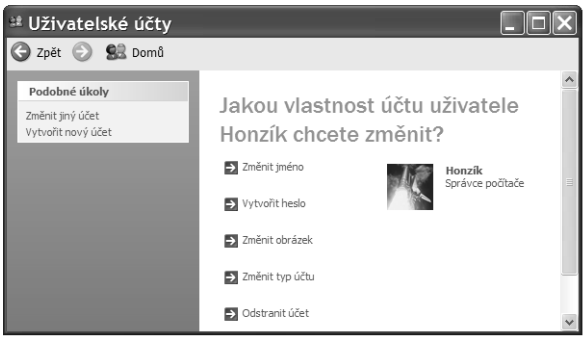


Obrázek 3.19: *Zřízení účtu*

Popíšeme si základní činnosti v obou panelech, nejdříve si přiblížíme práci v ovládacím panelu ***Uživatelské účty:***

- **Zřízení nového účtu** je poměrně jednoduché. V horní části ovládacího panelu vybereme *Vytvořit nový účet*, čímž spustíme průvodce se dvěma obrazovkami. V první účet pojmenujeme a ve druhé zadáme, zda nový účet bude *Správce počítače* nebo účtem *S omezeným přístupem*.
- **Nastavení vlastností účtu** – opět v horní části ovládacího panelu klepneme na řádek, tentokrát však *Změnit účet*. Co můžeme měnit, ukazuje obrázek. Zmíníme se pouze o nastavení hesla. To při zápisu nevidíme (kvůli utajení jsou znaky nahrazeny hvězdičkami), aby byl vyloučen překlep, zadává se heslo dvakrát.
- **Vymazání účtu** je dostupné z obrazovky sloužící ke změnám účtů. Pokud účet mažeme (volba *Odstranit účet*), objeví se dotaz na zachování souborů (viz obrázek *Mazání účtu*). Dotaz souvisí s uživatelským profilem. Pokud stiskneme tlačítko *Zachovat soubory*, zůstanou složky uživatelského profilu zachovány, v opačném případě se vymažou.

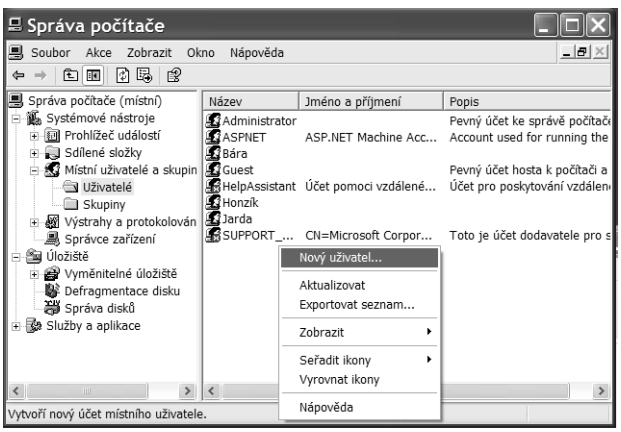
  Nyní budeme pokračovat výkladem o práci s uživatelskými účty v konzole MMC ***Správa počítače.*** Ta je určena k profesionálnější práci, neumožňuje konfiguraci grafických prvků a při mazání účtu ponechává na disku složky uživatelského profilu (a je dostupná pouze ve Windows XP Professional).



Obrázek 3.20: *Změna vlastností účtu*

Obrázek 3.21: *Mazání účtu*

- ***Zřízení nového účtu*** zahájíme klepnutím pravého tlačítka myši v okně *Správa počítače*, a v menu vybereme *Nový uživatel*. Otevřeme tak stejnojmennou obrazovku. Význam jejích voleb je patrný z obrázku (heslo se opět nezobrazuje, je nahrazeno hvězdičkami). Při tomto způsobu práce máme k dispozici rozšířené možnosti pro práci s heslem (jde o spodní část okna). Význam voleb je opět patrný z obrázku, pozastavíme se u prvního a posledního řádku: zatrhneme-li *Při dalším přihlášení musí uživatel změnit heslo*, bude uživatel při prvním přihlášení vyzván ke změně hesla. Jeho heslo tedy nebude znát nikdo, ani administrátor. Výsledkem zatržení *Účet je zablokován* je to, že se k existujícímu účtu nemůžeme přihlásit (i když existuje účet i jeho uživatelský profil). Zakázaným je na našich obrázcích účet *Guest*.



Obrázek 3.22: *Zřizování nového účtu*

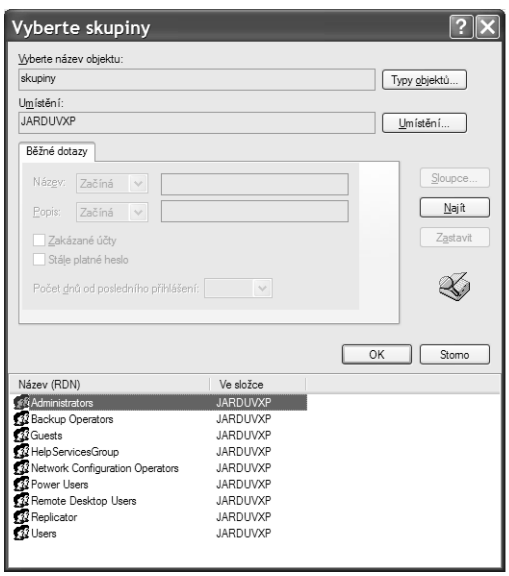
Obrázek 3.23: *Vlastnosti nového účtu*

- ***Nastavení vlastností účtu*** zahájíme poklepem na existující účet. Otevřeme tím obrazovku s vlastnostmi účtu. Ta má tři záložky: na záložce *Obecné* měníme základní údaje o účtu (popsané v předešlém odstavci). Záložka *Je členem* je pro nás zajímavější. Umístíme sem skupinu, jíž bude uživatel členem a jejíž vlastnosti tak přebere. Skupinu přidáme postupným stiskem tlačítek: *Přidat / Upřesnit* (obrazovka *Vyberte skupiny*) a *Najít* (obrazovka *Vyberte skupiny*). Poté již skupinu vybereme. (Krátká zmínka o skupinách je v následující odrážce). Poslední záložku *Profil* použijeme tehdy, pokud chceme uživatelský profil uložit jinam, než to standardně dělají Windows XP. Časté je ukládání profilu například na síťový server (složky má pak uživatel přístupné z libovolného síťového počítače). V sítích peer to peer se však tato záložka používá velmi málo.

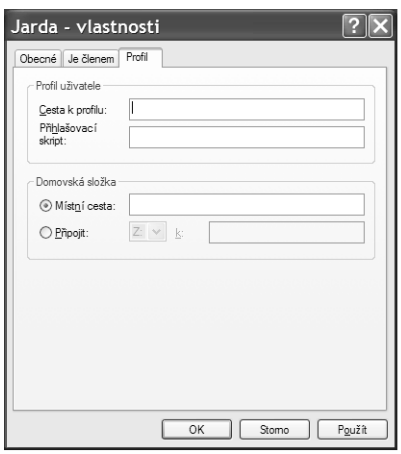
- **O skupinách** skupiny jsou podstatně důležitější (a používanější) u sítí klient/server. V příslušných kapitolách se jejich popisu budeme věnovat podrobněji. Nyní alespoň stručně. Skupina je tvořena několika uživatelskými účty, ale v zásadě je samostatným objektem. Lze jí tedy například přidělovat oprávnění, která se potom přenesou také na její členy. Microsoft ve svých Windows zřídil určité skupiny s typickými vlastnostmi. Pokud do takovéto skupiny přiřadíme uživatelský účet, přebere tento účet její vlastnosti. Předdefinované skupiny vidíte na obrázku *Výběr skupiny*. Pro práci v síti peer to peer (ale především pro práci na jednotlivém PC) mají význam skupiny:
  - *Administrators* jejíž členové jsou správci počítače. V ovládacím panelu *Uživatelské účty* se budou zobrazovat jako *Účet správce počítače*.
  - *Users jehož* příslušníci mají omezená práva pro práci. V ovládacím panelu *Uživatelské účty* se budou zobrazovat jako *Omezený účet*.

Obrázek 3.24: *Záložka Obecné*

Obrázek 3.25: *Záložka Je členem*



Obrázek 3.26: *Výběr skupiny*



Obrázek 3.27: *Záložka profil*

- **Vymazání účtu** je velmi snadné, kurzorem vybereme účet a klávesou *Delete* jej smažeme. Znovu upozorňuji na to, co je velmi důležité: mazáním uživatelského účtu tímto postupem neodstraníme složky uživatelského profilu! Při mazání je tedy vhodnější používat ovládací panel *Uživatelské účty*.

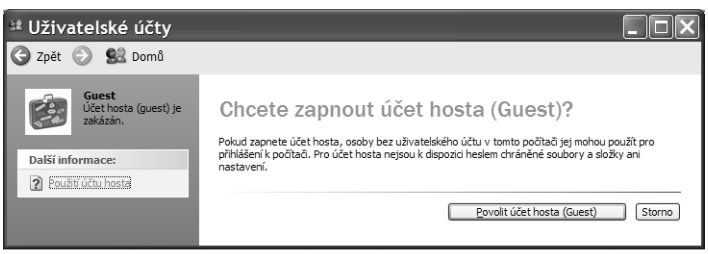
Tip: Jak to vypadá s uživatelskými účty, zjistíme v obrazovce Profily uživatelů (pravé tlačítko myši na ikoně Tento počítač / Vlastnosti, přejdeme na záložku Upřesnit, stiskneme tlačítko Nastavení – najdeme ho ve skupinovém rámečku Profily uživatelů). Zde vidíme všechny uživatelské profily. Pokud existuji složky uživatelského profilu, k nimž nepatří žádný účet, logicky to operační systém považuje za chybu. V obrazovce Profily uživatelů je účet, k němuž nepatří profil, označen jako Neznámý účet. Složky uživatelského profilu, k nimž účet nepatří, můžeme smazat tlačítkem Odstranit.

Obrázek 3.28: *Neznámý účet*

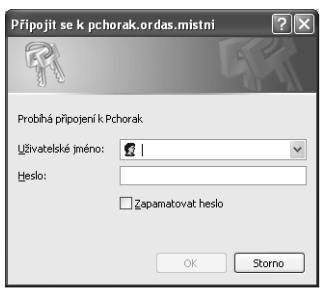
Přístup k počítači

Chceme-li přistupovat k počítači ze sítě (a sdílet jeho složky), máme k dispozici tři možnosti, jak to udělat. Jde o různé kombinace použití uživatelských účtů (především budeme hovořit o nejrozšířenější edici – Windows XP Professional).

1. Povolení uživatelského účtu *Guest* (host). Povolený účet hosta otevře přístup k počítači i těm, kteří zde nemají vlastní účet. Potenciálně jde o poměrně nebezpečný prvek, proto je po instalaci Windows XP účet *Guest* zakázán.
2. Na počítači (či počítačích) je stejný uživatelský účet, jako na počítači vzdáleném. Pak se ke vzdálenému PC také nemusíme hlásit, přihlašujeme se totiž k účtu, k němuž jsme již jednou přihlášeni.
3. Poslední možnost je standardním postupem. Na vzdáleném počítači jsou jiné účty než na našem a je zde zakázán účet *Guest*. Pak jsme při přihlášení vyzváni k zadání uživatelského jména a hesla, ke vzdálenému PC se přihlásíme a můžeme zde pracovat (podle oprávnění patřících k našemu účtu). Pozor, platí zde bezpečnostní omezení: k účtu, k němuž se přihlašujeme, musí existovat heslo! (Přihlásit se ze sítě k uživatelskému účtu s prázdným heslem není možné.)



Obrázek 3.29: *Povolení účtu Guest*



Obrázek 3.30: *Přihlášení ke vzdálenému PC*

Poznámka:

- *Edice Windows XP Home má možnosti přístupu ze sítě značně omezeny. K dispozici je obdoba první možnosti – ke sdíleným složkám PC se dostane každý, není nutné zadávat uživatelské jméno ani heslo!*
- *Windows XP Professional mají také jedno omezení: ze sítě se současně může připojit maximálně 10 uživatelů. Další jsou odmítnuti.*

Tabulka 3.1: Shrnutí možností přihlašování

	metoda	výhody	nevýhody	poznámka
1	**Povolení účtu Guest**	Snadný přístup všech	Snadný přístup všech	Výrazně snižuje bezpečnost
2	**Přihlášení ze stejného účtu**	Snadný přístup	Nižší bezpečnost	Je možné použít pro přístup k Windows XP z Windows 9x
3	**Standardní**	Standardní zabezpečení přístupu	Při přístupu musíme zadat jméno a heslo	Účty, k nimž se hlásíme, nesmějí mít prázdná hesla.

Tip: Druhá možnost, kdy se ke vzdálenému počítači hlásíme z již existujícího účtu, je jediným způsobem, jak se dostat ke sdíleným prostředkům počítače s Windows XP ze starých operačních systémů Windows 9x.

Sdílení složek v síti

Konečně již víme vše potřebné o uživatelských účtech a jejich uživatelských profilech. Můžeme se tedy věnovat síťovému sdílení.

Již víme, že kdo nemá ve Windows XP svůj účet, nemůže se sem přihlásit – ani ze sítě, ani místně (s výjimkou síťového přístupu k Windows XP Home, nebo přístupu k PC s otevřeným účtem *Guest*). Víme také že Windows XP rozeznávají dva způsoby sdílení složek:

- **Místní:** které pojednává o tom, kam budou moci přistupovat uživatelé lokální, střídající se u počítače. Ti se do systému hlásí svým účtem, podmínkou místního sdílení tedy je existence uživatelského účtu!
- **Síťové:** platící pro všechny, kteří do Windows XP vstoupí z vnějšku (ze sítě).

Postup při nastavování sdílení je následující: ťukneme pravým tlačítkem myši na složce, vybereme *Sdílení a zabezpečení…"* Dostaneme se na kartu *Sdílení,* ta má dvě části – vrchní polovina je určena ke konfiguraci místního sdílení, ve spodní povolujeme sdílení ze sítě.

Pro **místní sdílení** platí poměrně jednoduché pravidlo. Pokud chceme složku nabídnout ostatním, musíme ji umístit ve složce *Sdílené dokumenty*. Uvidíme ji po otevření ikony *Tento počítač*. Ve skutečnosti je umístěna v uživatelském profilu *All Users.*

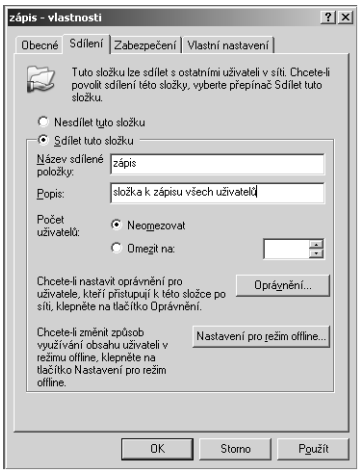
Z hlediska místního sdílení můžeme označit složku jako *soukromou.* O co jde: každý uživatel má vlastní složky umístěny ve svém uživatelském profilu (přesně složce *Disk:/Documents and Settings/Přihlašovací jméno*). Obsah těchto složek je před ostatními osobami chráněný, ale každý správce počítače se k němu bez obtíží dostane. Chceme-li složku zabezpečit důkladně (i před správci počítače), musíme ji označit jako *Soukromou složku.* Zatrhneme tedy okénko *Soukromá složka.* Od této chvíle může do složky jen jeden uživatel – ten, který si ji označil jako soukromou. Jako

soukromou můžeme označit pouze složku ve svém uživatelském profilu! (Tedy ve složce *Disk:/Documents and Settings/Přihlašovací jméno*.)

Síťového (vnějšího) sdílení se týká spodní polovina karty – skupinový rámeček *Sdílení v síti a zabezpečení*" Ten má dvě zaškrtávací políčka:

- Zaškrtnutím políčka *Složka sdílená v síti* zveřejníme složku ostatním počítačům v síti.
- Políčko *Povolit uživatelům v síti měnit mé soubory* rozhoduje o tom, co v naší složce povolíme. Pokud je políčko prázdné, mohou ostatní v naší složce pouze číst. Do souborů složky nemohou zapisovat, nemohou sem ukládat a soubory nemohou ani mazat. Jestliže však políčko zaškrtneme, mají síťoví uživatelé nad složkou úplnou kontrolu.

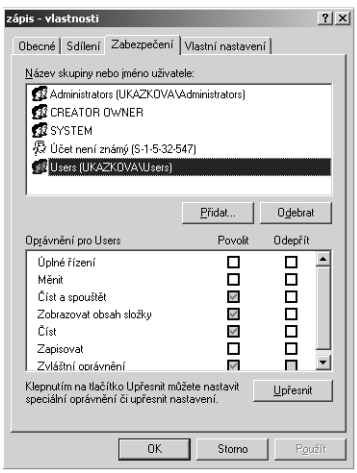
Poznámka: Mezi oběma políčky je řádek „Název sdílené složky". Pod zde zapsaným názvem je složka viditelná ze sítě. Ve jménu sdílené složky nemohou být mezery a délka názvu je omezena na 12 znaků.



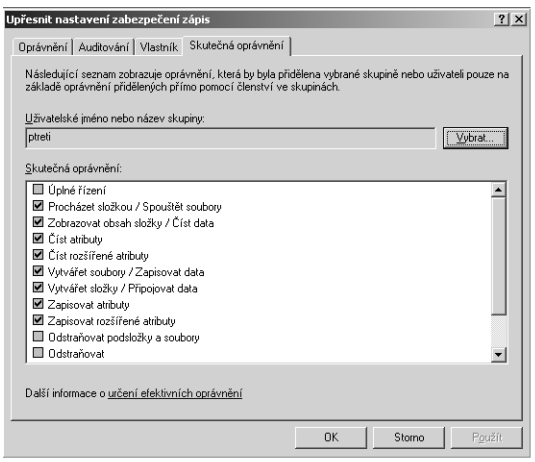
Obrázek 3.31: *Karta Sdílení*

Pokud není spodní polovina karty *Sdílení v síti a zabezpečení* dostupná, není síť nakonfigurována a Windows XP nabídnou spuštění *Průvodce instalací sítě*, kterého jsme si již popsali ve stejnojmenné kapitole.

Ve Windows XP Professional je dostupné podstatně dokonalejší a podrobnější sdílení souborů. To se automaticky zapíná po přiřazení počítače do domény Windows Serveru. V síti peer to peer jej můžeme použít také, ale musíme jej ručně zapnout. Otevřeme ikonu *Tento počítač*, v menu *Nástroje* vybereme M*ožnosti složky* a přejdeme na záložku *Zobrazení*. Sdílení přepínáme v řádku *Použít zjednodušené sdílení souborů*. Pokud není řádek zaškrtnut, budeme pracovat s kvalitnějším sdílením.



Obrázek 3.32: *Přepínání sdílení*



Obrázek 3.33: *Dvojí sdílení*

Srovnání možností variant sdílení ukazuje obrázek *Dvojí sdílení*. Je-li zjednodušené sdílení vypnuto, máme daleko podrobnější možnosti jak sdílení definovat. Tímto způsobem pracuje se sdílením serverový operační systém Windows Server. Podrobnosti o sdílení tímto způsobem (jaká oprávnění můžeme použít, jak je nastavit, jak se dědí, co je to vlastnictví atd.) najdete v kapitole *Windows Server 2003*.

Základní způsoby sdílení

Z předešlého výkladu je zřejmé, že sdílení je pojem, kterým definujeme přístup jak místní, tak síťový. Následující tabulka ukazuje jaké varianty sdílení jsou dostupné a jak je můžeme kombinovat. V tabulce vidíme skupinu *Everyone* (všechny legálně přihlášené), *Vlastníka* (toho, kdo složku nebo soubor vytvořil) a *Administrátora* (správce systému), objekty, s nimiž se u zjednodušeného sdílení setkáme.

Tabulka 3.2: Varianty sdílení

Úroveň	Everyone (Místní sdílení)	Vlastník	Administrators	Everyone (Sdílení ze sítě)
1	n/a	Úplné řízení	n/a	n/a
2	n/a	Úplné řízení	Úplné řízení	n/a
3	Čtení	Úplné řízení	Úplné řízení	n/a
4	Čtení	Úplné řízení	Úplné řízení	Čtení
5	Změna	Úplné řízení	Úplné řízení	Úplné řízení

Úroveň 1

Vlastník složky zde má oprávnění ke čtení a zápisu. Žádný jiný uživatel nemůže ze složky číst ani zde zapisovat. Všechny podsložky zůstávají soukromé (pokud nezměníte oprávnění nadřízené složky). Přístup ze sítě není povolen.

Konfiguraci na tuto úroveň provedete:

1. Klepněte na složku pravým tlačítkem myši a pak klepněte na příkaz *Sdílení a zabezpečení*.
2. Zaškrtněte políčko *Soukromá složka* a pak klepněte na tlačítko *OK*. (Označit složku jako soukromou můžeme pouze u uživatelského účtu v jeho vlastní složce *Dokumenty)*.

Úroveň 2 (výchozí)

Vlastník složky a správci místního počítače mají oprávnění ke čtení a zápisu. Žádný jiný uživatel nemůže ze složky číst ani zde zapisovat. Jde o výchozí nastavení pro všechny složky a soubory ve složce *Dokumenty* jednotlivých uživatelů. Přístup ze sítě není povolen.

Konfiguraci na tuto úroveň provedete:

1. Klepněte pravým tlačítkem myši na složku a pak klepněte na příkaz *Sdílení a zabezpečení*.
2. Zkontrolujte, zda nejsou zaškrtnuta políčka *Soukromá složka* a *Složka sdílená v síti*, a pak klepněte na tlačítko OK.

Úroveň 3

Do složky mají přístup všichni místní uživatelé. Správci místního počítače mohou soubory číst, zapisovat do nich a odstraňovat soubory ve složce *Sdílené dokumenty*. Uživatelé s *omezeným přístupem* mohou pouze číst soubory ve složce *Sdílené dokumenty*. V systému Windows XP Professional je k dispozici také skupina *Power Users*. Její členové zde mohou číst, zapisovat a odstraňovat libovolné soubory (stále jde o složku *Sdílené dokumenty*). Přístup ze sítě není povolen.

Konfiguraci na tuto úroveň provedete:

Zkopírujete nebo přesunete soubor nebo složku do složky *Sdílené dokumenty* ve složce *Tento počítač*.

Úroveň 4

Do složky mají přístup všichni (místní i síťoví) uživatelé. Každý zde může číst, ale pouze vlastník a administrátor mohou také měnit a mazat soubory.

Konfiguraci na tuto úroveň provedete:

1. Klepněte pravým tlačítkem myši na složku a pak klepněte na příkaz *Sdílení a zabezpečení*.
2. Klepnutím zaškrtněte políčko *Složka sdílená v síti*.
3. Klepnutím zrušte zaškrtnutí políčka *Povolit uživatelům v síti měnit mé soubory* .

Úroveň 5

Tato úroveň je nejdostupnější a nejméně zabezpečenou. Přístup do složky mají všichni uživatelé (jak místní, tak síťoví) a všichni zde mohou číst soubory, zapisovat do nich nebo je odstranit.

Konfiguraci na tuto úroveň provedete:

1. Klepněte pravým tlačítkem myši na složku a pak klepněte na příkaz *Sdílení a zabezpečení*.
2. Klepnutím zaškrtněte políčko *Složka sdílená v síti* a pak klepněte na tlačítko *OK*.

Poznámka: Veškerá místní oprávnění, která platí pro skupinu Everyone, zahrnují účet Guest.

Přístup ke sdíleným složkám

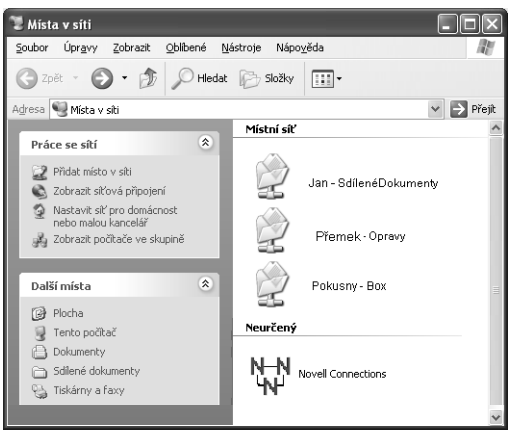
Nyní si řekneme jak používat složky, či tiskárny jiných počítačů, které jsme nasdíleli (nabídli ostatním). Přesná poloha síťového zdroje je popsána konvencí *UNC (Uniform Naming Conventions Names)*. Uvidíme ji na obrázcích, ale přesto si řekněme, že platí: popis sdíleného prostředku v síti začíná dvěma zpětnými lomítky. Pak následuje jméno počítače, další zpětné lomítko, jméno složky, zpětné lomítko atd. Windows naštěstí nahrazují UNC grafickými prvky, takže je UNC spíše pomocnou informací.

Ke sdíleným složkám vzdáleného počítače můžeme přistupovat několika způsoby: Postupně si je najdeme *v Průzkumníkovi*, či se k nim proklepeme přes ikonku *Místa v síti*. Další variantou je *Mapování*, kdy se vzdálená složka jeví jeden z disků našeho počítače.

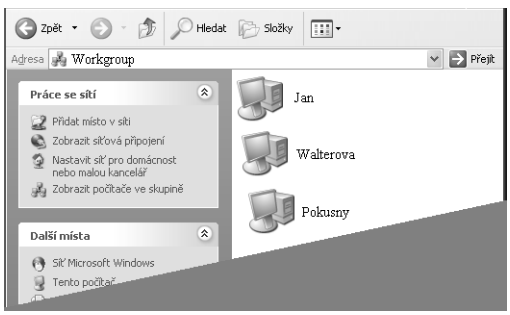
Přístup ke sdíleným složkám přes Místa v síti

Po otevření ikony *Místa v síti* uvidíme typické okno Windows XP, které má na levé straně panel pro ovládání. V pravém, větším vidíme *Místa v síti* (zástupce na složky jiných PC), případně se zde objevují další síťové prvky (skupiny a počítače). Pro práci v síti jsou důležité tyto řádky:

- ***Zobrazit síťová připojení:*** uvidíme jednotlivá síťová připojení (ať síťovou kartou či modemem). Následně můžeme upravovat jejich vlastnosti (např. přes pravé tlačítko myši).
- ***Nastavit síť pro domácnost nebo malou kancelář:*** spustí *Průvodce instalací sítě*.
- ***Zobrazit počítače ve skupině:*** zobrazí všechny počítače ve stejné skupině jako je náš PC.

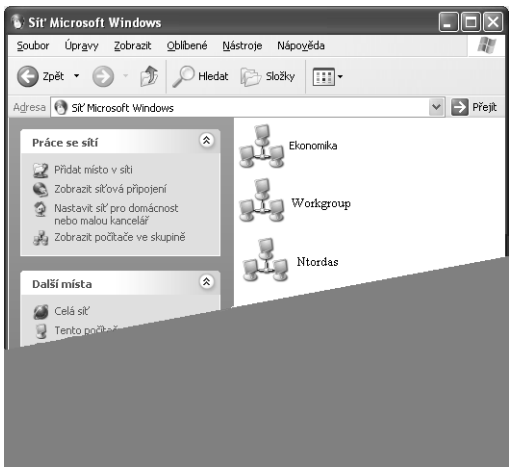


Obrázek 334: *Místa v síti*

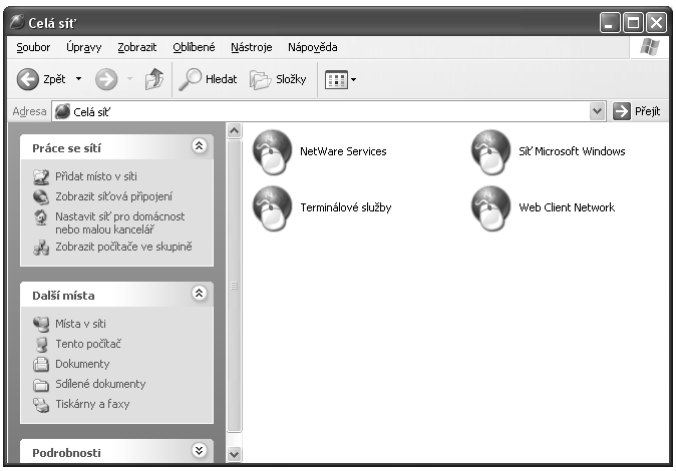


Obrázek 335: *Počítače ve skupině Workgroup*

Jestliže zobrazíme *Počítače ve skupině*, objeví se v levém pruhu další volba *Síť Microsoft Windows*. Jejím otevřením uvidíme skupiny v naší síti. Máme-li zobrazeny skupiny sítě, zpřístupní se v levém pruhu menu řádek *Celá síť*. Poklepáním na něj zobrazíme celou síť (např. také servery Novell).



Obrázek 3.36: *Skupiny v síti Microsoft Windows*



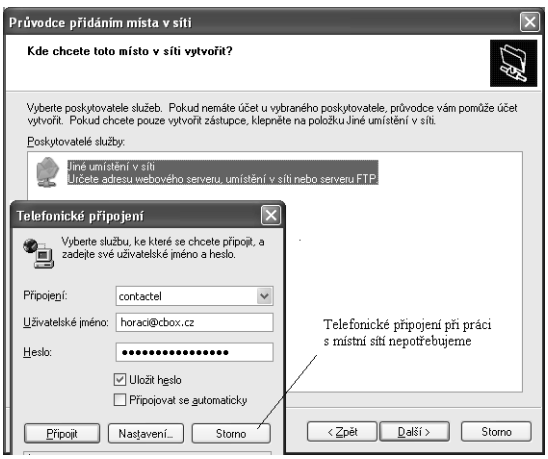
Obrázek 3.37: *Celá síť*

Poznámka: *Ikonu Místa v síti umístíme na Plochu stejným způsobem jako ikonu Tento počítač (klepnem pravým tlačítkem myši na Ploše / Vlastnosti / karta Plocha / tlačítko Vlastní nastavení plochy).*

Místa v síti

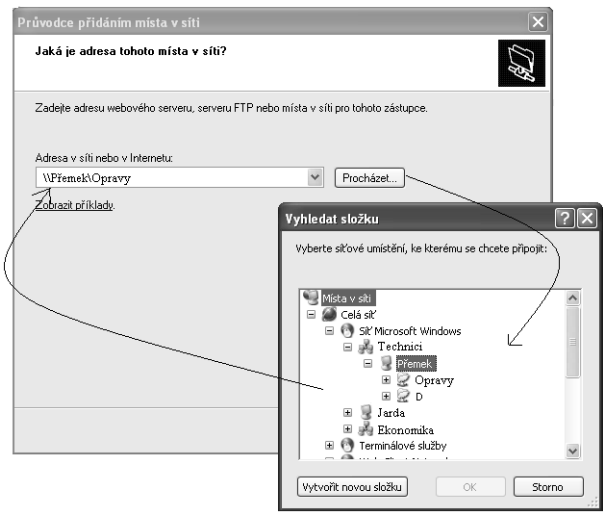
Předešlý odstavec byl věnován vstupu do sítě prostřednictvím ikony *Místa v síti*. Samotná *Místa v síti* jsou seznamem zástupců reprezentujících sdílené složky vzdálených počítačů, tiskáren a dalších prostředků v síti. Po otevření sdíleného síťového prostředku se zástupci vytvoří automaticky. Přístup ke sdílenému prostředku vzdáleného počítače (můžeme vytvořit také ručně):

- Na obrazovce *Místa v síti* (otevřeme ji poklepáním levým tlačítkem myši na ploše) klepneme v levé části obrazovky (v menu) na řádek *Přidat místo v síti*.
- Odstartujeme tak *Průvodce přidáním místa v síti*, který nás přivítá svou první obrazovkou.
- Windows XP chápou pod pojmem *Síť* vše, k čemu je možné se připojit. Po klepnutí na tlačítko *Další* Windows prozkoumají všechna instalovaná síťová připojení. Tvar další obrazovky pak závisí na tom, jaká síťová připojení používáme. Máme-li například definováno telefonické připojení, nabídnou jeho spuštění (tlačítkem *Storno* můžeme tuto možnost odmítnout). Při vytváření síťového zástupce místní sítě budeme používat řádek *Jiné umístění v síti*.

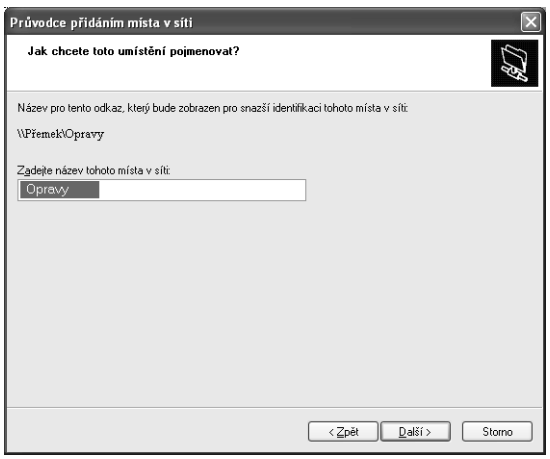


Obrázek 3.38: *Druhá obrazovka s oknem telefonického připojení*

- Dostaneme se do třetí obrazovky *Průvodce*. Zde je nejdůležitější řádek *Adresa v síti nebo v Internetu*. Sem se vkládá UNC adresa místa, na které bude náš zástupce ukazovat. UNC pravidla jsou však náročná na zápis, proto je mnohem jednodušší stisknout tlačítko *Procházet* a k dotyčnému místu se „proklepat" myší. Poklepáním levého tlačítka myši na cílové složce (v okně *Vyhledat složku*) se UNC adresa vloží do řádku automaticky.
- V předposlední obrazovce našeho zástupce pojmenujeme, poslední (pouze informativní) obrazovka průvodce ukončí.



Obrázek 3.39: *Výběr Místa v síti*



Obrázek 3.40: *Pojmenování místa v síti*

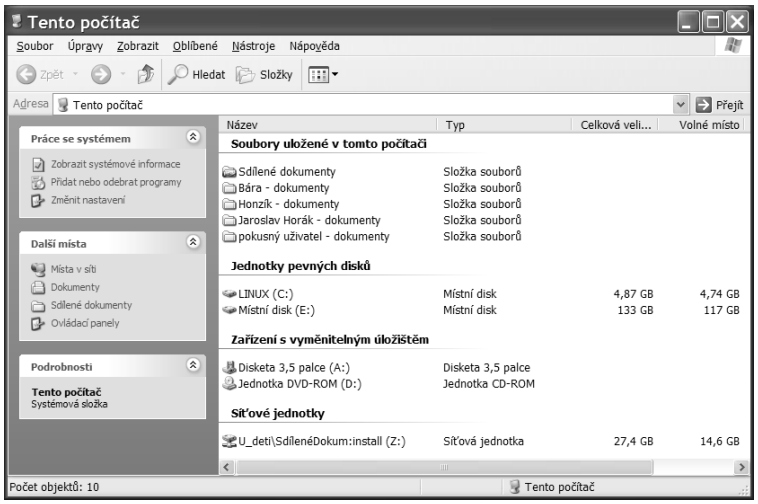
Přístup ke sdíleným složkám prostřednictvím mapování

Pokud určité složky cizích počítačů používáme velmi často, můžeme si je tzv. namapovat. Princip mapování je velmi jednoduchý – sdílené složce jiného počítače přiřadíme logické jméno disku (např. G:). Tento logický disk pak najdeme na našem počítači (v *Průzkumníkovi*, nebo po otevření ikony *Tento počítač*) mezi skutečnými disky. Výhoda je jasná – namapované zdroje nemusíme v síti pracně vyhledávat.

Příklad jednoduchého mapování ukazuje obrázek. Vidíme zde:

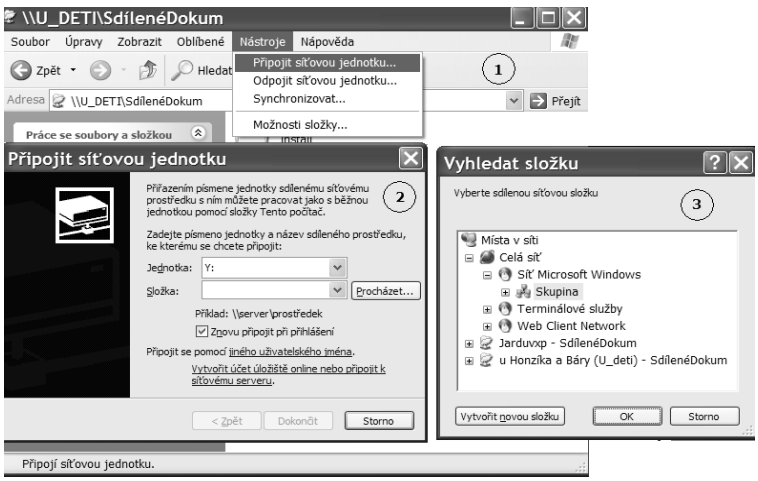
- ***Soubory uložené v tomto počítači:*** jde o složky *Dokumenty* jednotlivých uživatelských profilů, určené pro ukládání uživatelských souborů.
- ***Jednotky pevných disků:*** pevné disky počítače.
- ***Zařízení s vyměnitelným úložištěm:*** jsou zařízeními pro přenos dat. Na příkladu vidíme ta běžná, disketovou mechaniku a pevný disk.
- ***Síťové jednotky:*** to jsou složky (nebo disky) vzdálených počítačů. Přistupujeme k nim prostřednictvím mapování, a proto je vidíme jako tzv. *Síťové jednotky*. Na našem příkladu je pod písmenem *Z:* mapována složka *install,* umístěná ve složce *SdílenéDokum* počítače *U_deti*.

Zadání vlastního mapování je poměrně jednoduché. V *Průzkumníkovi,* či *Místech v síti,* nebo v *Tomto počítači* klepneme na *Nástroje* (v liště menu) a použijeme volbu *Připojit síťovou jednotku*. Otevřeme tak stejnojmenné okno a v něm v řádku *Jednotka* vybereme logické jméno připojované jednotky. Do řádku *Složka* můžeme zapsat UNC cestu sdíleného zařízení, pohodlnější však je použít tlačítko *Procházet*, jímž si otevřeme okno *Vyhledat složku*. Zde složku vyhledáme a stiskem tlačítka *OK* namapujeme k našemu počítači.

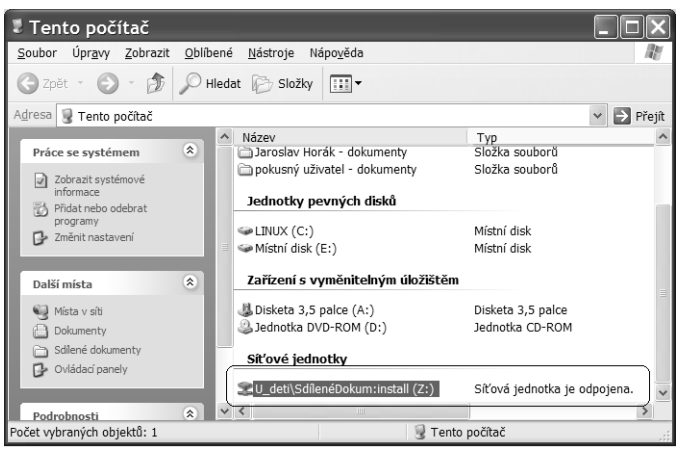


Obrázek 3.41: *Namapované disky*

Všimněte si zaškrtávacího políčka *Znovu připojit při přihlášení*. Pokud je zatrženo, bude mapovaný disk hledán a automaticky mapován při startu Windows XP. Bude-li počítač, jehož složky jsou namapovány zapnut, disk se připojí automaticky. Jestliže však zapnut nebude, mapování se odpojí.



Obrázek 3.42: *Mapování vzdálené složky*



Obrázek 3.43: *Mapování nebylo obnoveno*

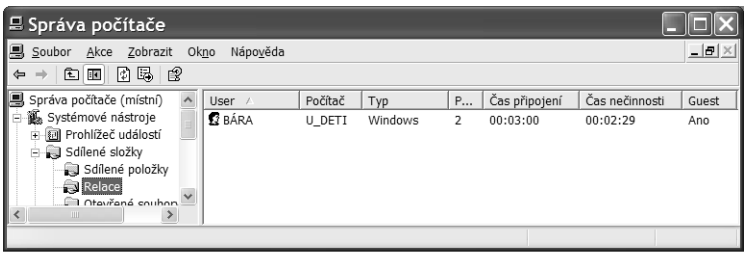
Poznámka: *V principu se mapování velmi podobá místům v síti. Místo v síti je však pouhým zástupcem, kdežto namapovaná složka je pro operační systém skutečně dalším diskem. Proto se mapování používá zejména tehdy, když chceme ze vzdáleného počítače spouštět programy. V mnoha případech se pak operačnímu systému jeví tento vzdáleně načítaný program jako program místní a operační systém s ním bez problémů spolupracuje.*

Kdo pracuje v mých složkách?

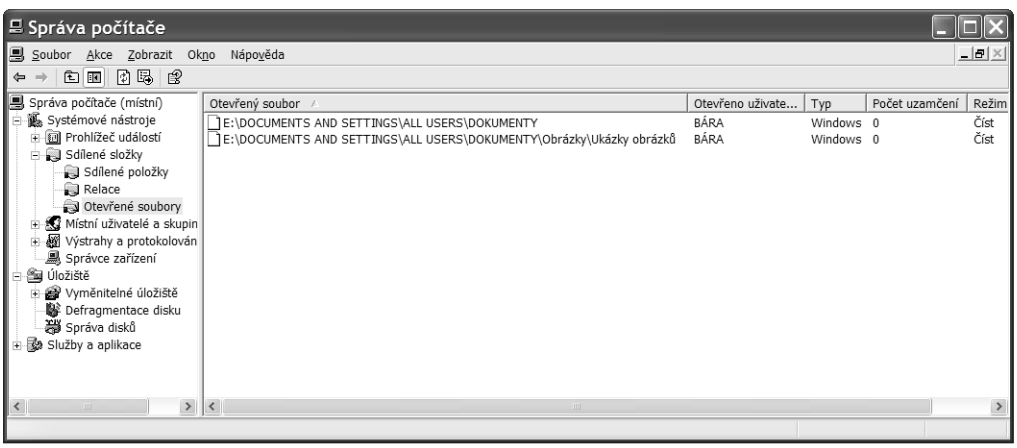
O tom, kdo ze sítě vstoupil do našich sdílených složek, nás informuje konzola *Správa počítače* (pravé tlačítko myši na ikoně *Tento počítač / Sdílené složky*). Klepneme-li v levém okně obrazovky na *Relace*, vidíme v pravé části konzoly uživatele, kteří se serverem pracují. Po umístění kurzoru na *Otevřené soubory* spatříme soubory s nimiž pracují vnější uživatelé našeho PC.

Informace o tom, kdo má na našem PC otevřené soubory, je důležitá z několika důvodů:

- předně je dobré vědět kdo „cizí" je v našem počítači a co zde dělá,
- při vypínání PC můžeme vzdáleně připojené uživatele násilně odpojit a způsobit jim tak ztrátu dat.



Obrázek 3.44: *Relace vnějšího uživatele*



Obrázek 3.45: *Vnějším uživatelem otevřené soubory*

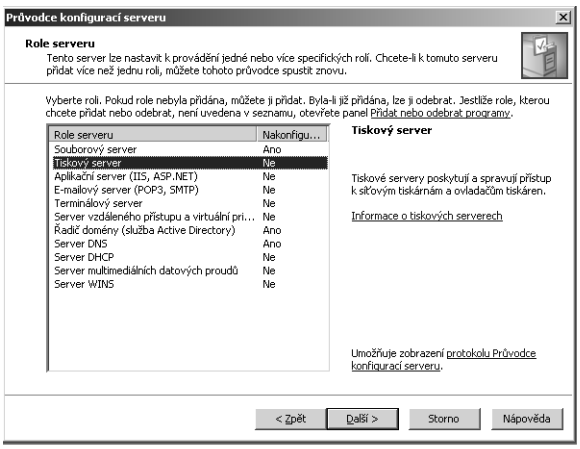
Poznámka*: Konzola Správa počítače je dostupná pouze ve Windows XP Professional.*

Sdílení tiskáren

Mimo složek jsou dalším často sdíleným prostředkem v sítích tiskárny. Výhoda společné tiskárny je jasná – jedna tiskárna slouží několika uživatelům. V zásadě existují dva způsoby jak tiskárnu nabídnout ostatním:

1. Prostřednictvím lokálního portu některého z počítačů sítě. Společná (sdílená) tiskárna je připojena k jednomu z počítačů v síti.
2. Pomocí print serveru. Společná tiskárna je připojena přímo do sítě. Připojení zprostředkuje hardwarové zařízení – print server.
3. Často je print server uvnitř tiskárny. Tiskárna se pak připojuje přímo k síti vlastní síťovou kartou.

Všechny metody řeší základní problém: co dělat, když chce současně tisknout více počítačů (přesněji jejich uživatelů) na jednu tiskárnu? Tehdy – při souběhu tiskových úloh se uplatňuje *tisková fronta*. Tisky jsou seřazeny jeden za druhý a tisknou se postupně. V prvním případě spravuje tiskovou frontu operační systém, v druhém print server.



Obrázek 3.46: *Varianty připojení síťové tiskárny*

Sdílení tiskárny prostřednictvím síťového PC

V malých sítích se s tímto řešením setkáme častěji. Tiskárna je v tomto případě připojena do místního portu některého síťového počítače. Jde vlastně o normální lokální připojení tiskárny, jaké se používá u nesíťových počítačů. Tiskárně je pak přiřazeno sdílení, díky čemuž ji vidí také ostatní uživatelé, mohou si ji nainstalovat a začít používat.

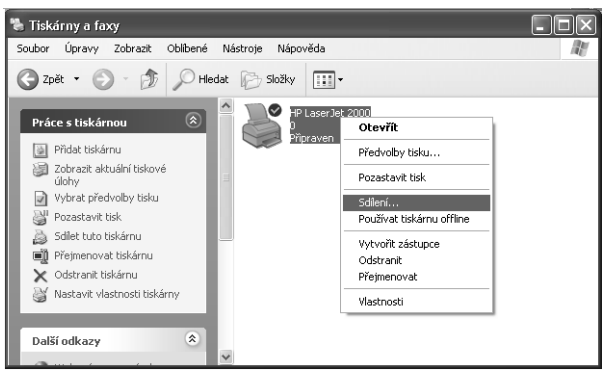
Jde o jednoduché a levné řešení, u malých sítí často používané. Na počítači se síťovou tiskárnou může samozřejmě kdokoliv pracovat. Abychom mohli tisknout, musí být počítač zapnutý, jinak by společná tiskárna nebyla v síti viditelná.

Tiskárnu připojíme k počítači běžným způsobem. Počítač a tiskárnu spojíme kabelem (dnes to bude kabel USB, starším řešením je kabel paralelní), nainstalujeme ovladač a můžeme tisknout. Jde o běžné lokální připojení tiskárny k PC.

Nastavení sdílení

Jestliže při instalaci tiskárny k počítači postupujeme běžným způsobem, je zveřejnění tiskárny (povolení sdílení) v síti již složitější - sdílení tiskárny zapneme takto:

- Přes *Start/Ovládací panely/Tiskárny a faxy* vyvoláme ovládací panel *Tiskárny a faxy*.
- Zde vidíme nainstalované tiskárny. Klepneme pravým tlačítkem myši na tiskárně a v menu vybereme *Sdílení*.



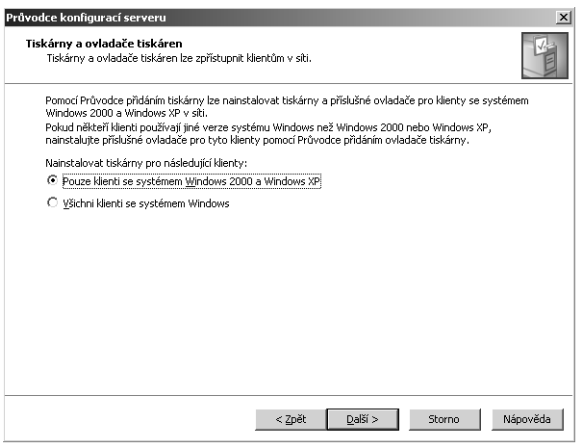
Obrázek 3.47: *Ovládací panel Tiskárny a faxy*

- V následující obrazovce *Vlastnosti tiskárny* vidíme kartu *Sdílení*, kde klepnutím na políčko *Sdílet tuto tiskárnu* sdílení povolíme. Od tohoto okamžiku je tiskárna viditelná ze sítě.

Obrázek 3.48: *Karta sdílení*

Použijeme-li složitější sdílení souborů (*Tento počítač / Nástroje / Možnosti složky /* záložka *Zobrazení,* v řádku *Použít zjednodušené sdílení souborů* nesmí být zatržítko), budeme moci určovat, kdo s naší tiskárnou může a nemůže pracovat. Zakázáním zjednodušeného sdílení zpřístupníme kartu *Zabezpečení* ve vlastnostech tiskárny. Na této kartě pak můžeme zadat jaké možnosti práce s tiskárnou bude mít určitý uživatel či skupina. Kompletní popis tohoto sdílení (především vysvětlení základních možností jednotlivých skupin), najdete v kapitole *Síť Windows Server 2003.* Nyní jenom stručně (příklad ukazuje obrázek). Pro práci s tiskárnou jsou k dispozici tři základní oprávnění:

- ***Tisk:*** Uživatel (skupina) může posílat dokumenty do tiskárny. Implicitně (po instalaci) je oprávnění k tisku přiděleno všem členům skupiny *Everyone*. (Do skupiny *Everyone* jsou automaticky zařazeni všichni uživatelé, kteří se legálně přihlásili k operačnímu systému).
- ***Správa tiskáren*** Uživatel (skupina) může na tiskárně tisknout, a navíc má oprávnění ke správě tiskárny. Může pozastavit a restartovat tiskárnu, měnit nastavení zařazovací služby pro tisk, sdílet tiskárnu, nastavovat oprávnění k tiskárně a měnit vlastnosti tiskárny. Implicitně je toto oprávnění přiděleno členům skupiny *Správci* a *Power Users*.
- ***Správa dokumentů*** Uživatel může pozastavit, obnovit, restartovat a zrušit dokumenty zaslané všemi ostatními uživateli nebo změnit pořadí těchto dokumentů. Oprávnění *Správa dokumentů* umožňuje pouze manipulaci s dokumenty v tiskové frontě (je jí věnován zvláštní odstavec). Neumožňuje posílat dokumenty do tiskárny (na to potřebuje oprávnění *Tisk*), nebo řídit stav tiskárny (na to potřebuje oprávnění *Správa tiskáren*).



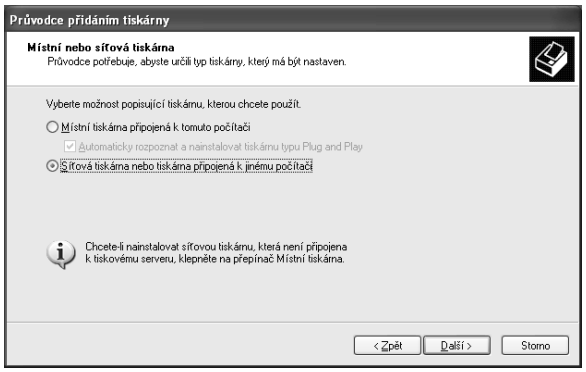
Obrázek 3.49: *Karta Zabezpečení*

Instalace sdílené tiskárny

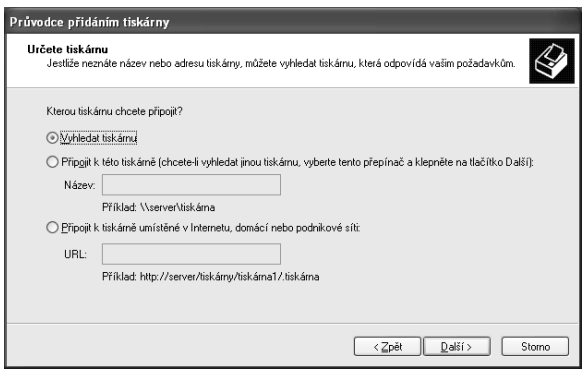
Na vzdálenou tiskárnu (připojenou k jinému počítači) můžeme tisknout až po nainstalování jejího ovladače do našeho počítače. Síťovou tiskárnu přidáme prostřednictvím *Průvodce přidáním tiskárny.*

1. První obrazovka *Průvodce* je pouze informativní.
2. Druhá je velmi důležitá, protože zde musíme zaškrtnout řádek *Síťová tiskárna nebo tiskárna připojená k jinému počítači. Průvodce* tak začne pracovat v síťovém režimu.
3. Ve třetí obrazovce máme zadat jméno tiskárny, k níž se chceme připojit. Jméno musíme zadávat podle pravidel UNC (druhý řádek), nebo URL (třetí řádek). Obě metody vyžadují přesně definovaný tvar, s lomítky atd. Uživatelsky nejpříjemnější je ponechat zaškrtnutý první řádek *Vyhledat tiskárnu* a stisknout tlačítko *Další.*

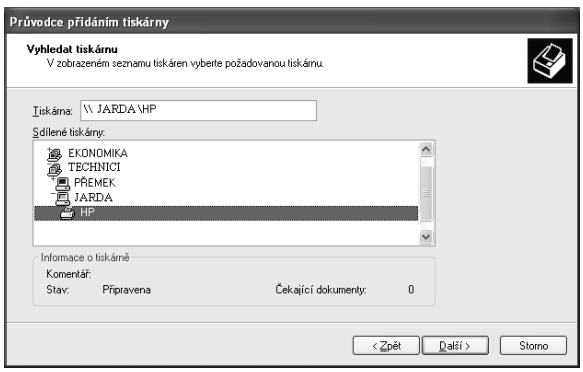
4. Dostaneme se do obrazovky s obsahem naší sítě. Uvidíme dva typy objektů – skupiny a počítače. V levém horním rohu každého objektu je buď +, znamenající že objekt můžeme rozvinout, nebo -, objekt je rozbalen. U skupin uvidíme + vždy (v každé skupině je alespoň jeden počítač). U počítačů + značí, že počítač obsahuje sdílenou tiskárnu.
5. Tlačítkem *Další* pokračujeme v instalaci tiskárny stejným způsobem jako u lokální tiskárny. Máme-li oba dva operační systémy stejné (na vzdáleném i našem PC), nainstaluje se ovladač tiskárny automaticky, ze vzdáleného počítače. Pokud jsou oba systémy rozdílné, budeme muset nainstalovat ovladač z diskety nebo CD.



Obrázek 3.50: *Druhá obrazovka, síťová instalace*



Obrázek 3.51: *Třetí obrazovka – metoda vyhledání síťové tiskárny*



Obrázek 3.52: *Čtvrtá obrazovka – hledání síťové tiskárny v síti*

Poznámka: *Výše popsaný způsob sdílení (instalace ovladače a následné sdílení) je většinou možné aplikovat také na jiný sdílený hardware, například skener.*

Sdílení tiskárny prostřednictvím print serveru

Print server je zvláštní hardwarový prvek, zkonstruovaný pro sdílení tiskáren. Jde o „krabičku“ se vstupem pro síťový kabel (konektorem RJ-45) a výstupem s několika porty pro připojení tiskáren. Typicky bývají k dispozici 1–3 porty, k nimž se připojují sdílené tiskárny. Dnes se tiskárny připojují portem USB, dříve to byl port paralelní. Při nákupu print serveru na to musíme pamatovat a koupit print server s výstupními porty pro naše konkrétní tiskárny. Port USB existuje navíc ve dvou normách, starší 1.x a novější a rychlejší 2.x. Výhodnější je tedy koupit print server s USB normy 2.x.

Použití print serveru má mnoho výhod: tisky nezatěžují žádný počítač, print server je vždy k dispozici (kvůli tisku nemusíme zapínat počítač se sdílenou tiskárnou). Do tiskáren určených k tisku v síti bývá navíc často integrován. Jeho jediným nedostatkem je cena, která ve srovnání s připojením tiskárny k PC celé řešení mírně prodražuje.

Instalace print serveru do sítě probíhá ve dvou krocích:

- Prvním, jednodušším je instalace hardwarová, spočívající v propojení kabelů. Print server připojíme ke switchi (budeme potřebovat jeden jeho port) a k tiskárně (případně tiskárnám). Většina dražších tiskáren, určených pro provoz v síti, má print server integrován. Takovou tiskárnu připojíme pouze jedním síťovým kabelem ke switchi.

- Stejně jako síťové karty a koncentrátory, může také print server komunikovat rychlostí 10, 100 nebo 10/100 Mb/s. Musíme si tedy pořídit takový print server, aby komunikoval s protilehlým switchem (viz kapitola *Strukturovaná kabeláž*).
- Druhým krokem je nahrání ovladačů, popsané v následující kapitole.

Ovladače tiskáren připojených k print serveru

Během nahrávání lokálního ovladače tiskárny sdělíme Windows, který port počítače jsme použili. U print serveru to tak jednoduché není, protože port print serveru ve Windows nenajdeme (není lokální a Windows ho nenajdou). Prvním krokem tedy je vytvoření portu print serveru. Tento port (ačkoliv vzdálený) se pak přiřadí k lokálním portům operačního systému. Poté již probíhá instalace ovladače tiskárny běžným, lokálním způsobem – ve třetí obrazovce *Průvodce přidáním tiskárny* zadáme, že tiskárna je připojena k portu print serveru.

Hlavním úskalím softwarové instalace tiskárny je tedy vytvoření lokálního portu, zastupujícího skutečný vzdálený port print serveru. K vytvoření tohoto portu slouží program dodávaný s print serverem. Print servery vyrábí mnoho firem specializujících se na prvky počítačových sítí, navíc je integrují do svých výrobků také producenti tiskáren. Proto obecný popis instalace portu není možný, přesto jej alespoň naznačím na postupu instalace tiskárny Hewlett Packard.

Program určený ke správě print serveru Hewlett Packard se jmenuje JetAdmin. Po spuštění jeho instalace se nejprve objeví první, pouze informační obrazovka. Pak již následuje druhá obrazovka, nazvaná *Zvolte typ instalace*. Zde máme tři možnosti volby:

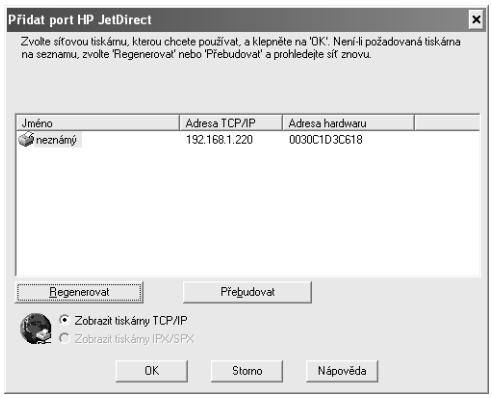
- *Síťový tisk* – kdy vytvoříme pouze port pro připojení tiskárny.
- *Síťový tisk a stav* – k portu navíc přibude možnost, kdy nás bude JetAdmin informovat o stavu tiskárny.
- *Síťový tisk a řízení* – kromě portu máme možnost spravovat tiskárnu.

Poté se dostaneme do *Průvodce*, který nám pomůže vytvořit port. Stiskneme tlačítko *Další* a budeme mít možnost zadat informace o hledaném print serveru ručně (např. jeho *adresu hardware* najdeme v manuálu), ale snadnější je tlačítkem *Seznam tiskáren* spustit automatické vyhledání. Nalezenou tiskárnu print server vidíte v okně *Přidat port HP JetDirect*.

Obrázek 3.53: *Druhá obrazovka – Volba typu instalace*

Obrázek 3.54: *Třetí obrazovka – Start Průvodce pro vytvoření tiskového portu*

Obrázek 3.55: *Čtvrtá obrazovka – Hledání print serveru, k němuž vytváříme port*

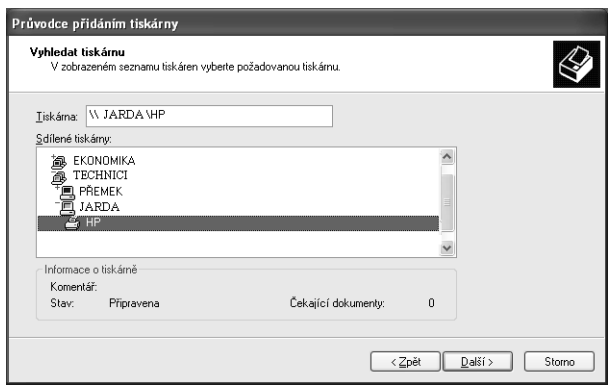


Obrázek 3.56: *Pátá obrazovka – Nalezený print server*

Nově vytvořený tiskový port se zařadí k ostatním lokálním portům tiskárny. Pokud se podíváme do vlastností jakékoliv tiskárny, uvidíme nový port mezi ostatními.

Nyní již můžeme nainstalovat ovladače k tiskárně připojené prostřednictvím print serveru. Během instalace ji samozřejmě připojíme k portu print serveru. Někdy se print serverový port při instalaci neobjeví, pak tiskárně přiřadíme jiný dostupný lokální port.

> ***Poznámka:*** *Každý síťový operační systém nabízí službu tiskového serveru (print serveru), čímž v podstatě supluje činnost hardwarového serveru. Protože se servery zpravidla umísťují do zvláštních místností, mimo běžně přístupné prostory, a jejich propojení s tiskárnou není snadné, bývá v poslední době častěji používán hardwarový print server.*



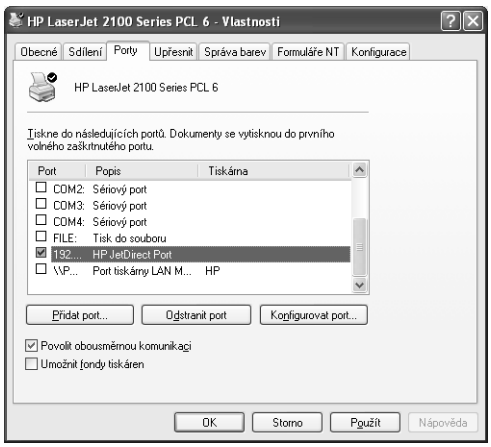
Obrázek 3.57: *Tiskový port print serveru mezi porty lokálními*

Tisková fronta

Základním prvkem společného tisku je tisková fronta. Zde se řadí tiskové úlohy jedna za druhou a pak se postupně tisknou. V ovládacím panelu *Tiskárny a faxy* vidíme všechny instalované tiskárny (lokální i síťové). Poklepáním levým tlačítkem myši na tiskárně otevřeme pohled do tiskové fronty konkrétní tiskárny. Vše si vysvětlíme na obrázku *Pohled do tiskové fronty*, kde v tiskové frontě tiskárny HP LaserJet 2100 Series PCL 6 vidíte dvě tiskové úlohy. Tím, kdo je sem poslal, je uživatel Administrator. Klepnutím pravého tlačítka myši na úloze vyvoláme menu spojené s úlohou:

- *Pozastavit* – pozdrží tisk úlohy
- *Restartovat* – způsobí nový tisk dokumentu (od začátku)
- *Storno* – zruší tisk dokumentu
- *Vlastnosti* – zde zjistíme podrobnější informace o tištěném dokumentu

Zacházení s obsahem tiskové fronty se řídí přístupovými právy. Každý uživatel může manipulovat pouze se svými dokumenty. Měnit vlastnosti dokumentů může pouze správce tiskové fronty. U tiskárny sdílené prostřednictvím počítače jím je uživatel PC, k němuž je tiskárna připojena. V případě print serveru se manipulační práva k tiskové frontě přidělují prostřednictvím programu ovládajícího tiskárnu (v případě našeho příkladu to byl HP JetAdmin). Máme-li povoleno rozšířené sdílení souborů, můžeme oprávnění k manipulaci s tiskovými úlohami v tiskové frontě přidělovat konkrétním uživatelům a skupinám.



Obrázek 3.58: *Pohled do tiskové fronty*

Kapitola 4

Síť Windows Server 2003

V této kapitole se budu věnovat síti klient server, založené na síťovém operačním systému Windows Server 2003. Než začnu s výkladem, prohlédneme si tabulku s přehledem operačních systémů Windows. Vyjasníme si tak terminologii a předejdeme nedorozumění, vyplývajícím z podobných názvů různých operačních systémů firmy Microsoft. Ujasníme si také, které operační systémy jsou síťové a které desktopové. V první tabulce najdete desktopové operační systémy Windows. Dnešním standardem jsou Windows XP, ale jsou zde uvedeny také starší produkty, které ještě často najdeme na mnoha počítačích.

Tabulka 4.1: Přehled desktopových operačních systémů Windows

Operační systém	určení
Windows 98	Určen pro stolní počítače. Je zde obsažen klient pro připojení k síti peer to peer i klient/server. Neobsahují žádný zabezpečovací systém. (Podobné vlastnosti a určení mají také operační systémy Windows 95 a Millennium.) Dnes jde o systém dožívající ve starých počítačích.
Windows 2000 Professional	Pro stolní počítače, je zde obsažen klient pro připojení k síti peer to peer i klient/server (Windows 2000 i Novell NetWare). Mají propracovaný zabezpečovací systém, velmi podobný Windows 2000 Serveru. K počítači se může přihlásit pouze uživatel, jehož přihlašovací účet existuje v databázi uživatelů stanice. Uživatelům je možné přidělovat oprávnění definující jejich povolené činnosti. Windows 2000 byly podstatně kvalitnějším systémem než Windows 98, ale i ony jsou dnes staré a dožívající.
Windows XP Home Edition	Dnes standardní desktopový operační systém, určený pro použití v domácnostech. Má omezenu především možnost práce v síti.
Windows XP Professional Edition	Dnes standardní desktopový operační systém, určený pro použití ve firmách. Jsou přímým pokračovatelem Windows 2000, přebraly jejich zabezpečovací vlastnosti. Dovolují kvalitní práci v síti peer to peer a klient/server.

Druhá tabulka je věnována síťovým operačním systémům. Úspěšný serverový systém Windows 2000 Server byl nahrazen operačním systémem Windows 2003 Server. Na mnoha serverech najdeme ještě starší variantu Windows Serveru, a tak je jí v tabulce věnováno patřičné místo.

Tabulka 4.2: Serverové operační systémy

Windows 2000 Server	Obsahuje všechny vlastnosti Windows 2000 Professional, které jsou doplněny o vlastnosti potřebné pro souborový, tiskový a aplikační server. Obsahuje databázi Active Directory, v níž jsou soustředěny údaje o objektech sítě. Umožňuje tedy centrální správu uživatelů, skupin, služeb ... Podporuje 1 až 4procesorové systémy.
Windows 2000 Advanced Server	Má všechny vlastnosti Windows 2000 Serveru, ale je určen pro velké sítě. Podporuje až 8procesorové systémy.
Windows 2000 Datacenter Server	Rozšířená verze operačního systému Windows 2000 Server, určená pro rozsáhlé podnikové sítě. Podporuje až 16procesorové systémy.

Windows Server 2003, Web Edition	Je funkčně zaměřený webový server. Poskytuje platformu pro provoz webových serverů a hostitelských služeb, kterou lze snadno zavádět a spravovat. Funkce běžných síťových serverů však jsou značně omezeny, a tak se jako souborový server nedá použít.
Windows Server 2003, Standard Edition	Nabízí řešení pro sdílení souborů a tiskáren, bezpečné připojení k Internetu a centralizované zavádění osobních aplikací. Podporuje zpracování dvěma procesory a až 4 GB paměti. Určitě je nejpoužívanější variantou Serveru Microsoft u menších a středních sítí LAN (v naší knize vycházíme z jeho popisu). Od svého předchůdce, serveru Windows 2000 Server, se na první pohled liší podobným uživatelským rozhraním jako mají Windows XP.
Windows Server 2003, Enterprise Edition	Podporuje využití až osmi procesorů a poskytuje funkce pro vytváření clusterů se čtyřmi uzly, a až 32 GB paměti. K dispozici je také pro 64bitové počítačové platformy. Je určen pro střední a velké organizace.
Windows Server 2003, Datacenter Edition	Jde o nejvýkonnější serverový operační systém Microsoftu. Podporuje symetrické zpracování až 32 procesory a poskytuje možnost vytváření clusterů s osmi uzly a vyrovnávání zatížení jako standardní funkce. Je k dispozici také pro 64bitové počítačové platformy.

V tabulce vidíme vždy několik variant základního operačního systému. Varianty se liší svým zaměřením na různě velké sítě. V našem popisu budeme vycházet především z Windows Serveru 2003 (jakéhosi protějšku Windows XP).

Souborový systém

Data jsou síťovým operačním systémem Windows Server 2003 obhospodařována podle známého schématu:

- Základní jednotkou dat seskupených za určitým účelem je soubor.
- Soubory se shromažďují do složek (starší termín adresář).
- Všechny tyto objekty jsou uloženy na disku: soubory ve složkách a složky na svazcích.

Uspořádání pevných disků

Windows Server 2003 rozeznávají dva typy úložišť (uspořádání disků):

Základní disky

Základní disky, které je možné rozdělit na několik nezávislých primárních oddílů. V každém oddílu může být nahrán jiný operační systém. Dále je zde možné vytvářet rozšířené oddíly, které se dělí na segmenty. Každý segment má pak vlastní logické jméno (písmeno s dvojtečkou).

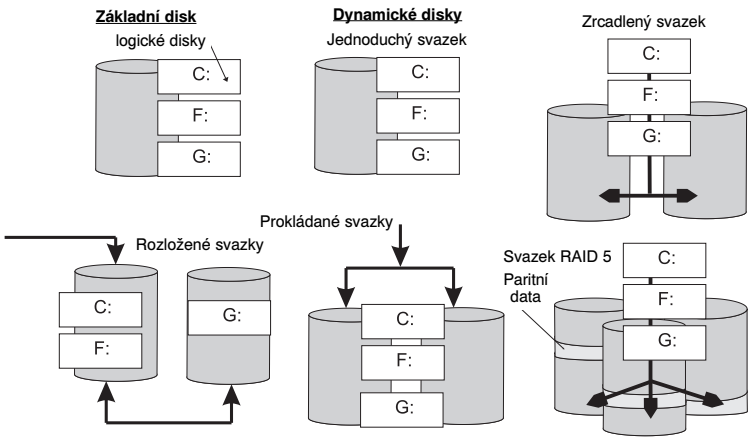
Výhodou takovéhoto uspořádání je to, že je možné použití více operačních systémů, ale u základních disků nemůžeme použít žádnou z metod ochrany dat RAID (kterou serverové systémy Windows nabízejí). Pro servery je tedy výhodnější použít disky dynamické.

Dynamické disky

Základní disky můžeme inovovat na disky dynamické, které jsou čitelné pouze z Windows 2000, XP a serverových systémů (v podstatě ze systémů podporujících NTFS), nepoužijeme je při kombinovaném provozu více operačních systémů). Původní diskové oddíly základních disků jsou nahrazeny svazky dynamických disků.

Na dynamických discích můžeme vytvářet svazky několika typů:

- **Jednoduchý svazek:** je tvořen místem na jednom fyzickém disku. Může zabírat jen jednu oblast disku nebo se může skládat z více vzájemně propojených oblastí na disku (max. 32 oblastí). Jednoduchý svazek můžete rozšířit v rámci téhož disku, nebo na další disk. (Po rozšíření na více disků se jednoduchý svazek stane svazkem rozloženým.)
- **Rozložený svazek:** obsahuje diskový prostor z více disků (max. ze 32 disků). Windows 2000 pracují tak, že daty zaplní diskový prostor prvního disku, pak druhého atd.
- **Zrcadlený svazek:** jde o dvě stejné kopie jednoho svazku. Každá kopie je uložená na jiném disku (jedná se o metodu RAID 1 – viz Disková pole v kapitole Servery).
- **Prokládaný svazek:** pracuje podobně jako Rozložený svazek, je složen z více pevných disků (až 32). Narozdíl od Rozloženého svazku však data zapisuje rovnoměrně na všechny disky (používá metodu RAID 0).
- **Svazek RAID 5:** je prokládaným svazkem, který na jednotlivé disky ukládá ještě paritní informace. Jde o nejvyšší stupeň zabezpečení dat, k jeho aplikaci jsou potřeba minimálně 3 disky.



Obrázek 4.1: *Uspořádání disků*

Odolnost proti chybám

Jednotlivé typy disků a svazků vytváříme při instalaci. Typy svazků je možné změnit i po instalaci, je to však nebezpečná činnost, během níž může dojít ke ztrátě dat a tak se této problematice nebudeme podrobně věnovat. Pokud však budete plánovat nasazení Windows Serveru, je nutné uvědomit si jakou jednotlivé typy svazků nabízejí odolnost proti chybám.

Tabulka 4.3: Odolnost pevných disků Windows Server proti chybám

Základní disk	Neposkytuje odolnost proti chybám.
Jednoduchý svazek dynamického disku	Neposkytuje odolnost proti chybám.
Rozložený svazek dynamického disku	Neposkytuje odolnost proti chybám.
Zrcadlený svazek dynamického disku	Odolnost je definována metodou RAID 1. Svazek sestává ze dvou disků, při poruše jednoho z nich je možné dále pracovat (data jsou uložena ještě na druhém disku).
Prokládaný svazek dynamického disku	Pracuje podle metody RAID 0, a tak neposkytuje odolnost proti chybám.
Svazek RAID 5 dynamického disku	Z paritních dat uložených na discích je schopen zrekonstruovat data na poškozeném disku. Pro činnost RAID 5 jsou nutné minimálně 3 disky.

Tip: Z tabulky vyplývá, že pro servery je vhodná některá varianta dynamického disku. Jen toto úložiště nabízí možnost ochrany dat (některou z metod RAID). Vytvářet disková pole můžeme také hardwarově, prostřednictvím diskových řadičů. Dnes tuto možnost nabízí téměř všechny servery (a také mnoho desktopových základních desek). Pokud je diskový řadič pole RAID k dispozici, je lepší použít hardwarové řešení, které je rychlejší a nezatěžuje operační systém.

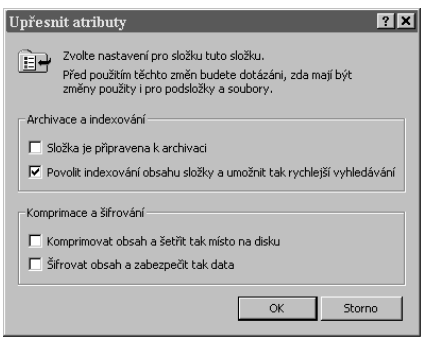
Obnova smazaných dat

Ze všech operačních systémů rodiny Windows jsme zvyklí na to, že mazaná data se přesunují do speciální složky nazývané *Koš*. Odtud je pak možné je později obnovit.

Stejná metoda je použita i u Windows Serverů. Funguje však pouze pro soubory (a složky) mazané z konzoly serveru. Položky odstraněné ze síťové stanice (ze síťové jednotky) jsou odstraněny trvale a do koše nejsou umístěny!

Komprimace dat

Windows XP nabízejí možnost komprimace (komprese) dat. Zkomprimované soubory (nebo složky) jsou zakódovány speciálním algoritmem, čímž se zmenší jejich velikost na disku. Komprimace je tedy určena k úspoře místa na disku, což je pro servery určitě výhodné.



Obrázek 4.2: *Nastavení komprimace složky*

Nastavení komprimace

Kompresi dat zadáme tak, že na příslušnou složku (soubor) klepneme pravým tlačítkem myši a otevřeme dialog *Vlastnosti*. Na kartě *Obecné* stiskneme tlačítko *Upřesnit*. Pak zaškrtneme políčko *Komprimovat obsah a šetřit tak místo na disku*.

Po nastavení komprimace a stisku tlačítka *Použít* se zobrazí dialog *Potvrdit změnu atributů*. Zde máme dvě možnosti:

- ***Použít změny pouze pro tuto složku:*** zkomprimují se pouze soubory ve zvolené složce.
- ***Použít změny pro tuto složku, podsložky a soubory:*** zkomprimují se všechny soubory ve složce a jejích podsložkách. Budou se také komprimovat všechny soubory, které sem vložíme v budoucnu.

Doporučení pro práci s komprimací

Pokud se rozhodnete komprimaci používat, je dobré respektovat určitá pravidla:

- Komprimujte spíše statická data (tj. ta, která se často nemění). Komprimace a dekomprimace zabere určitý čas a při častém používání by zdržovala. Z těchto důvodů rozhodně nekomprimujte systémovou složku (C:\Windows).
- Komprimované složky a soubory jsou označeny jinou barvou. Provádí se to v *Průzkumníkovi Windows*, v nabídce *Nástroje* příkazem *Možnosti*. Zde na kartě *Zobrazit* zaškrtněte políčko *Zobrazovat komprimované složky a soubory jinou barvou*. (Po instalaci je barevné zobrazení zapnuto, ale je dobré vědět, kde to můžeme ovlivnit).
- Nemá cenu ukládat do zkomprimované složky soubory, které jsme dříve zkomprimovali v jiném programu. Windows budou takový soubor znovu komprimovat, čímž se zpomalí, ale na disku nezískáme žádné místo.

Při manipulaci se zkomprimovanými objekty se systém chová takto:

- Pokud kopírujeme soubor (složku) do složky, bude jeho stav odpovídat vlastnostem cílové složky (kopírujeme-li jej do zkomprimované složky, tak se automaticky zkomprimuje).

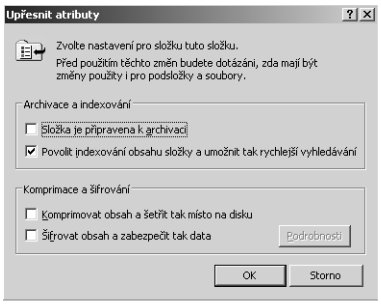
- Pokud přesunujeme soubor (složku), tak si zachová svůj původní stav (přesunujeme-li nezkomprimovaný soubor do komprimované složky, tak se soubor zapíše nezkomprimovaně)
- Kopírujeme-li nebo přesunujeme soubor (složku) na disketu, Windows 2000 ji automaticky dekomprimují (na disketě tedy musíme mít dost místa pro „rozbalený" soubor!).

Atributy

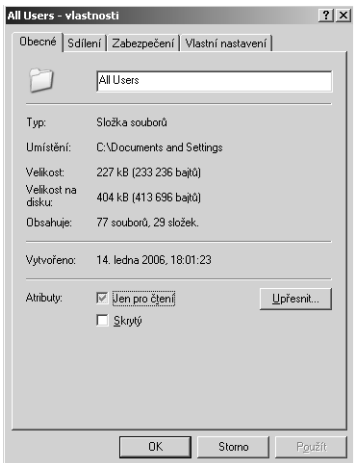
Souborové systémy FAT a NTFS mají k dispozici atributy. Jsou to doplňkové informace, rozšiřující vlastnosti složek a souborů. Pokud klepneme na souboru (složce) pravým tlačítkem myši a zvolíme Vlastnosti, tak si dole na kartě Obecné všimneme dvou okének:

- *Jen pro čtení* – složka nebo soubor jsou určeny pouze ke čtení (atribut R – read only).
- *Skrytý* – složka nebo soubor jsou neviditelné, skryté (atribut H – hidden).

Pokud ještě stiskneme tlačítko *Upřesnit*, uvidíme okénko *Složka je připravena k archivaci*. To souvisí s archivačním atributem *A* (archive). Jeho hodnota se vždy při změně souboru automaticky nastavuje na 1. Podle tohoto atributu pak systém pozná, které soubory se změnily a měly by se archivovat. O použití archivního atributu při zálohování se více dozvíte z kapitoly Zálohování (archivace) dat.



Obrázek 4.3: *Nastavení archivačního atributu*



Obrázek 4.4: *Atributy složky*

Tip: Atributy se v souvislosti s oprávněními moc nepoužívají. Pokud však soubor nebo složka nejdou smazat, zkontrolujte právě atributy.

Diskové kvóty

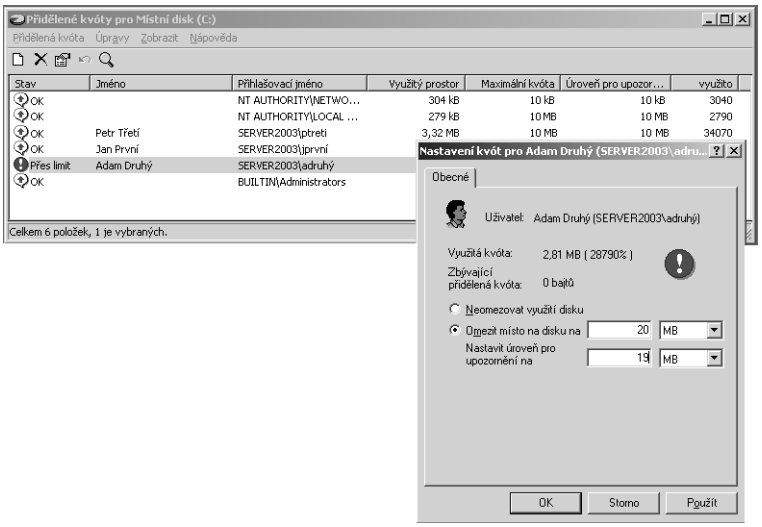
Každý správce serveru ocení možnost přidělení diskových kvót. Prostřednictvím kvót definujeme, jak velké místo na disku mohou uživatelé obsadit. Postup je poměrně jednoduchý (ale účinný). Práci s kvótami definujeme na obrazovce vlastností pevného disku, kde máme k dispozici kartu *Přidělená kvóta*. Otevřeme ji například klepnutím pravým tlačítkem myši na ikoně disku a následnou volbou *Vlastnosti*. Na kartě pak:

- Zaškrtneme *Povolit správu přidělování kvót*.
- Zaškrtneme *Odepřít místo na disku uživatelům překračujícím maximální kvótu*. Tím přinutíme uživatele hospodařit s prostorem na disku.
- Zaškrtneme *Omezit místo na disku* a zadáme velikost disku, která bude uživatelům přidělena (v pravém rozbalovacím okénku můžeme volit jednotky velikosti disku).
- Vyplníme políčko *Nastavit úroveň pro upozornění na*. Překročí-li velikost uživatelových dat tuto hodnotu, bude operačním systémem upozorněn na to, že jeho diskový prostor se zaplňuje. Uživatel pak bude muset některá data umazat, nebo požádat správce serveru o zvýšení limitu.
- Práci systému s kvótami můžeme protokolovat (spodní dvě zaškrtávací políčka).

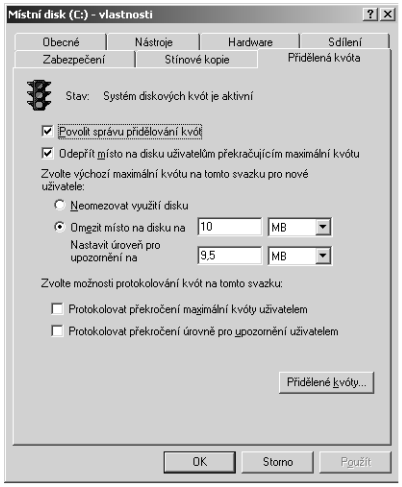
Stiskem tlačítka *Přidělené kvóty* otevřeme stejnojmennou obrazovku:

- zde jednak vidíme stav čerpání diskového prostoru
- navíc můžeme měnit hodnotu kvóty pro každého uživatele individuálně

Poznámka: *Diskové kvóty fungují, pokud je nainstalována role file server. Během instalace této role je možné také definovat diskové kvóty (viz kapitola Role serveru).*



Obrázek 4.5: *Obrazovka Přidělené kvóty*



Obrázek 4.6: *Karta přidělená kvóta*

Základní činnosti se serverem

Start serveru

Pro start serveru jsou kritické dvě oblasti na disku:

- Master Boot Record (MBR) – hlavní spouštěcí záznam, umístěný na začátku pevného disku. Je zde uložena tabulka diskových oblastí. Jedna z těchto oblastí je aktivní – z ní se provádí start systému.
- Spouštěcí sektor disku. Ten se nachází v každém diskovém oddílu. Jsou v něm uložena data potřebná pro start systému.

Další důležitou oblastí jsou registry. Databáze, v níž jsou soustředěny informace o hardwaru, softwaru a uživatelích počítače.

Při startu si systém přečte MBR, najde zde aktivní oddíl disku a z něho načte do operační paměti spouštěcí sektor. Během startu vlastního operačního systému přijdou na řadu také registry, z nichž se načte konfigurace počítače.

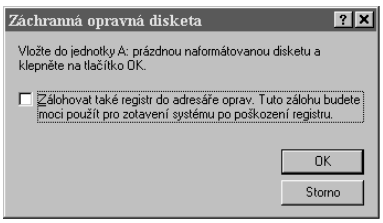
Pokud by se některá z těchto kritických součástí narušila, Windows Server nenastartuje. Proto bychom si měli vytvořit zálohu, v níž jsou kritické oblasti uloženy! V serverových operačních systémech se způsob zálohování liší:

- Ve Windows Serveru 2000 vytváříme *Záchranou a opravnou disketu.*
- Ve Windows 2003 Serveru je k dispozici *ASR (Automated system Recovery)*, jde o nástroj, který je součástí zálohovacího programu a v kapitole *Zálohování dat* si jej popíšeme.

Tip: Po startu serveru se automaticky otevře program Správa Serveru. Zde jsou soustředěni průvodci, kteří nás provedou základními konfiguracemi – rolemi serveru. Se základními rolemi serveru se ještě několikrát setkáme.

Záchranná a opravná disketa

Protože se ještě můžeme setkat s mnoha Windows 2000 Servery, alespoň stručně si vytvoření záchranné diskety popíšeme. Vytvoříme ji v programu *Zálohování* (*Start/Programy/Příslušenství/Systémové nástroje/Zálohování).* Na jeho první obrazovce stiskneme úplně spodní tlačítko *Záchranná a opravná disketa.* Systém nás vyzve k vložení diskety do mechaniky. K dispozici je zaškrtávací políčko *Zálohovat také registr….* Jeho zaškrtnutím zazálohujeme rovněž soubory systémových registrů.

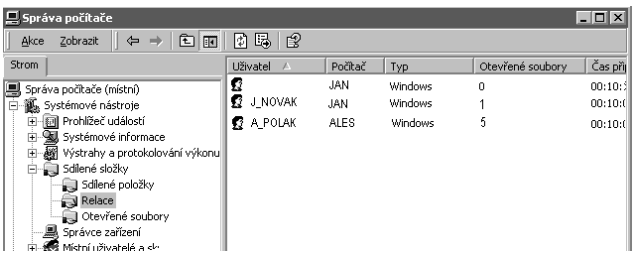


Obrázek 4.7: *Záchranná a opravná disketa*

Tip: Je vždy dobré pořídit také zálohu registrů. V registrech se odrazí jakákoliv změna v konfiguraci systému (instalace nového programu, změna hardwaru, vytvoření uživatele). Proto je nutné záchrannou disketu pravidelně obnovovat. Aktualizujte ji pokaždé před složitější operací se serverem.

Vypnutí serveru

Ze všech operačních systémů Windows jsme zvyklí na to, že před vypnutím PC musíme nejdříve ukončit operační systém. Provádíme to tlačítkem *Start/Vypnout.*



Obrázek 4.8: *Otevřené soubory na serveru*

U serveru je uložení systému ještě důležitější než u pracovní stanice. Navíc musíme před stiskem vypínacích tlačítek zajistit to, aby nikdo z uživatelů na serveru nepracoval a neměl zde otevřené soubory. Tuto informaci získáme v konzole *Sdílené složky* (*Start/Nástroje pro správu/Správa počítače*) – jde o stejný postup jako u Windows XP.

Klepneme-li v levém okně obrazovky na *Relace*, vidíme v pravé části konzoly uživatele, kteří se serverem pracují. Po umístění kurzoru na *Otevřené soubory* spatříme soubory, s nimiž se na serveru pracuje.

Před vypnutím serveru by v pravém okně obrazovky neměly být žádné otevřené soubory!

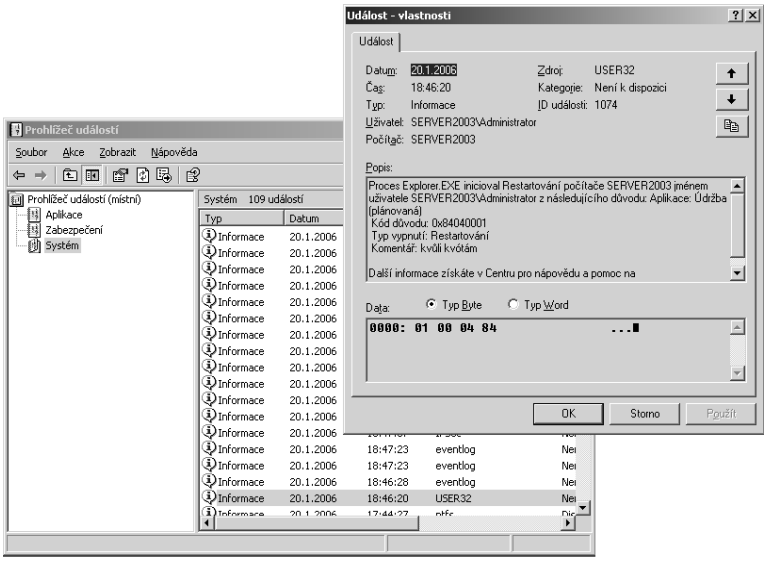
Nástroj Přehled událostí vypnutí

Tuto novinku přináší Windows Server 2003 (je k dispozici i ve Windows XP, ale není zde aktivována). Před vypnutím serveru musíme zadat důvod, proč k vypnutí dochází. Tato informace je zaznamenána a uchovávána v *Protokolu událostí.* Kdykoliv později můžeme provést analýzu vypínání. A nyní konkrétně:

- Zaznamenání události při vypnutí ukazuje obrázek *Vypnutí Windows Serveru 2003.*
- K analýze událostí slouží *Prohlížeč událostí* (pravé tlačítko myši na ikoně *Tento počítač / Spravovat / Prohlížeč událostí*), v *Systémovém Protokolu událostí* pak informaci o vypnutí najdeme. Výhodné je použít menu *Akce / Najít.*

Poznámka: *V Prohlížeči událostí najdeme také mnoho jiných užitečných informací o činnosti (a poruchách) počítače.*

Obrázek 4.9: *Vypnutí Windows Serveru 2003*



Obrázek 4.10: *Informace o vypnutí serveru*

Ovládání Windows XP

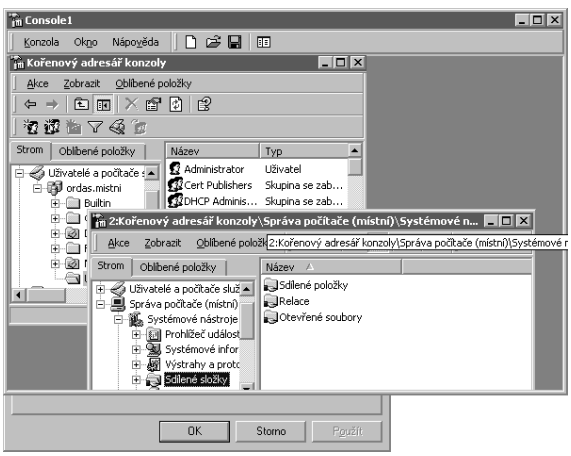
Ještě než začneme s popisem systému, zmíním se o jeho ovládání. Základním prostředkem ke konfiguraci jsou moduly uložené ve složce *Nástroje pro správu*. Dostaneme se k nim přes tlačítko *Start/Nástroje pro správu*. V podstatě jde o předdefinované konzoly správy systému. Při správě systému používáme tyto konzoly automaticky, navíc Windows umožňují vytvoření vlastních konzol.

Konzola MMC (Microsoft Management Console)

Konzola MMC je obrazovkovým rozhraním soustřeďujícím správu počítače operačního systému do jednoho místa. V principu jde o obrazovku, do níž je možné jednotlivé správní moduly doinstalovávat. Moduly správy jsou dodávány v zásuvné (snap-in) formě. Mezi hlavní výhody MMC patří:

- centralizování správy do jednoho místa
- možnost použití většiny modulů pro vzdálenou správu jiného počítače (např. serveru)
- vytvoření přizpůsobené konzoly. Můžeme vytvořit několik konzol a pak je přiřadit skupinám uživatelů.

Při instalaci Windows se některé konzoly nainstalují automaticky, najdeme je v nabídce *Nástroje pro správu*. Někdy je však výhodné připravit si vlastní správcovskou konzolu.



Obrázek 4.11: *Okno konzoly MMC*

Popis konzoly

Program spustíme přes tlačítko *Start/Spustit* a do řádku zadáme příkaz MMC. Otevře se okno konzoly, v němž může být umístěno několik podřízených oken s moduly snap-in. Menu základního okna obsahuje nabídky: *Konzola, Okno, Nápověda*. Jimi se ovládají okna podřízená. Podřízené okno připomíná Průzkumníka. V jeho levé části vidíme strom konzoly (v podstatě nainstalované ovládací moduly a jejich složky) a v pravé části pak detaily složek jednotlivých modulů.

Přidání modulu snap-in

Do podřízeného okna se instalují především ty moduly, s nimiž často pracujeme. Uděláme to tak, že klepneme na položku *Konzola* v menu hlavního okna a pak vybereme položku *Přidat nebo odebrat modul snap-in*. (Spustíme tak *Průvodce*, který nás provede instalací modulu).

- Na následující obrazovce (s přehledem nainstalovaných modulů) klepneme na tlačítko *Přidat*. Zobrazí se seznam dostupných modulů snap-in. Kurzorem modul vybereme a tlačítkem *Přidat* přejdeme do další obrazovky.
- Tady stanovíme, pro který počítač bude modul platný. Buď pro ten, z něhož jsme konzolu spustili, nebo pro jiný – například server (vzdálené správě serveru je věnována kapitola *Vzdálený přístup*).
- Pak přidávání modulu uzavřeme tlačítkem *Dokončit*. Nabídne se nám ještě obrazovka se seznamem dostupných modulů (pokud bychom chtěli doplnit další modul), tu uzavřeme tlačítkem *Zavřít* a okno s přehledem nainstalovaných modulů potvrdíme tlačítkem OK.

Odebrání modulu snap-in

Opět použijeme volbu *Konzola/Přidat nebo odebrat modul snap-in*. Vyvoláme obrazovku *Přidat nebo odebrat modul snap-in*, v níž je seznam nainstalovaných modulů. Na modul klepneme myší a tlačítkem *Odebrat* jej odinstalujeme.

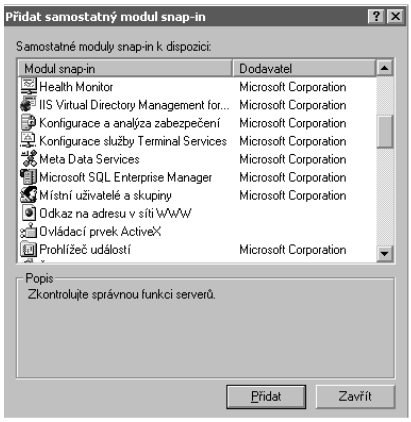
Uložení konzoly

Menu hlavního okna *Konzola/Uložit* slouží k uložení vlastní konzoly s moduly snap-in. Nastavení se ukládá do souboru s příponou **.msc*. Uloženou konzolu najdeme v menu *Start/Nástroje pro správu*. Obsah složky *Nástroje pro správu* je originální pro každého uživatele, a tak i konkrétní konzola je vlastnictvím svého tvůrce.

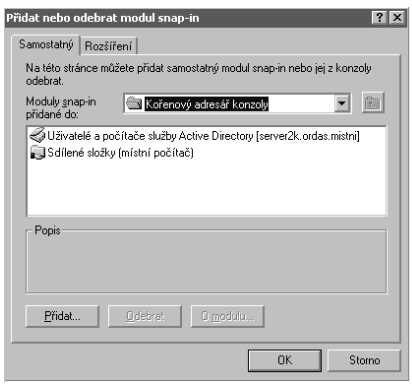
Režimy konzoly

Rozeznáváme dva základní režimy práce konzoly, k jejichž přepínání slouží menu *Konzola/Možnosti*.

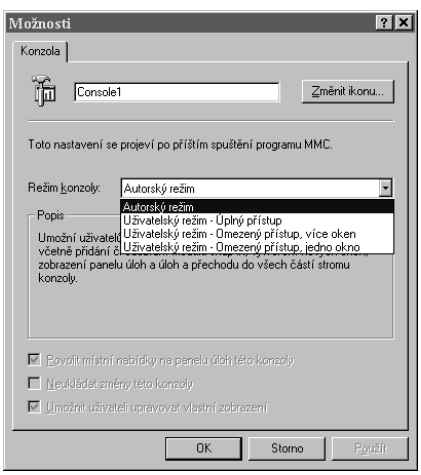
- **autorský režim**, dovoluje všechny činnosti konzoly, především přidávání a odebírání modulů snap-in,
- **uživatelský režim,** v němž není možné měnit moduly snap-in a ukládat konzolu. Tento režim se používá pro distribuování konzoly dílčím správcům sítě. K dispozici jsou tři typy uživatelského režimu, jejichž popis ukazuje tabulka.



Obrázek 4.12: *Přehled modulů snap-in, dostupných pro instalaci*



Obrázek 4.13: *Nainstalované moduly snap-in*



Obrázek 4.14: *Režimy konzoly MMC*

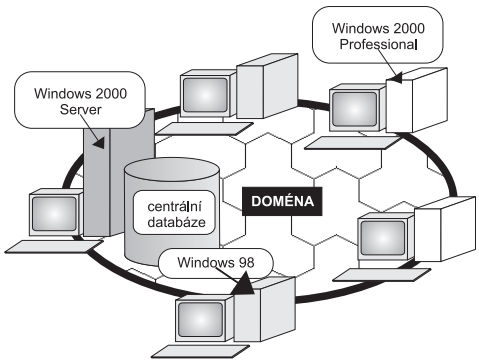
Tabulka 4.4: Typy konzol MMC

Typ uživatelského režimu	popis
Úplný přístup	Přístup ke všem částem stromu konzoly (v podřízeném okně) může otevírat nová okna
Omezený přístup – více oken	Není přístup ke stromu konzoly, ale může zobrazit více oken
Omezený přístup – jedno okno	Není přístup ke stromu konzoly, může zobrazit jen jedno okno konzoly

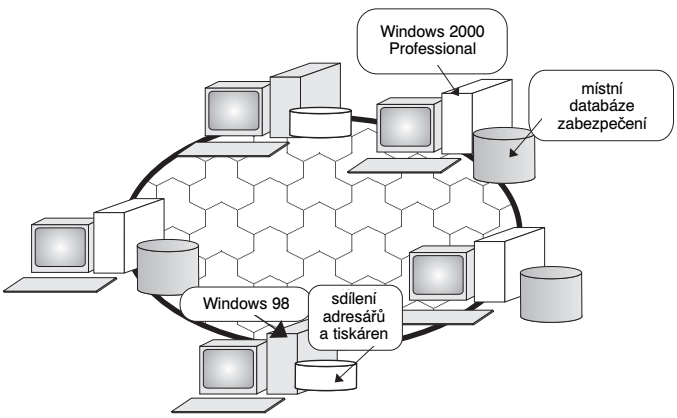
Doména a adresářové služby

Základním principem sítí klient/server je soustředění všech síťových údajů (a také uživatelských dat) na jedno místo – na centrální počítač, server. V terminologii systémů Windows Server tak vznikne *doména*. Doména je tedy logické seskupení síťových počítačů, které sdílejí centrální databázi síťových údajů (uživatelské účty, účty počítačů, informace o zabezpečení – o tom, co mají jednotliví uživatelé povoleno a zakázáno atd.). Po přihlášení k centrální databázi (doméně) máme k dispozici všechny zdroje serveru (definované naším uživatelským účtem).

Oproti tomu v síti peer to peer (které odpovídá logické uspořádání pracovní skupina) je databáze bezpečnostních údajů uložena na každém PC a platí pouze pro jeden počítač. Přesněji řečeno, funkční bezpečnostní databází disponují pouze stanice, na nichž je nahrán operační systém Windows 2000 Professional a Windows XP. U počítačů s Windows 98 jsou k dispozici pouze jednoduchá pravidla, týkající se sdílení souborů a tiskáren. Ke každému zdroji (PC, adresář) se musíme přihlašovat.



Obrázek 4.15: *Doménové uspořádání sítě*



Obrázek 4.16: *Síť peer to peer*

Active Directory

Databáze síťových objektů sítě Windows Server se nazývá *Active Directory*. Tu si představíme ze dvou pohledů: logického a fyzického.

Logická struktura Active Directory

Logická struktura organizuje všechny prvky databáze podle pravidel, snažících se kopírovat správní strukturu organizace. Při logickém popisu nás nezajímá fyzické (skutečné) umístění síťových prvků.

Základním prvkem Active Directory je **objekt**. Jde o množinu vlastností reprezentující síťový prostředek (sdílenou složku, tiskárnu, uživatelský účet, skupinu...). Objekty tedy zastupují skutečný síťový prostředek.

Objekty můžeme seskupovat do kontejnerů. **Kontejnerem** se rozumí objekt Active Directory, v němž jsou uloženy další kontejnery nebo objekty. Nižším stupněm kontejneru je **organizační jednotka (OU)**. Představuje jakousi administrativní skupinu (může například odpovídat jednomu oddělení firmy).

Základní jednotkou logické struktury Active Directory je **doména**. V ní může být několik OU, libovolně uspořádaných (např. vnořených v sobě, či postavených na stejnou úroveň). Jedná databáze Active Directory může obhospodařovat několik domén, jejichž vnitřní struktura je rozdílná. V podstatě platí pravidlo, že doména obsahuje informace pouze o svých vlastních objektech (ne o objektech jiné domény).

Fyzická organizace Active Directory

Údaje o objektech jedné domény jsou uloženy na počítači s operačním systémem Windows Server 2003. Takový počítač nazýváme řadičem domény. Je-li v síti několik domén (a několik počítačů – řadičů domén), tvoří jejich objekty a kontejnery dohromady databázi Active Directory. Počítače – řadiče domény mohou být geograficky vzdáleny, přesto budou tvořit jednu síť popsanou společnou databází Active Directory.

V jedné doméně bývá jeden počítač – řadič domény s operačním systémem Windows Server, dále zde budou klientské stanice (nejčastěji s operačním systémem Windows XP Professional). Může tu být také další server, ten však nebude řadičem domény, bude pouze poskytovat své zdroje (soubory, složky, tiskárny). Pro něj se používá termín členský server.

Při našem výkladu se zaměříme na jednoduchou variantu sítě – s jedinou doménou a jedním serverem – řadičem.

Objekty Aktive Directory:

V Active Directory nejčastěji používáme tyto objekty:

- **Uživatel** nese informaci o přihlašovacím jméně a heslu – je tedy základem zabezpečení Active Directory. Dále je zde k dispozici mnoho volitelných položek, doplňujících údaje o uživateli. (Termín Uživatel je to samé, co uživatelský účet.)
- **Skupina** obsahuje uživatele nebo jiné skupiny. Všem ve skupině je možné přidělit najednou stejnou vlastnost nebo právo.
- **Tiskárna** zveřejňuje tiskárnu použitelnou v síti, v podstatě jde o ukazatel na tiskárnu jednoho z počítačů v Active Directory.
- **Počítač** reprezentuje počítač v síti, o němž nese všechny potřebné informace.
- **Sdílená složka** informuje o sdílené složce. Sdílení složky je zapsáno v registru konkrétního počítače. Zveřejněním složky v Active Directory se vytvoří objekt zveřejňující sdílenou složku určitého PC.

Takovéto doménové uspořádání přináší dvě výhody (obecné pro sítě klient/server): dovoluje centralizovanou správu (všechny informace jsou uloženy centrálně). Další výhodou je jednotný přihlašovací proces. Uživatel se přihlásí k jednomu počítači a může přistupovat k prostředkům jiného PC (má-li k tomuto PC dostatečná oprávnění).

Objekty Active Directory administrujeme prostřednictvím konzoly *Uživatelé a počítače služby Active Directory* (*Start/Nástroje pro správu)*. Při pohledu na obrazovku konzoly si všimněte, že jednotlivé typy objektů jsou soustředěny do předdefinovaných kontejnerů:

- **Builtin:** předdefinované místní skupiny domény automaticky poskytované systémem Windows Server, například Administrators a Account Operators.
- **Computers:** účty počítačů, členů domény.
- **Domain Controllers:** počítače – řadiče domény.
- **Users:** uživatelské účty a společné globální skupiny, například *Domain Admins* a *Domain Users*.

(Práce s konzolou *Uživatelé a počítače služby Active Directory* je popsána v kapitole Uživatelské účty.)

Přihlášení uživatele k systémům Windows Server

Víme, že můžeme pracovat ve dvou typech sítí:

- Peer to peer, obsažené ve všech Windows.
- Klient server, založené na operačním systému Windows Server (nebo na síťovém operačním systému od Novellu či na Linuxu).

Obě sítě mohou spolupracovat (být použity na stejné kabeláži). Při startu počítače, jehož součástí je také přihlášení do sítě, je nutné definovat k jakému typu sítě se počítač bude hlásit.

Přihlášení do sítě je úkolem příslušného síťového klienta. U sítí Microsoftu jím je *Klient sítě Microsoft*, v jehož vlastnostech stanovíme, k jaké „microsoftí" síti se budeme přihlašovat. Možnosti klienta vycházejí z operačního systému, proto si jeho konfiguraci popíšeme. Ukážeme si raději nastavení i pro starší typy operačních systémů Windows (v sítích se se staršími Windows ještě občas potkáme).

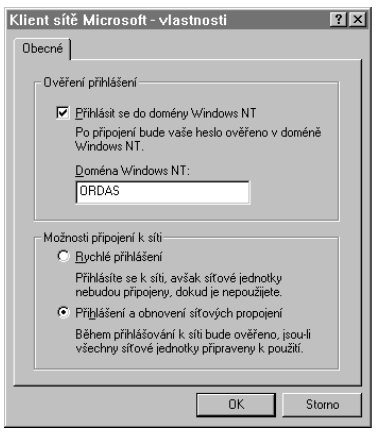
Dříve než bude možné počítač do domény přihlásit, je nutné vytvořit v doméně účet (to si ukážeme v následující kapitole). Trochu předběhnu chronologii výkladu, ale upozorním na to, že účet může vytvořit kdokoliv ze skupiny: *Administrators, Domain Administrators nebo Account Operators*. (Je to vysvětleno v kapitole *Skupiny*.)

Přihlašování z Windows 98

Zda se chceme přihlásit do domény (pokud ne, přihlašujeme se do pracovní skupiny), stanovíme takto: Klepneme pravým tlačítkem myši na ikonku *Okolní počítače*, vybereme *Vlastnosti*. Na obrazovce uvidíme všechny síťové komponenty, zvýrazníme řádek *Klient sítě Microsoft* a poté stiskneme tlačítko *Vlastnosti*.

Do horní části obrazovky (*Ověření přihlášení)* se zadávají kritéria pro přihlášení do domény. Zaškrtnutím políčka *Přihlásit se do domény Windows NT* dáme klientovi pokyn, aby stanici přihlásil do domény, jejíž jméno zapíšeme do políčka *Doména Windows NT*. (Windows 98 byly vyvinuty v době, kdy se o doménové uspořádání staral operační systém Windows NT Server. Windows Server 2003 je jeho nástupcem, a tak nás okénka odkazující na Windows NT nesmějí plést.)

Při startu počítače bude řadič domény Windows Server kontrolovat přihlašovací jméno a heslo. Tyto dva údaje musíme správně zadat, jinak nebudeme do domény přihlášeni!



Obrázek 4.17: *Přihlášení do domény*

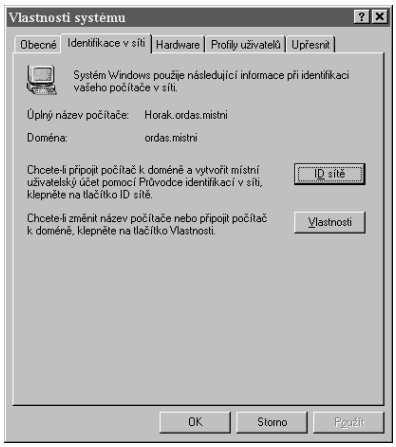
Tip: Při ověřování hesla rozlišují operační systémy Windows Server malá a velká písmena. Při přihlášení musíme tedy zapsat správně také velikost jednotlivých znaků!

Přihlašování z Windows 2000

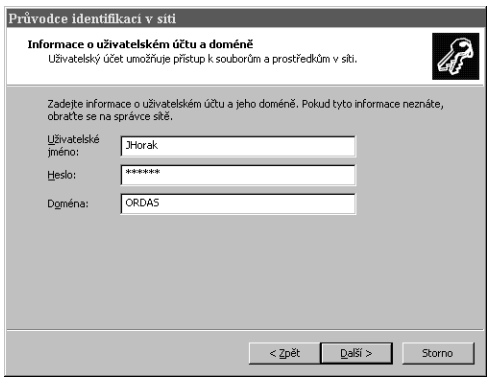
Parametry pro přihlášení do domény nastavíme ve Windows 2000 Professional takto:

1. Klepneme pravým tlačítkem myši na ikonku *Tento počítač* a vybereme *Vlastnosti*.
2. Použijeme kartu Identifikace v síti.
3. Myší stiskneme tlačítko *ID sítě* (vyvoláme *Průvodce identifikací v síti*) a v jeho první obrazovce klepneme na tlačítko *Další*.

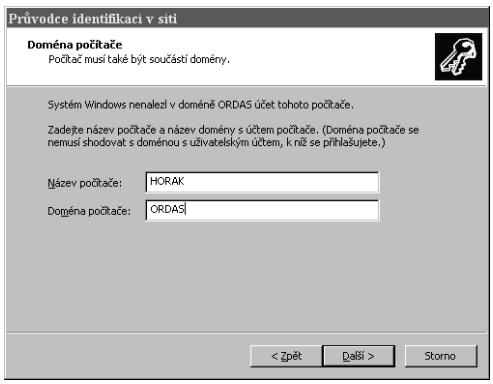
4. V následující obrazovce zvolíme možnost *Vybrat* a pokračujeme stiskem tlačítka *Další*.
5. K připojení do domény vybereme volbu *Společnost používá síť s doménou* a klepneme (2x) na *Další*. Následuje obrazovka, v níž nás průvodce upozorní na parametry, které musíme při přihlašování k doméně vyplnit.
6. V další obrazovce vyplníme přihlašovací parametry domény: uživatelské jméno, heslo a jméno domény, v níž je účet uložen.
7. Nakonec klepneme na tlačítko *Dokončit*, čímž skončíme *Průvodce*. Poté bude následovat restart počítače!
8. Správce sítě může při definici našeho účtu, přiřadit do domény také náš počítač. (Pak se do něho budou kopírovat účty podle pravidel popsaných v následující kapitole Skupiny). Pokud náš počítač nebyl ještě do domény přiřazen, objeví se obrazovka, v níž zadáme údaje potřebné k přiřazení PC do domény.



Obrázek 4.18: *Karta Identifikace v síti*



Obrázek 4.19: *Údaje potřebné k přihlášení k doménovému účtu*



Obrázek 4.20: *Údaje potřebné k přihlášení počítače do domény*

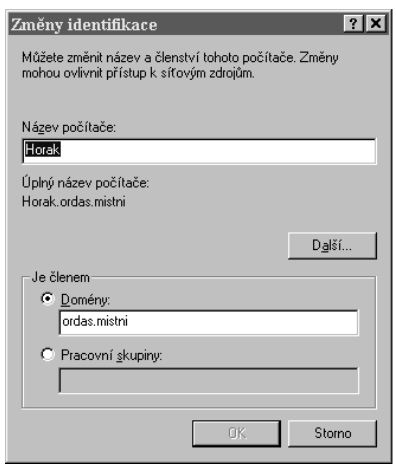
Poznámka: *Kdybychom potřebovali připojení k pracovní skupině, vybereme v bodu 5 Společnost používá síť bez domény, klepneme na Další a vyplníme jméno pracovní skupiny.*

Aktuální přihlašovací nastavení spatříme, pokud na kartě Identifikace v síti stiskneme tlačítko Vlastnosti. (Přihlašovací parametry můžeme změnit i zde.)

Přihlašování z Windows XP Professional

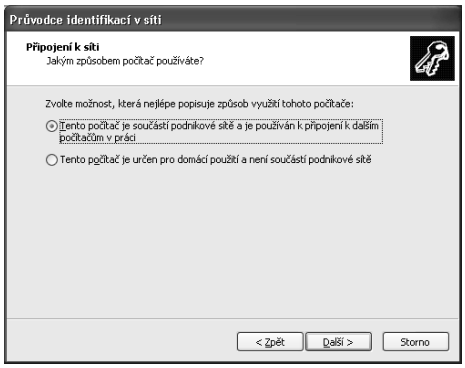
Podobně jako ve Windows 2000 Professional klepneme pravým tlačítkem myši na ikoně *Tento počítač* a vybereme *Vlastnosti*. Pak přejdeme na kartu *Název počítače*. Stiskneme tlačítko *Identifikace v síti*, čímž spustíme *Průvodce identifikací v síti*:

- V první obrazovce nás průvodce přivítá.
- Ve druhém okně zadáme, že je naše PC připojeno do sítě.

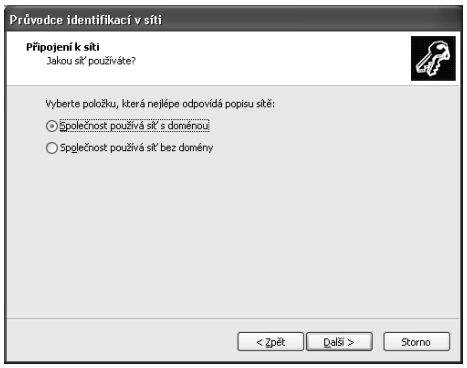


Obrázek 4.21: *Identifikace přihlašování*

- Třetí okno rozhoduje o tom, zda pracujeme v síti peer to peer (*Společnost používá síť bez domény*) nebo v síti s doménou.
- Na čtvrté obrazovce jsme upozorněni na údaje, které po nás bude operační systém požadovat (údaje o doméně, účtu a heslu).
- V páté obrazovce zadáme základní přihlašovací údaje k doméně (uživatelské jméno a heslo, název domény).



Obrázek 4.22: *Druhá obrazovka – je PC zapojeno do sítě?*



Obrázek 4.23: *Třetí obrazovka – připojujeme PC do domény?*

- V šesté obrazovce zapíšeme přihlašovací údaje účtu počítače (název PC a doménu).

(Obrazovky 5 a 6 jsou shodné s obdobou ve Windows 2000.)

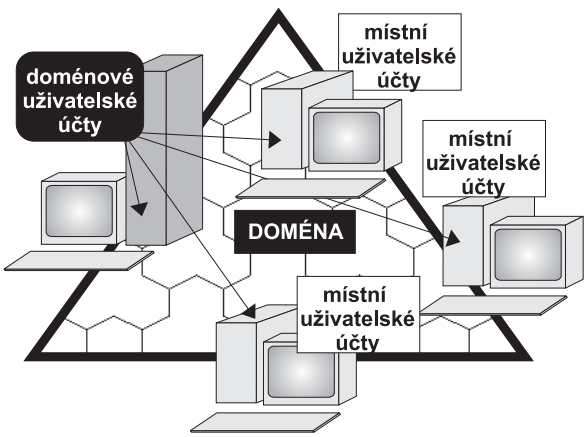
Uživatelské účty

Jak již víme, je objekt *Uživatel* (často se k jeho označení používá termín uživatelský účet) nositelem základních informací o uživateli připojujícím se k počítačům s novějšími systémy Windows. Při práci musíme důsledně rozlišovat kde je účet umístěn a jaké přihlášení tak zabezpečuje. V zásadě rozeznáváme:

- **Doménové uživatelské účty**: jejich prostřednictvím se uživatel přihlásí do domény (a do Active Directory), čímž získá přístup ke všem síťovým prostředkům. (Přesněji řečeno k těm síťovým prostředkům, k nimž má oprávnění.)
- **Místní uživatelské účty**: zprostředkovávají připojení uživatelů k místnímu počítači, na němž je účet vytvořen. Jejich prostřednictvím se nejčastěji hlásíme k PC s desktopovými operačními systémy Windows.

Rozdíl mezi oběma typy účtů zachycuje obrázek. Z místního uživatelského účtu přistupujeme pouze k prostředkům jedné stanice, kdežto majitel doménového účtu může mít přístup ke všem síťovým prostředkům (jeho skutečné možnosti definuje správce sítě).

Operační systémy Windows Server dovolují přihlášení k libovolnému účtu (ať doménovému, či uživatelskému) přímo ze serveru. Server této sítě tedy patří do serverů nededikovaných. Běžnou aplikační práci na serveru však nedoporučuji. Uvědomme si, že uživatel by pracoval na počítači, kde jsou soustředěny všechny síťové údaje (ať data či databáze objektů) a k němuž se průběžně připojují ostatní uživatelé. Nevědomky (a nechtěně) může způsobit poruchu s nebezpečnými následky. K obrazovce serveru občas zasedne pouze správce sítě, který zde bude opatrně konfigurovat nastavení sítě.



Obrázek 4.24: *Doménové a místní účty*

Předdefinované účty:

Ve Windows jsou dva účty vytvořeny automaticky: jde o účet *Administrator* a *Guest*.

- **Administrator** je účtem určeným ke správě počítače, konfiguraci domény přidělování přístupových práv atd. V sítích se administrátorem nazývá ten uživatel, který má na starosti správu sítě.
- **Guest** je účtem pro příležitostné uživatele systému. Jejich práva by měla být minimální, spíše informativní. Ve výchozím stavu je tento účet sice zřízen, ale zároveň zakázán. Je na administrátorovi, zda tento účet dovolí používat a co uživatelům tohoto účtu povolí.

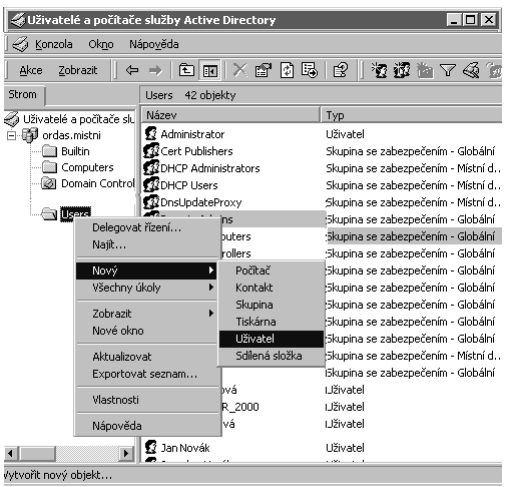
  Ke každému uživatelskému účtu patří (stejně jako u desktopových Windows) také uživatelský profil – viz kapitola *Uživatel, skupina a uživatelský účet*.

Tip: Při běžné práci by se administrátor měl přihlašovat k účtu postačujícímu k běžné práci, ale s nižším oprávněním než Administrátor. Vyhnete se tak nechtěným zásahům do konfigurace sítě.

Vytvoření účtu

Pro práci s účty je určen kontejner *Users* modulu *Uživatelé a počítače služby Active Directory* (*Start/Nástroje pro správu*). V levé části obrazovky konzoly nejdříve klepneme pravým tlačítkem myši na kontejner *Users*, v menu vybereme *Nový* a *Uživatel*. Tím vyvoláme průvodce tvorbou nového účtu. Na první obrazovce, věnované identifikaci uživatele, najdeme řádky:

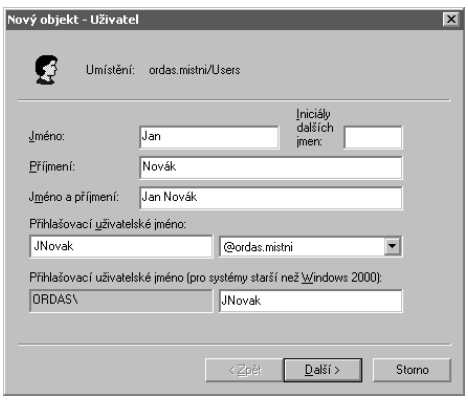
- **Jméno:** určen pro jméno uživatele účtu.
- **Příjmení:** pro příjmení uživatele. (Jeden z prvních dvou řádků musí být vyplněn!)
- **Jméno a příjmení:** celé jméno uživatele, které sem systém doplní automaticky. Tento údaj se bude zobrazovat v organizační jednotce, v níž je účet vytvořen.
- **Přihlašovací uživatelské jméno:** je nejdůležitějším údajem na obrazovce. Je to jméno, jímž se bude uživatel přihlašovat k Windows Serveru. V rámci Active Directory musí být uživatelské jméno jedinečné.



Obrázek 4.25: *Spuštění průvodce pro tvorbu nového uživatele*

Po stisku tlačítka Další přejdeme do druhého dialogového okna, jež je věnováno požadavkům na heslo:

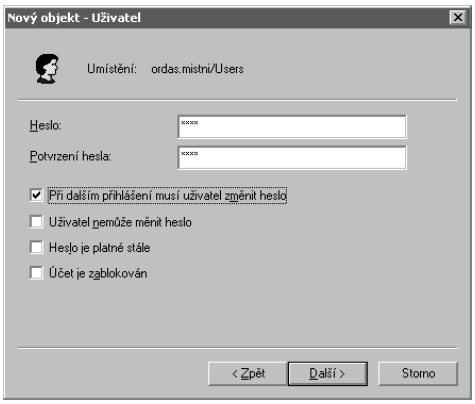
- Řádky **Heslo, Potvrzení hesla** slouží pro zadání hesla, kterým se bude uživatel identifikovat při přihlášení do systému. Abychom měli jistotu, že jsme heslo zapsali správně (místo znaků hesla se zobrazují hvězdičky), je nutné je shodně zapsat do obou řádků.
- **Při dalším přihlášení musí uživatel změnit heslo:** Při prvním přihlášení bude muset uživatel změnit námi zadané heslo. Stane se tak jediným, kdo heslo zná. Tato volba by měla být nejčastější.
- **Uživatel nemůže změnit heslo:** změnu hesla může provést pouze Administrátor. Tato možnost se doporučuje především pro společné účty, používané více lidmi.



Obrázek 4.26: *Identifikační obrazovka uživatele*

- **Heslo je stále platné:** heslo nebude možné změnit. Kvůli vyšší bezpečnosti účtu by se heslo mělo pravidelně měnit.
- **Účet je zablokován:** k účtu nebude možné se přihlásit. Má význam pro účet zaměstnance, který ještě nenastoupil, či je dlouhodobě nepřítomný.

Základním prvkem zabezpečení ve Windows jsou skupiny (viz kapitola *Skupiny*). Nového uživatele bychom měli okamžitě zařadit do některé ze skupin. Klepneme pravým tlačítkem myši na příslušném objektu uživatele a vybereme *Vlastnosti*. Na kartě *Je členem* vidíme skupiny, do nichž je uživatel zařazen. Pro zařazování do skupin máme k dispozici tlačítko *Přidat*. Za skupiny můžeme účet vyřadit tlačítkem *Odebrat*.



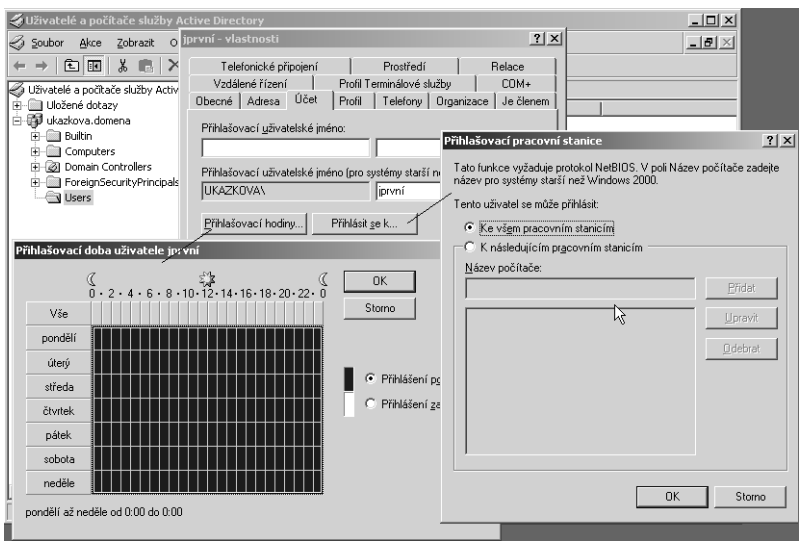
Obrázek 4.27: *Obrazovka hesla*

Restrikce účtů

Pro účty v doméně můžeme stanovit restrikce – omezení, která budou platit pro určitý účet. Restrikce jsou dvě:

- *přihlašovací hodiny* – jimiž zadáváme, v jaké době se bude moci uživatel hlásit do domény,
- *přihlásit s k...* – čímž stanovujeme, k jakým stanicím v doméně se bude moci uživatelský účet přihlásit.

Restrikce nastavíme v konzole *Uživatelé a počítače služby Active Directory*, kde otevřeme kontejner *Users*. V pravé části obrazovky poklepeme na účet (jemuž restrikci přidělíme). Otevřeme obrazovku vlastností účtu a přejdeme na kartu *Účet*. Zde již máme k dispozici tlačítka pro přidělení restrikce (viz obrázek).



Obrázek 4.28: *Restrikce*

Silná hesla

Heslo je jedním z nejdůležitějších prvků bezpečnosti, může se však stát nejslabším místem zabezpečení počítače. Pro odhalení hesla se používá software, jímž (pokud je k dispozici dostatek času) lze odtajnit jakékoli heslo. Proto je dobré používat silná hesla, která se v pravidelných intervalech mění. Silná hesla splňují několik kritérií, která znesnadňují jejich dešifrování. Odhalení silného hesla tak může trvat několik měsíců. Za silné se považuje heslo splňující následující kritéria:

- V důsledku principů šifrování jsou nejbezpečnější hesla obsahující 7 nebo 14 znaků. Silné heslo se tedy skládá nejméně ze sedmi znaků.

- Obsahuje znaky ze všech tří následujících skupin: *Písmena* (velká a malá), *Číslice*, *Symboly* (všechny znaky kromě písmen a číslic, např.: @ # $ % ^ & * ( ) _ +).
- Obsahuje nejméně jeden symbol umístěný na druhé až šesté pozici.
- Hesla je dobré měnit v určitém intervalu, nové heslo se musí výrazně lišit od hesel předchozích.
- Neobsahuje uživatelské jméno, ani jméno či příjmení uživatele účtu.
- Nejedná se o běžné slovo nebo jméno.

Hesla systému Windows mohou obsahovat až 127 znaků. Jestliže však používáte ve své síti ještě Windows 98, je vhodné používat hesla nejvýše o 14 znacích.

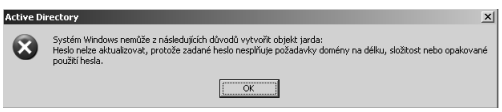
Při práci s heslem se řiďte těmito pravidly:

- Heslo nikam nezapisujte.
- Nikdy nesdělujte heslo jiným osobám.
- Heslo pro přihlášení k síti nikdy nepoužívejte k jinému účelu.
- Používejte jiné heslo pro přihlášení k síti a jiné pro přihlášení k účtu správce počítače.
- Heslo měňte každých 60 až 90 dnů nebo tak často, jak odpovídá vašim konkrétním potřebám.
- Pokud si myslíte, že heslo bylo prozrazeno, okamžitě je změňte.

Měli byste si také dát pozor na to, kam heslo v počítači ukládáte. Některá dialogová okna, jako například okna pro vzdálený přístup a telefonická připojení, umožňují uložení nebo zapamatování hesla. Tuto možnost raději nepoužívejte.

Úprava zásad hesel a účtů

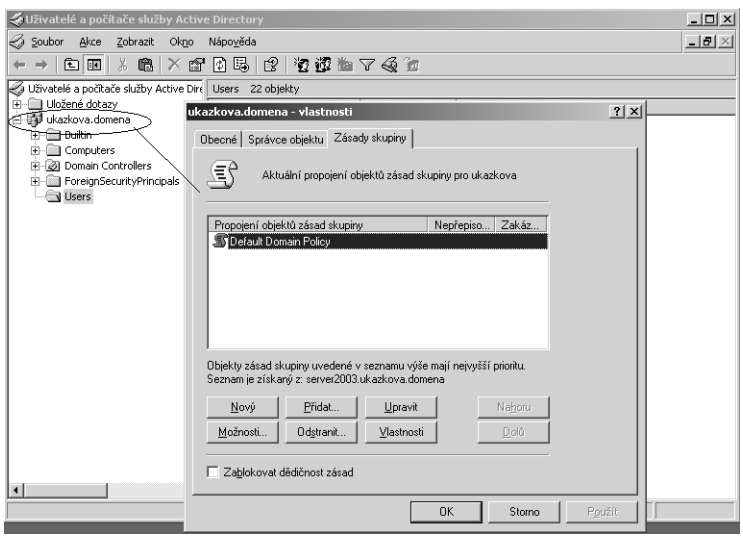
Windows Server 2003 má po instalaci nastaveny zásady pro silná hesla. Pokud je při tvorbě účtu nedodržíme, nedovolí nám Windows Server 2003 účet zřídit.



Obrázek 4.29: *Reakce na nedodržení silného hesla*

Vlastnosti účtu a hesla bychom neměli měnit bez úvahy, ale pokud máme důvod (ať k zesílení, nebo zeslabení) bezpečnostních zásad, můžeme to udělat následujícím způsobem:

- Otevřeme nástroj *Uživatelé a počítače služby Active Directory* (*Start/Nástroje pro správu).*
- Bezpečnostní zásady se nastavují pro doménu nebo její organizační jednotku. Ve stromu konzoly klepneme pravým tlačítkem myši na doménu nebo organizační jednotku, vybereme příkaz *Vlastnosti* a přejdeme na kartu *Zásady skupiny.*
- Zde v okně *Propojení objektů zásad skupiny* uvidíme *Objekty zásad skupiny* (po instalaci je jediný – *Default Domain Policy*). Na objekt poklepeme (případně použijeme tlačítko *Upravit*) a otevřeme *Editor objektů zásad skupiny.*



Obrázek 4.30: *Objekty zásad*

- Zde již můžeme zásady přímo ovlivňovat. V *Editoru zásad* postupně otevřeme kontejnery *Nastavení systému Windows / Nastavení zabezpečení / Zásady účtů*.

Tady nastavujeme parametry, které upravují pravidla pro tvorbu hesel uživatelských účtů. Tato pravidla budou obecně platná pro hesla všech uživatelů v doméně. Hodnotu položky měníme poklepáním levého tlačítka myši na řádek hodnoty (v pravém okně konzole), ovlivnit můžeme tyto položky:

Úprava zásad hesel

V kontejneru *Zásady hesla* zadáváme:

Heslo musí splňovat požadavky na složitost

Jestliže je tato zásada povolena, musí být při vytváření a úpravách hesel splněny minimálně následující požadavky (v podstatě požadujeme vytvoření *Silného hesla* – viz kap. *Zásady pro práci s hesly*):

- Heslo nesmí obsahovat celý nebo část názvu uživatelského účtu.
- Musí mít délku alespoň šesti znaků.
- Musí obsahovat znaky ze tří z následujících čtyř kategorií: velká písmena anglické abecedy (*A* až *Z*), malá písmena anglické abecedy (*a* až *z*), 10 základních číslovek (*0* až *9*), nealfanumerické znaky (například *!, $, #, %*).

Maximální stáří hesla

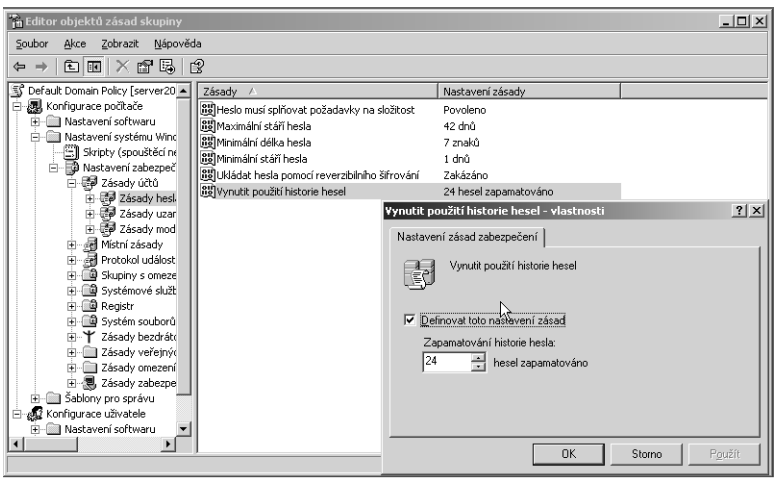
Určuje dobu (zadanou ve dnech), po kterou smí být heslo používáno, než systém začne vyžadovat jeho změnu. Nastavitelné rozmezí dní (po kterých přestanou hesla platit) je od 1 do 999. Jestliže je počet dní nastaven na hodnotu 0, platnost hesla omezena není. Doporučuje se změna hesla po 30 až 90 dnech (nelze to však stanovit obecně, záleží na konkrétních podmínkách).

Důležité je dát uživateli čas na změnu starého hesla – upozornit ho na to, že jeho heslo zanedlouho vyprší (např. 10 dnů před ukončením platnosti hesla).

Minimální stáří hesla

Vymezuje nejkratší dobu (zadanou ve dnech), po kterou musí být heslo používáno, než je uživatel může změnit. Hodnotu můžete nastavit v rozmezí od 1 do 999 dnů. Pokud nastavíte hodnotu 0, může být heslo změněno okamžitě.

Minimální stáří hesla musí být menší než *Maximální stáří hesla*. Jestliže chcete, aby byla platná možnost *Vynutit historii hesla*, nakonfigurujte nejnižší stáří hesla na hodnotu větší než 0.



Obrázek 4.31: *Editor objektů zásad*

Minimální délka hesla

Stanovuje nejnižší počet znaků, který může obsahovat heslo uživatelského účtu. Hodnotu můžete nastavit v rozmezí od 1 do 14 znaků. Nastavením počtu znaků na hodnotu 0 zařídíte, aby nebylo vyžadováno žádné heslo. Z hlediska šifrování jsou nejvhodnější hesla o délce 7 nebo 14 znaků.

Vynutit použití historie hesel

Tato zásada zajistí, aby nebyla opakovaně používána stará hesla. Určuje počet jedinečných nových hesel, která musí být přiřazena uživatelskému účtu před tím, než může být znovu použito staré heslo. Počet hesel je z rozmezí 0 až 24.

Bude-li hodnota Minimální délka hesla nízká, mohlo by dojít k opakování hesla velmi brzo a vynucení historie hesel by tak ztrácelo význam.

Zásady zamknutí účtů

Zadáváme jimi, co se stane po neúspěšném přihlášení k některému z účtů (může to znamenat pokus o průnik). V podstatě stanovujeme počet neúspěšných pokusů o přihlášení, po nichž dojde k uzamčení účtu.

Prahová hodnota pro uzamknutí účtu

Po zde stanoveném počtu neúspěšných pokusů pro zadání hesla bude účet uživatele uzamčen. Uzamčený účet nelze použít, dokud není znovu odemčen správcem nebo dokud nevyprší doba uzamčení účtu. Počet neúspěšných pokusů můžete nastavit v rozmezí od 1 do 999. Pokud nastavíte hodnotu 0, účet nebude nikdy uzamčen.

Neúspěšné pokusy při zadávání hesla na pracovních stanicích, které byly uzamčeny pomocí kombinace kláves CTRL+ALT+DEL (nebo pomocí spořiče obrazovky chráněného heslem) se nepočítají jako neúspěšné.

Doba uzamčení účtů

Určuje počet minut, po který uzamčený účet zůstane uzamčený, než se znovu automaticky odemkne. Přípustné hodnoty jsou v rozmezí od 1 do 99999 minut. Nastavením hodnoty na 0 dosáhneme toho, že účet bude moci odemknout pouze správce.

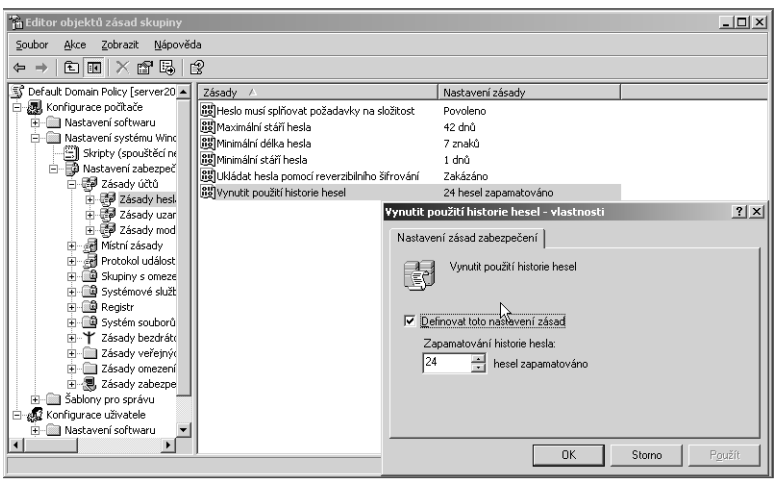
Vynulovat čítač pro zamknutí účtů po

Určuje počet minut, které musí po neúspěšném zadání hesla uběhnout před tím, než je čítač počtu neúspěšných pokusů nastaven na 0. Přípustné rozmezí je od 1 do 99999 minut.

Jestliže je nastavena prahová hodnota uzamčení účtu, musí být tato doba menší nebo rovna *Době uzamčení účtu*. Ve výchozím nastavení je *Prahová hodnota pro uzamknutí účtu* nastavena na 0 a zbylé dvě zásady nemají význam.

Řádkový příkaz pro vypsání stavu zásad zabezpečení

Momentální hodnoty bezpečnostních zásad ukazuje MMC konzola *Zásady skupiny*. Můžeme je však velmi snadno vypsat na obrazovku příkazem *NET ACCOUNTS*. Přes *Start / Spustit* a příkaz *cmd* vyvoláme obrazovku *Příkazového řádku*. Napíšeme příkaz *NET ACCOUNTS* a stiskneme *Enter*. V okně *Příkazového řádku* uvidíme momentální stav zabezpečení.

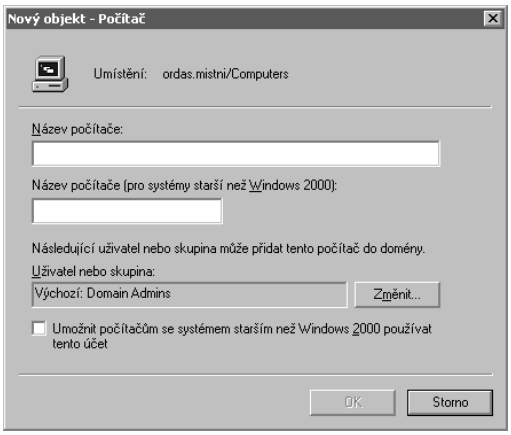


Obrázek 4.32: *Zásady účtů*

Účty počítačů

Mnoho činností (sdílení složek, propojování skupin, vzdálená správa) probíhá v doméně pouze tehdy, je-li počítač členem domény. Proto každý počítač používající systém Windows 2000 či XP, který je připojen do domény, má svůj účet počítače. Účty počítačů, podobně jako účty uživatelů, vidíme v nám již známé konzole *Uživatelé a počítače služby Active Directory* (*Start/Ovládací panely*).

Účet počítače se vytváří automaticky, při připojování počítače do domény (viz kapitola *Přihlášení uživatele k systémům Windows Server)*. Můžeme jej vytvořit také „ručně" (postup je velmi podobný vytvoření uživatelského účtu): V levém okně konzoly *Uživatelé a počítače služby Active Directory* klepneme pravým tlačítkem myši na kontejner *Computers*, vybereme *Nový* a *Počítač*. Na následující konfigurační obrazovce musíme zadat název počítače. Ten by se měl shodovat se jménem konkrétního počítače. (Pravé tlačítko myši na ikoně *Tento počítač / Vlastnosti* karta *Název počítače*, tlačítko *Identifikace v síti*).



Obrázek 4.33: *Základní údaje počítačového účtu*

Poznámka: *Počítače se systémy Windows 98 nemají tak vyspělé zabezpečovací funkce a nelze jim v doménách systémů Windows Server přiřadit účty počítačů. Je však možné se z nich přihlásit do sítě a používat je v doménách služby Active Directory.*

Skupiny

Obecně je skupina množinou několika uživatelských účtů. Předností skupiny je snadné přidělení určitých vlastností více uživatelům. Toho plně využívají právě serverové operační systémy Windows Server. Ty při své instalaci vytvářejí předdefinované skupiny, jimž dopředu přidělují vlastnosti a oprávnění. Administrátor sítě pak může přiřazovat uživatele do již připravených skupin, což mu značně zjednoduší správu. Skupiny tedy představují jeden ze základů administrace sítě Windows Server. (Stejný princip je možné využít pro místní skupiny stanic desktopových Windows XP Professional.)

Rozsahy skupin

Víme, že síťové objekty jsou zařazeny do domén, že v rámci jedné velké sítě může být několik domén (sjednocených prostřednictvím Active Directory), že skupiny jsou použity také ke správě jednotlivých počítačů. Takovéto uspořádání sítě kopírují také skupiny, které mohou mít různé rozsahy působnosti, popsané v tabulce.

Tabulka 4.5: Rozsah skupin v rámci sítě Windows Server

Rozsah skupiny	Obvyklé použití	Je možné přiřadit účty	Přístup k síťovým prostředkům
Místní doménová	Pro přidělení oprávnění k prostředkům	Je možné sem přiřadit účet z jakékoliv domény	Je možné přidělit oprávnění k prostředkům jedné domény
Globální	Organizace uživatelů s podobnými požadavky na přístup k síti	Můžeme přiřadit účet uživatele jen z té domény, v níž je skupina vytvořena	Oprávnění k síťovým prostředkům libovolné domény

Univerzální	Přidělení oprávnění k podobným prostředkům v různých doménách	Je možné sem přiřadit účet z jakékoliv domény	Oprávnění k síťovým prostředkům libovolné domény

Naše kniha se zabývá jednoduchými sítěmi LAN, v nichž je pouze jedna doména. Při tvorbě skupin však budeme dotazováni na rozsahy skupin, a tak jsme si alespoň stručně tuto problematiku vysvětlili.

Předefinované skupiny

Již víme, že skupiny jsou jedním ze základních pilířů administrace Windows Serveru. Systém administrátorovi ulehčuje práci, protože při instalaci již skupiny vytvoří, přidělí jim oprávnění a předurčí je pro určité typy účtů.

Podle síťového prostředí (hlavně počet domén) se můžeme setkat s několika kategoriemi skupin:

- **Univerzální skupiny:** se používají ve vícedoménových strukturách velkých sítí.
- **Systémové skupiny:** nejsou v nich umístěny konkrétní uživatelské účty, ale zastupují různé uživatele podle toho, jak uživatelé k počítači přistupují.

Místní skupiny počítače

Platí pouze pro jeden počítač, na němž jsou také uloženy. Definují oprávnění pro práci pouze s tímto počítačem. U sítí peer to peer jsou k dispozici pouze místní skupiny, příslušné vždy jednomu PC s Windows XP Professional. (Pokud na desktopové stanici pracujeme ve *Zjednodušeném sdílení souborů*, jsou k dispozici pouze skupiny *Správce počítače* a s *Omezeným přístupem*. Vypneme-li zjednodušené sdílení, budeme moci skupiny používat.)

skupina	*určení, oprávnění*
Guests	„Nejslabší" skupina, je určena pro přihlašování příležitostných uživatelů. Po instalaci je vypnuta. Její zapnutí a přidělení oprávnění je na úvaze (a potřebách) administrátora stanice.
Users	Její účty mají k většině součástí systému oprávnění číst. Každý uživatel má na disku vlastní složky. K nim mají členové skupiny oprávnění číst a mazat. Nemohou instalovat programy, ani provádět správu PC.
Power Users	Mohou instalovat aplikace a provádět správu PC (např. měnit místní uživatelské účty).
Backup Operators	Mohou zálohovat a obnovovat soubory prostřednictvím programu Microsoft Backup.
Administrators	Členové této skupiny mají úplnou kontrolu nad operačním systémem.

Místní skupiny domény

Používají se pro přidělování oprávnění ke sdíleným prostředkům jakéhokoliv počítače v doméně. Skupiny Operators definují oprávnění k určitým činnostem na serveru.

skupina	*určení, oprávnění*
Guests	Členové této skupiny mohou provádět jen ty úkoly, které jim povolí správce (při instalaci neobdrží žádná oprávnění).
Users	Mohou dělat jen to, co jim povolí správce. Správce definuje jejich oprávnění. Používá se pro přidělení těch oprávnění, která by měl mít každý účet v doméně.
Account Operators	Mohou konfigurovat uživatelské účty, nemají povolenou práci s účty skupin Administrators a Operators.

Server Operators	Mohou sdílet diskové prostředky (složky, soubory), zálohovat a obnovovat soubory na serveru – řadiči domény.
Print Operators	Mohou instalovat a spravovat tiskárny na serverech – řadičích domény.
Backup Operators	Mohou zálohovat a obnovovat soubory prostřednictvím programu Microsoft Backup na všech serverech – řadičích domény.
Administrators	Mohou provádět veškeré úkony na všech počítačích v doméně.

Globální skupiny

Po připojení do domény se tyto skupiny přidávají do skupinových účtů místních nebo doménových skupin. Oprávnění přidělená této skupině se tak „roznesou“ na celou doménu.

skupina	*určení, oprávnění*
Domain Guests	Ve výchozím stavu je zakázána. Přidává se automaticky do Místní doménové skupiny Guests.
Domain Users	Automaticky se přidává do Místní skupiny Users, členy této skupiny se stávají všechny doménové uživatelské účty.
Domain Admins	Automaticky se přidává do Místní doménové skupiny Administrators.
Enterprise Admins	Sem přiřazení uživatelé mohou spravovat celou síť. Ve výchozím stavu sem jsou zařazeny všechny Místní doménové skupiny Administrators.

Systémové skupiny:

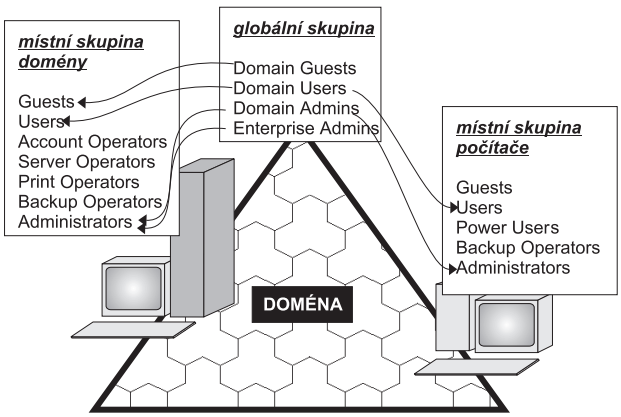
Existují na všech počítačích systémů Windows 2000. Reprezentují určité skupiny uživatelů, podle toho jak momentálně přistupují k PC. Tyto skupiny nejsou viditelné při správě skupin, ale je možné je použít při přidělování oprávnění k prostředkům. Skupiny nelze smazat, ani jinak ovlivňovat.

skupina	*členové*
Everyone	Patří sem všichni uživatelé momentálně pracující s PC.
Authenticated Users	Patří sem všichni uživatelé momentálně pracující s PC, jejichž připojení bylo ověřeno účtem na místním počítači nebo v Active Directory. Je to obdoba skupiny Everyone, ale nejsou v ní anonymně přihlášení!
Creator Owner	Reprezentuje uživatele – vlastníka nějakého prostředku (vlastníkem je zpravidla ten, kým byl prostředek vytvořen).
Network	Všichni uživatelé momentálně připojení ke sdíleným prostředkům ze sítě.
Interactive	Jde o skupinu dosahující interakce s PC. Patří sem všichni, kteří jsou fyzicky přihlášeni k tomuto PC. Ne však ti, kteří přistupují k některému sdílenému prostředku ze sítě.
Anonymous Logon	Uživatelské účty neověřené Windows.
Dialup	Uživatelé momentálně používající telefonické připojení.

Tip: Při použití účtu Guest a Everyone je nutná opatrnost. Guest je totiž automaticky členem skupiny Everyone a přebírá její oprávnění!

Spolupráce skupin

Přidáním počítače do domény dojde k propojení skupin. *Globální skupiny* se nainstalují do *Místní skupiny* domény i počítače. Také *Místní skupina domény* nainstaluje některé ze skupin do *Místní skupiny počítače*. Automaticky se tak přenesou oprávnění nadřazených skupin na skupiny místní. Přesné propojení skupin ukazuje obrázek.



Obrázek 4.34: *Propojení skupin po začlenění PC do domény*

Z obrázku vyplývají určitá pravidla:

- Přidáme-li uživatele do *Globální skupiny Domain Users*, stává se automaticky členem skupiny *Users* v *Místní skupině počítače* – je členem skupiny *Users* všech PC. Zároveň je členem *Místní doménové skupiny Users* – je členem skupiny *Users* ve všech doménách.
- Výše uvedená závislost platí i pro členy skupiny *Domain Admins*.
- Uživatel *Globální skupiny Domain Guests* se stává členem všech *Místních doménových skupin Guests*, ale nepronikne do skupiny *Guests* na jednotlivých počítačích.
- Výše uvedená závislost platí i pro členy skupiny *Enterprise Admins*.

Práce se skupinami

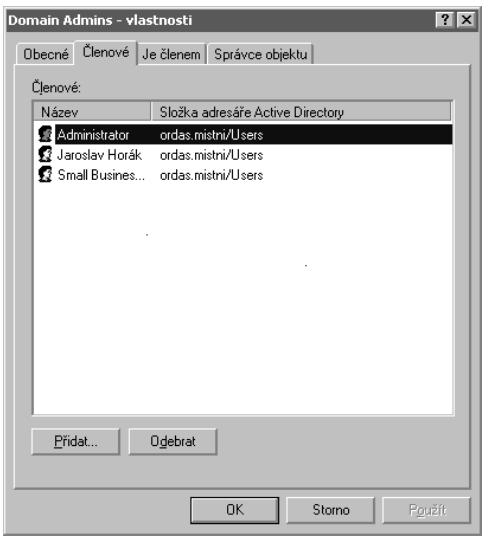
Předdefinované skupiny

Na serveru si otevřeme stejnou konzolu jako pro práci s jednotlivými uživateli – *Uživatelé a počítače služby Active Directory* (*Start/Nástroje pro správu*). Můžeme přiřazovat uživatele do skupiny, nebo si otevřít seznam členů skupiny a rozšířit je o další účet.

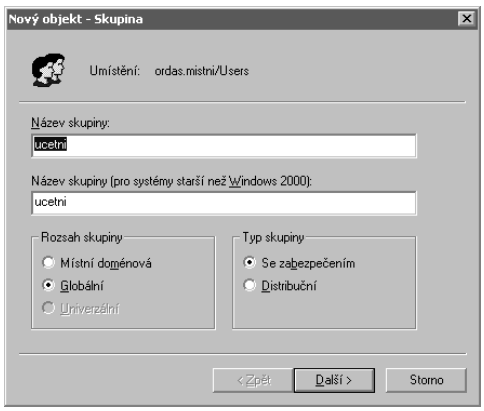
- Pokud klepneme pravým tlačítkem myši na uživatelský účet (v pravém okně konzoly) a vybereme *Vlastnosti*, můžeme na kartě „*Je členem*“ tlačítky *Přidat* či *Odebrat* měnit skupiny, do nichž bude uživatel patřit.
- Pokud klepneme pravým tlačítkem myši na účet některé skupiny a vybereme *Vlastnosti*, můžeme na kartě *Členové* přidávat či odebírat členy skupiny. (Tlačítka *Přidat*, *Odebrat*).

Poznámka: *Skupiny jsou systémem umístěny v několika kontejnerech: Builtin (předdefinované místní skupiny domény) a Users (společné globální skupiny).*

Obrázek 4.35: *Skupiny, v nichž je uživatel členem*



Obrázek 4.36: *Členové skupiny Domain Admins*



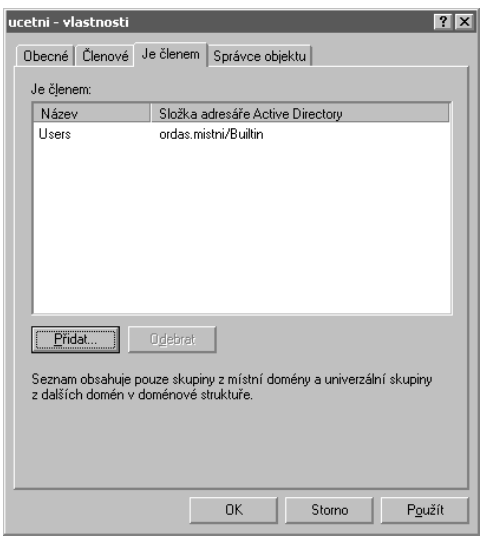
Obrázek 4.37: *Základní údaje skupiny*

Vlastní skupiny

Administrátor může v případě potřeby vytvořit vlastní skupinu, zařadit do ní uživatelské účty a přidat oprávnění ke sdíleným prostředkům. V levém okně konzoly *Uživatelé a počítače služby Active Directory* klepneme pravým tlačítkem myši na kontejner, do něhož novou skupinu umístíme (např. kontejner *User* pro novou globální skupinu). Vybereme *Nový objekt* a *Skupina* (postup je podobný tvorbě nového uživatele). Na obrazovce zadáme název a rozsah skupiny.

Nová skupina má význam jen tehdy, pokud do ní doplníme uživatele (viz předešlý odstavec). K nové skupině je možné přiřadit některou z předdefinovaných skupin. Všichni členové nové skupiny tak zdědí vlastnosti standardní skupiny. Použijeme k tomu kartu *Je členem* z *Vlastností skupiny*.

Tip: Přidávání skupiny do skupiny nazýváme zanořováním. Zanořováním se zrychluje přidělování oprávnění, ale ztrácí se přehled o tom, v jaké skupině je který uživatel (a jaká tedy má oprávnění – jež získal od zanořených skupin). Snažte se proto používat maximálně jedno zanoření.



Obrázek 4.38: *Přiřazení skupiny do jiné skupiny*

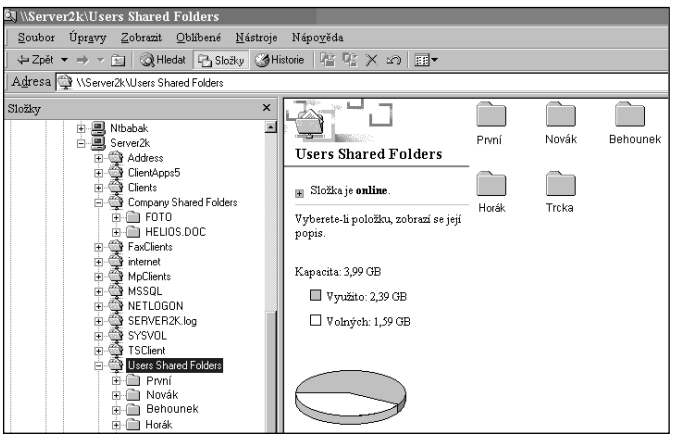
Sdílení složek

Zpřístupnění složek více uživatelům je jednou ze základních činností v síti. Nyní se pozastavíme u některých pravidel sdílení v sítích Windows Server (většina těchto pravidel platí také pro stanici Windows XP Professional, pracující v rozšířeném režimu sdílení).

Ve Windows Serveru 2003 můžeme sdílení složek použít až po definici role souborový server (kapitola *Role Souborový server*).

Pohled na server ze stanice

Poklepeme-li z libovolného počítače na ikonku serveru (uvidíme ji v *Okolních počítačích*, či *Místech v síti*, nebo *Průzkumníkovi*), otevře se pohled pouze na sdílené složky serveru. (Uživatel nevidí ani disky ani složky, v nichž jsou složky uloženy.) Pohled na složky se samozřejmě liší podle oprávnění, která má přidělena uživatel (a hlavně skupina, v níž je zařazen).



Obrázek 4.39: *Pohled na server Windows 2000*

aktualizovat obrázek?

2003????

Pohled na Windows Server 2003 ukazuje obrázek. Vidíme zde řadu sdílených složek. Ty se jednak instalují automaticky, podle aplikací nahraných na server, jednak je zde vytváří Administrátor. Automaticky jsou například vytvářeny složky *Company Shared Folders* a *User Shared Folders*. Do první z této dvojice mají přístup všichni. Ve složce *User Shared Folders* najdeme složky jejichž název se shoduje se jmény jednotlivých uživatelů. Ti pak mají přístup pouze do „svých" složek.

Tip: Uživatel vidí všechny sdílené složky, ale zpravidla nemá oprávnění všechny otevírat!

Systémová pravidla pro sdílení složek

V síti Windows Server je sdílení složek závislé na tom, zda počítač, z něhož do sítě vstupujeme, je členem domény, nebo pracovní skupiny. Dalším důležitým faktorem je zařazení uživatele do některé z předdefinovaných skupin.

- V doméně Windows Server mohou uživatelé skupin *Administrators* a *Server Operators* sdílet složky na jakémkoliv počítači.
- V doméně Windows Server mohou uživatelé skupiny *Power Users* (jde o místní skupinu) sdílet složky na serveru, nebo na počítači s operačním systémem Windows XP Professional, kde je skupina umístěna.
- V pracovní skupině Windows mohou uživatelé skupin *Administrators* a *Power Users* sdílet složky na serveru, nebo na počítači s operačním systémem Windows XP Professional, kde je skupina umístěna.

Pro sdílení složek nestačí být jen ve správné skupině, ale skupina musí mít přiděleno patřičné *oprávnění* (Oprávněním definujeme, kdo může se složkou pracovat – této problematice je věnována další kapitola.)

Sdílené složky pro účely správy systému

Aby bylo možné operační systém spravovat, je definováno automatické sdílení některých složek. Takto sdílené složky mají na konci názvu sdílení připojen znak dolar *$*. Složky s dolarem nejsou vidět z *Průzkumníka* (nebo *Okolních počítačů*), ale lze je namapovat. Automatické sdílení je nastaveno:

- ke kořenovým složkám každého svazku (název takových složek pak je např. *C$, D$*),
- ke složce, v níž je nainstalován operační systém. Zpravidla jde o složku serveru C:\Windows, která je sdílena pod názvem *Admin$*,

- ke složce s ovladači tiskáren. Ta bývá umístěna ve složce *C:\Windows\System32\Spool\Drivers*. V síti je sdílena pod názvem *Print$*. Vytváří se při instalaci první sdílené tiskárny.

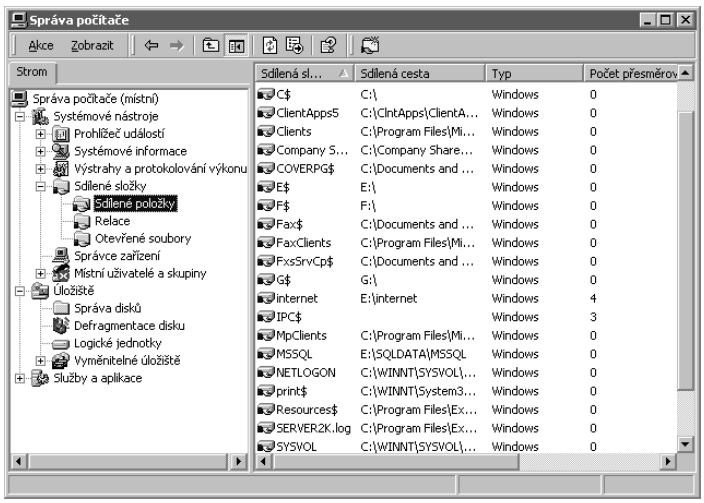
  Poznámka: *Pro práci se složkami je nutné patřičné oprávnění (minimálně Číst). (Oprávněním se zabývá následující kapitola.)*

Práce se sdílenými složkami

Sdílení i oprávnění přidělujeme každé složce individuálně. To může být někdy problematické, protože musíme každou složku vyhledat a teprve pak s ní pracovat. Windows Server nabízí konfigurační konzolu *Sdílené složky* (*Start/Nástroje pro správu/Správa počítače*). V ní jsou soustředěny všechny sdílené složky, což zjednodušuje jejich správu (např. přidělování oprávnění). Na obrázku vidíme řadu složek sdílených pro účely správy systému (jsou zakončeny $). Ty při připojení ze stanice nevidíme a ani je nemůžeme administrovat.

Ve Windows Serveru 2003 můžeme definovat sdílení složek také prostřednictvím obrazovky *Správa serveru* (kapitola Role Souborový server).

Poznámka: *Sdílet můžeme rovněž celý disk, ale z hlediska bezpečnosti a kontroly přístupu to není šťastné řešení.*



Obrázek 4.40: *Sdílené složky*

Oprávnění ke složkám a souborům

Základem práce každého správce serveru je vytváření uživatelských účtů a definování pravidel pro práci se složkami. Je nutné stanovit který uživatel bude moci se složkou pracovat a co mu bude v konkrétní složce dovoleno. V operačních systémech Windows se možnosti práce jednotlivých uživatelů (a skupin) ve složkách definují prostřednictvím *Oprávnění*. Přidělením oprávnění definujeme přesné možnosti práce ve složce.

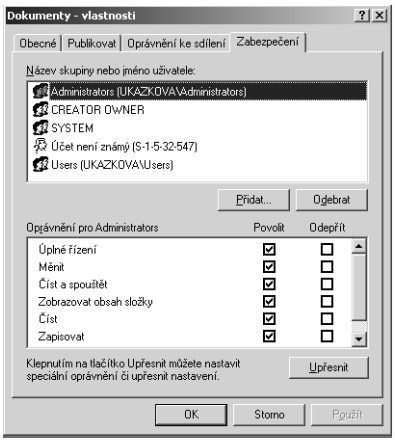
Nejdříve je nutné vysvětlit si, jaká pravidla pro tvorbu oprávnění platí. Oprávněními se řídí dva druhy uživatelů, místní (přistupující k PC lokálně, střídající se u počítače) a síťoví (přistupující k PC z vnějšku, ze sítě). Pro každý typ uživatele se oprávnění tvoří jiným způsobem:

- ***Místní*** uživatelé mají oprávnění přidělené přímo, definujeme je na kartě *Zabezpečení* (přesný postup si ukážeme později), používá se pro ně označení *Oprávnění NTFS*.
- Oprávnění ***Síťových*** uživatelů se skládá ze dvou částí: z *Oprávnění ke sdílení* a z *Oprávnění NTFS*.

  Poznámka: *Podobné vlastnosti jako oprávnění mají také atributy, i ony omezují možné činnosti se složkami a soubory. Na rozdíl od oprávnění však jejich omezení platí plošně, pro všechny (viz Souborový systém/Atributy).*

Základní oprávnění – Oprávnění NTFS

Jsou zabezpečením složky, vycházejícím ze souborového systému NTFS a platí nejen pro síťové uživatele, ale i pro uživatele přistupující z místního počítače. Oprávnění se dědí na podsložky a soubory. Oprávnění můžeme definovat také pro jednotlivé soubory ve složce. Každému uživateli (skupině) můžeme přidělit oprávnění pro práci ve složce (nebo se souborem). Základní oprávnění jsou *Úplné řízení, Změnit, Číst a spouštět, Zobrazovat obsah složky, Číst* a *Zapisovat*. Jejich přehled a povolené činnosti, které oprávnění umožňují, ukazuje tabulka. Tato oprávnění přidělujeme na kartě *Zabezpečení* a platí pro místní a síťové uživatele. V případě síťových uživatelů se *Oprávnění NTFS* kombinují s *Oprávněními ke sdílení*.



Obrázek 4.41: *Karta Zabezpečení místního sdílení*

Tabulka 4.6: Přehled oprávnění ve Windows

Zvláštní oprávnění	Úplné řízení	Měnit a spouštět	Číst obsah složky	Zobrazovat	Číst	Zapisovat
Přecházet složku Spouštět soubory	x	x	x	x		
Zobrazovat obsah složky Číst data	x	x	x	x	x	
Číst atributy	x	x	x	x	x	
Číst rozšířené atributy	x	x	x	x	x	
Vytvářet soubory Zapisovat data	x	x			x	
Vytvářet složky Připojovat data	x	x			x	
Zapisovat atributy	x	x			x	
Zapisovat rozšířené atributy	x	x			x	
Odstraňovat podsložky a soubory	x					
Odstraňovat	x	x				
Číst oprávnění	x	x	x	x	x	x
Měnit oprávnění	x					
Přebírat vlastnictví	x					

Oprávnění síťových uživatelů – Oprávnění ke sdílení

Přístup uživatelů ze sítě je řízen ještě jednou skupinou oprávnění – pro síťové uživatele. Tato oprávnění s přesným názvem: *Oprávnění ke sdílení* jsou pouze tři, platí jen pro uživatele přistupující ze sítě (nikoliv pro místní uživatele) a jejich význam ukazuje tabulka.

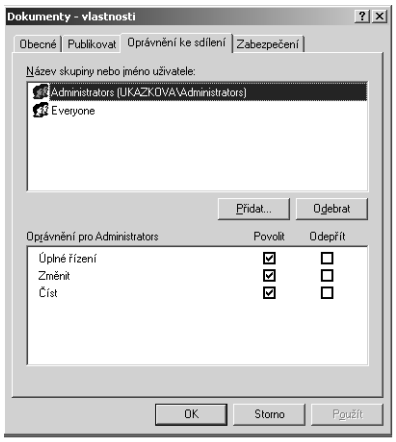
Tabulka 4.7: Přehled Oprávnění ke sdílení

oprávnění	umožňuje
Číst	zobrazení názvů souborů a podsložek, přecházení do podsložek, zobrazení dat v souborech, spouštění programů
Měnit	zahrnuje oprávnění *Číst*, a navíc umožňuje vytváření souborů a podsložek, změnu dat v souborech, odstraňování podsložek a souborů
Úplné řízení	je výchozí oprávnění každého nového sdílení, které vytvoříte. Úplné řízení zahrnuje všechna oprávnění *Číst* a *Měnit*

Celý systém funguje následujícím způsobem: přistupuje-li uživatel ke složce ze sítě, vyhodnotí systém jeho oprávnění a na jejich základě pak rozhodne, co bude tomuto uživateli dovoleno. Při tvorbě výsledného (někdy se používá termín *efektivního)* oprávnění se v principu provádí logický součin s *Oprávněními NTFS*. Uživateli jsou pak povolena ta oprávnění, jejichž součin byl 1.

Vše si ukážeme na příkladu, uživatel Jan má ke složce nastavena oprávnění takto:

- hodnota *Oprávnění ke sdílení* je Číst
- hodnota *Oprávnění NTFS* je *Úplné řízení*
- pokud obě dvě oprávnění porovnáme, vidíme, že místní oprávnění NTFS *Úplné řízení* umožňuje Janovi provádět ve složce všechny operace se soubory a složkami. Ale při přístupu ze sítě (až se do systému přihlásí svým jménem a heslem) bude pouze vidět názvy souborů a podsložek, bude moci přecházet do podsložek, číst soubory a spouštět programy. V tomto případě funguje *Oprávnění ke sdílení* jako jakási maska, filtrující (omezující) oprávnění ze sítě.



Obrázek 4.42: *Karta Oprávnění ke sdílení (pro přístup ze sítě)*

Systém může fungovat také opačně, opět si to ukážeme na příkladu. Tentokrát má Jan přidělena oprávnění takto:

- hodnota *Oprávnění ke sdílení* je *Úplné řízení*
- hodnota *Oprávnění NTFS* je *Číst*
- pokud obě dvě oprávnění porovnáme, vidíme, že místní oprávnění *Číst* umožňuje Janovi pouze vidět obsah složky a procházet složkami. Při přístupu ze sítě není nijak omezen, má přiděleno maximální oprávnění *Úplné řízení*. Výsledkem je to, že Janovo efektivní oprávnění odpovídá pouze oprávnění *Číst,* ať přistupuje k počítači místně, nebo ze sítě. V tomto případě je rozhodující oprávnění místní.

Role Souborový server

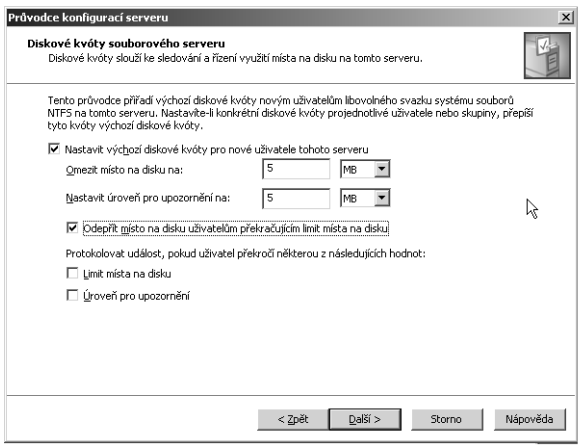
Síťový server může plnit více funkcí – nabízet více služeb. Každá taková služba však vyžaduje systémové prostředky, zabírá operační paměť a celkově namáhá operační systém. Windows Server 2003 umožňuje jednotlivé služby vypínat, či zapínat a tak si jej můžeme nakonfigurovat podle vlastních potřeb. Nastavení provádíme prostřednictvím obrazovky *Správa serveru*. Ta se otevírá ihned po startu Windows Serveru 2003, případně ji můžeme spustit přes tlačítko *Start / Nástroje pro správu*. Ve *Správě serveru* jsou nabízené služby serveru označovány jako *Role*. Role (služba) serveru organizující práci se soubory se označuje jako *Souborový server* (*File server*) a po instalaci Windows Serveru 2003 není aktivní. Prostřednictvím *Správy serveru* ji doinstalujeme.

V horní polovině obrazovky *Správa serveru* vidíme zelenou šipku s odkazem *Přidat nebo odebrat roli*. Jejím stiskem spustíme *Průvodce konfigurací serveru*. Jeho první obrazovka ukazuje přehled serverových rolí. Zároveň vidíme, která role je aktivní. Vybereme roli *Souborový server* a stiskneme tlačítko *Další*.

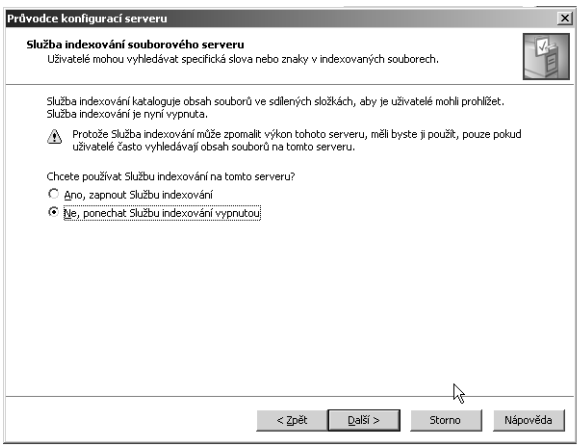
Ve druhé obrazovce Průvodce vyplníme údaje týkající se diskových kvót. Jejich význam známe z kapitoly *Diskové kvóty*.

Třetí obrazovka se týká indexování a všechny potřebné informace najdete na ní. Implicitní nastavení většinou není třeba měnit.

Obrázek 4.43: *Výběr role serveru*



Obrázek 4.44: *Nastavení diskových kvót*

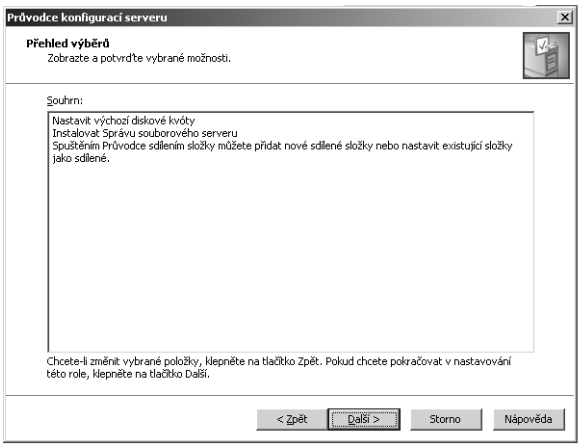


Obrázek 4.45: *Třetí obrazovka*

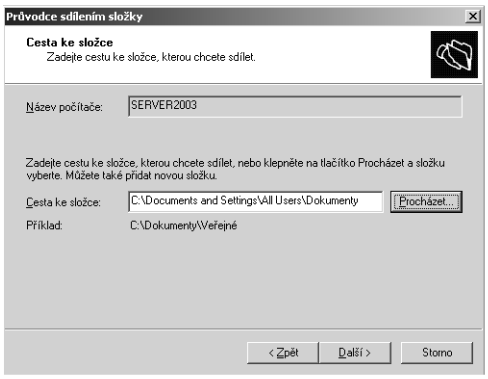
Ve čtvrté obrazovce jsme upozorněni na to, že bude spuštěn *Průvodce sdílením složky*. S jeho pomocí budeme nastavovat oprávnění složky.

V první obrazovce nás nový *Průvodce* pouze přivítá, ale ve druhé již musíme zadat cestu ke složce, kterou chceme nabízet.

Následující okno slouží k zadání popisu sdílené složky (popis uvidí uživatelé přistupující ze sítě).

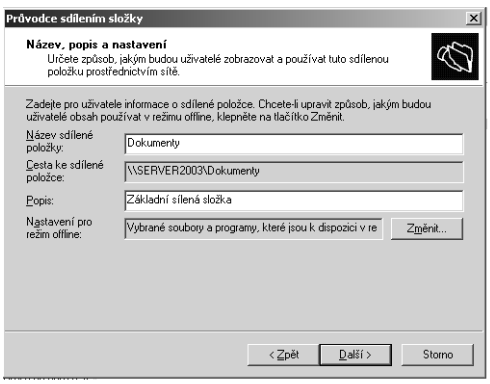


Obrázek 4.46: *Čtvrtá obrazovka*

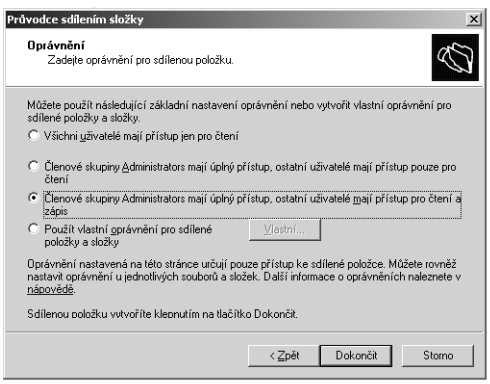


Obrázek 4.47: *Zadání cesty ke sdílené složce*

Další obrazovka *Průvodce* je zaměřena na přidělování oprávnění. Přesně jde pouze o *Oprávnění ke sdílení* – tedy o přístup ze sítě. Jednotlivé varianty sdílení jsou patrné z obrazovky.



Obrázek 4.48: *Popis sdílené složky*



Obrázek 4.49: *Přidělování oprávnění*

Poslední obrazovka *Průvodce sdílením* ukáže souhrn přidělených oprávnění a nabídne možnost spustit *Průvodce sdílením* znova a přidělit oprávnění dalším složkám. Tlačítkem *Zavřít* průvodce skončíme a role *Souborového serveru* je připravena k použití. Na obrazovce *Správa serveru* je možné *Průvodce sdílením složky* spustit kdykoliv, odkaz na něho vidíme v část *Souborový server*.

Poznámka: *Pokud chceme, aby náš server plnil roli řadiče domény, musíme ji také doinstalovat ve Správě serveru. (Je to spíše součástí instalace, kterou se v knize nezabýváme).*

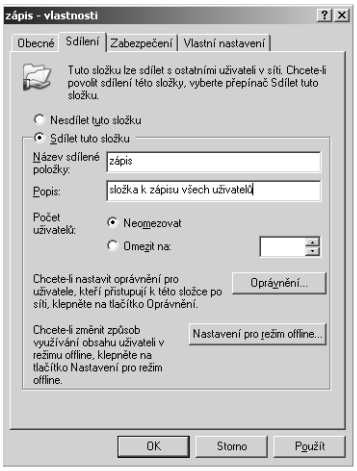
Práce s oprávněními

Ukázali jsme si několik způsobů jak s oprávněními pracovat, většinou šlo o práci prostřednictvím různých průvodců. Oprávnění je však často rychlejší přidělovat přímo, ve vlastnostech složky:

Definování síťového sdílení složky

Složku, kterou chceme nabízet do sítě, musíme nejdříve na disku najít (*Průzkumníkem*, nebo přes ikonku *Tento počítač*). Pak na ni klepneme pravým tlačítkem myši a z menu vybereme *Vlastnosti*. Na kartě *Sdílení* pak nastavíme vlastnosti pro použití složky jiným uživatelem:

- Zatrhneme možnost *Sdílet tuto složku* a v políčku *Název sdílené složky* ponecháme nabídnutou možnost (je shodná s názvem složky), do řádku *Komentář* můžeme přidat popis obsahu složky. Ten se bude zobrazovat na klientských PC.
- *Omezení počtu uživatelů* – lze definovat kolik uživatelů může současně se složkou pracovat, ale většinou tuto volbu nepoužíváme. Maximální hodnota současných připojení není neomezená, je však shodná s počtem klientských licencí serveru! (U počítačů s Windows XP Professional je současný počet připojení pro tiskové a souborové služby omezen na 10!)
- Tlačítkem *Oprávnění* definujeme *Oprávnění ke sdílení* (viz kapitola *Oprávnění síťových uživatelů – oprávnění ke sdílení*) týkající se uživatelů přistupujících ke složce ze sítě



Obrázek 4.50: *Nastavení sdílení*

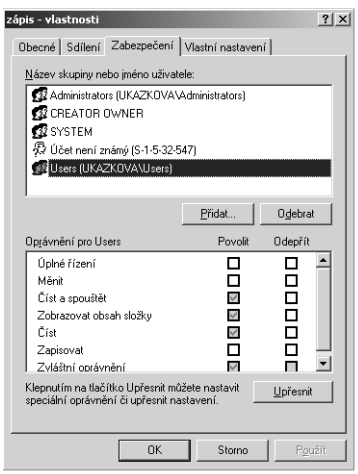
Tip: Pokud budeme tlačítko Oprávnění ignorovat, bude přiřazeno oprávnění Úplné řízení skupině Everyone. Každý bude mít ve složce úplná oprávnění! Definicí oprávnění NTFS však tuto vlastnost upravíme podle svých potřeb.

Přidělování oprávnění NTFS

Oprávnění nemůže přidělovat každý, k této činnosti je nutné oprávnění *Úplné řízení*, jehož majiteli jsou vlastníci složky (vlastníkem je ten, kdo složku vytvořil). Člen skupiny *Administrators* může získat plnou kontrolu nad složkou tak, že převezme její vlastnictví (vlastnictví je věnován zvláštní odstavec). Oprávnění NTFS přiřazujeme na záložce *Zabezpečení* okna vlastností složky (pravé tlačítko myši na složce *Vlastnosti*). Karta *Zabezpečení* má dvě části:

- V horním skupinovém rámečku *Název skupiny nebo jméno uživatele* vidíme skupiny a uživatele, jimž bylo přiděleno oprávnění ke složce. Tlačítkem *Přidat* skupiny a uživatele přidáváme, tlačítkem *Odebrat* jejich oprávnění rušíme.
- Spodní skupinový rámeček *Oprávnění* povoluje, nebo jednotlivá oprávnění odebírá. Vždy kurzorem vybereme skupinu (uživatele) v horním okně a pak ve spodním okně oprávnění měníme. Můžeme je *povolit*, nebo *odepřít*. Je-li okno šedě podbarvené, bylo oprávnění zděděno.

Při práci s oprávněními si musíme uvědomit, že odepřené oprávnění má nejvyšší prioritu. Odepřeme-li uživateli oprávnění, platí tento zákaz i v případě, že bude dotyčný uživatel členem skupiny, která má odepřené oprávnění povoleno.



Obrázek 4.51: *Zadávání oprávnění NTFS.*

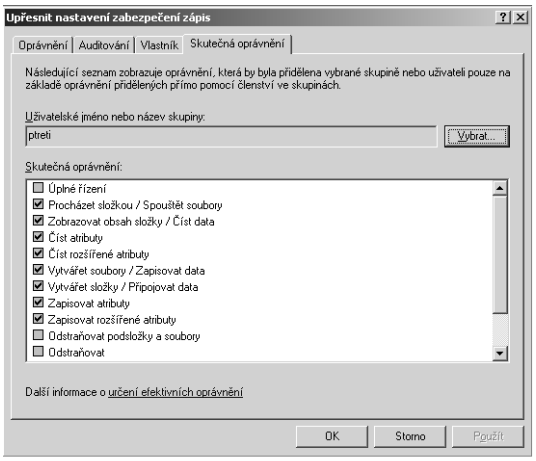
Vícenásobná oprávnění NTFS

Oprávnění můžeme přidělit uživatelům a skupinám. K jedné složce se tak uživateli může sejít více oprávnění – jeho přímá a ta ze skupin, jichž je členem. V takovémto případě se oprávnění vyhodnocují podle jednoduchého pravidla: Výsledné, skutečné (efektivní) oprávnění je sjednocením obou skupin oprávnění. Například: uživatel má ke složce oprávnění *Číst*, ale z jeho členství ve skupině vyplývá oprávnění *Zapisovat*. Výsledné oprávnění tedy je *Číst* a *Zapisovat*. Dále platí, že oprávnění k souboru má přednost před oprávněním ke složce.

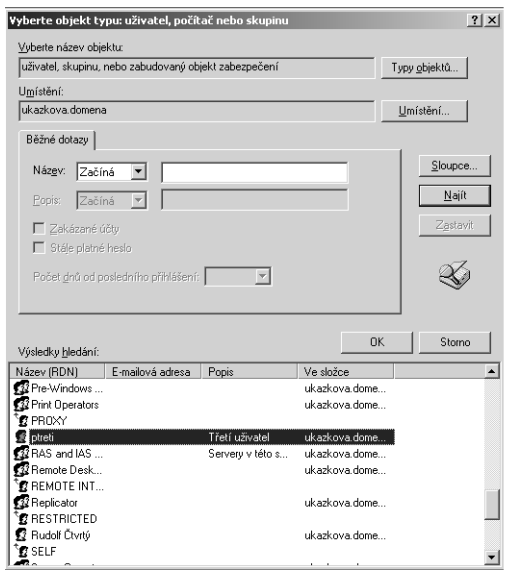
Aby bylo možné jednoduše zjistit *Skutečná oprávnění*, nabízí Windows Server 2003 (a také Windows XP Professional) možnost zjištění skutečných oprávnění. Na záložce *Zabezpečení* okna vlastností složky stiskneme tlačítko *Upřesnit,* a přejdeme na záložku *Skutečná oprávnění*. Zde musíme nejdříve vybrat skupinu nebo uživatele, jejichž oprávnění zjišťujeme. Pomůže nám v tom tlačítko *Vybrat,* po jehož stisku můžeme vyhledat uživatele v Active Directory. Budeme procházet několika obrazovkami a u menší jednoserverové sítě je postup následující:

1. Nejdříve se otevře obrazovka *Vyberte objekt typu*, kde stiskneme tlačítko *Upřesnit*.
2. Dostaneme se na další obrazovku, kde použijeme tlačítko *Najít*.
3. Zobrazí se seznam uživatelů a skupin v Active Directory, jednoho z nich zde vybereme.

Tím jej umístíme do řádku *Uživatelské jméno nebo název skupiny* a ve spodním skupinovém rámečku *Skutečná oprávnění* spatříme skutečná oprávnění.



Obrázek 4.52: *Skutečná oprávnění*

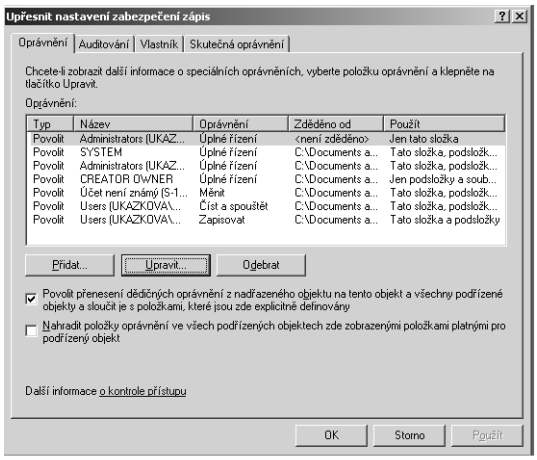


Obrázek 4.53: *Výběr uživatele, jehož skutečná oprávnění zjišťujeme*

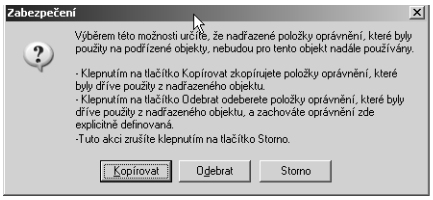
Dědění oprávnění

Ve výchozím stavu se oprávnění přidělená složce dědí také na její podsložky a soubory. Je to užitečná vlastnost, protože šetří správci práci s definicí oprávnění (podsložka přebírá oprávnění nadřazené složky), přesto je dědění nutné občas potlačit. Dědění je věnována záložka *Oprávnění* obrazovky *Upřesnit nastavení zabezpečení* (otevřeme ji stiskem tlačítka *Upřesnit* na záložce *Zabezpečení*): Zde složce dědění přímo zakážeme – zaškrtávacím políčkem *Povolit šíření dědičných oprávnění…* karty *Zabezpečení*. Po vymazání zatržítka se nás systém zeptá, zda chceme zděděná oprávnění:

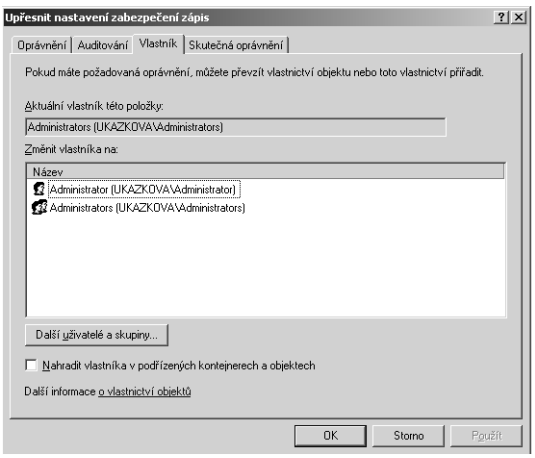
- *Kopírovat* – do podřízené složky se před odebráním dědění děděná oprávnění zkopírují.
- *Odebrat* – oprávnění se zrušením dědění podřízené složce odeberou.



Obrázek 4.54: *Odebrání dědění oprávnění 1*



Obrázek 4.55: *Odebrání dědění oprávnění 2*



Obrázek 4.56: *Převzetí vlastnictví*

Změna vlastnictví složky (souboru)

Již několikrát jsme se setkali s pojmem *vlastník*. Je to uživatel, který vytvořil složku (soubor) a je tak jejím vlastníkem. Z hlediska oprávnění má úplnou kontrolu nad složkou (oprávnění *Úplné řízení*). Členové skupiny *Administrators* však mohou vlastnictví složky převzít a získat nad ní úplnou kontrolu. Je to potřeba například po havárii složky, odstranění uživatelského účtu a ztrátě kontroly nad složkou atd.

K této činnosti se dostaneme opět z karty *Zabezpečení* stiskem tlačítka *Upřesnit* a v okně *Upřesnit nastavení zabezpečení* vybereme kartu *Vlastník*. V poli *Vlastník* vidíme členy administrátorské skupiny, kteří mohou vlastnictví převzít. Některého z potenciálních majitelů vybereme a vlastnictví převezmeme tlačítkem *Použít*.

Automatická oprávnění

Již víme, že systém automaticky některým složkám přiděluje sdílení a oprávnění. Konkrétní hodnoty jsou shrnuty v tabulce.

Tabulka 4.8: Automatická oprávnění

název sdílené složky	oprávnění	poznámka
C$, D$, E$...	Úplné řízení pro skupinu Administrators	Pomocí dědění získává Administrator přístup ke složkám na disku
Admin$	Úplné řízení pro skupinu Administrators	Administrátor získává přístup ke složce se systémovými soubory
Print$	Úplné řízení pro skupinu Administrators, Server Operators a Print Operators. Oprávnění Číst pro skupinu Everyone	Prostřednictvím tohoto sdílení je zajištěna automatická instalace ovladačů tiskáren

Mapování

Ze síťových stanic můžeme ke sdíleným složkám serveru přistupovat prostřednictvím mapování, které bylo popsáno v kapitole Sítě peer to peer (Přístup ke sdíleným složkám/Mapování).

Tisky ve Windows Serveru

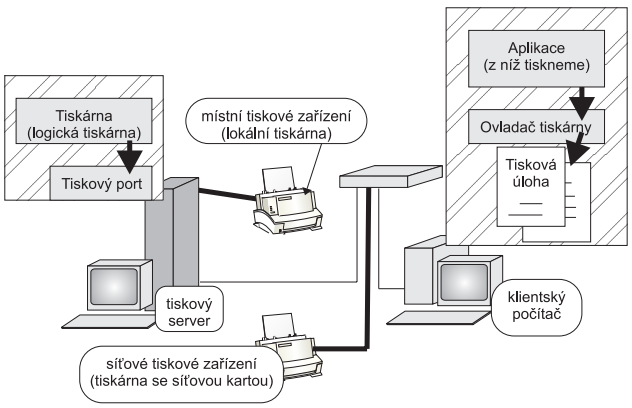
Zprostředkování tisku ze síťových stanic na společnou tiskárnu je jednou ze základních vlastností sítí. Tuto službu nabízí také Windows Server 2003. Dnes je používán častěji hardwarový server instalovaný v tiskárnách (vysvětlili jsme si to v kapitole o sítích peer to peer), přesto se o tiskové službě (roli) serveru zmíníme. V úvodu si musíme vysvětlit terminologii použitou při konfiguraci síťových tisků.

Terminologie a princip

Na začátku kapitoly se seznámíme s terminologií, která je použita ve Windows Serverech v souvislosti s tisky.

Tiskové zařízení: je hardwarové zařízení, které tiskne, můžeme mít:

- *Místní tiskové zařízení*, fyzickou tiskárnu připojenou k počítači (ten se pak označuje jako tiskový server). Připojení bývá nejčastěji přes paralelní port.
- *Síťová tisková zařízení*, jsou fyzické tiskárny připojené přímo do sítě (mají svoji vlastní síťovou kartu a síťovou adresu).



Obrázek 4.57: *Tiskové prostředí Windows 2003*

Tiskový server: je počítač, který tisky řídí. Zpracovává tiskové dokumenty odeslané klientskými počítači. Síťová tisková zařízení musíme konfigurovat na tiskových serverech. Tiskový server může být spuštěn na počítačích s operačním systémem Windows Server a Windows XP Professional (u verze Professional je současný počet tiskových připojení omezen na 10).

Ovladač tiskárny: je program, který převádí tiskové příkazy do jazyka tiskárny. Ovladač je závislý na typu tiskárny. Používáme jej vždy, i u nesíťových tisků (když k PC připojujeme tiskárnu, musíme ji nainstalovat – rozšířit operační systém o její ovladač).

Princip činnosti tisků je patrný z obrázku. Úloha napsaná na klientském PC, v nějakém aplikačním programu (např. Wordu) je zpracována ovladačem tiskárny. Forma tiskových příkazů, přizpůsobená konkrétnímu typu tiskárny je převedena do tiskové úlohy. Tisková úloha je odeslána do počítače – tiskového serveru. Zde je přijata programem Tiskárna. Ten ji pak pošle na konkrétní tiskové zařízení, buď připojené přímo k tiskovému serveru, nebo k síťové kabeláži.

Možné připojení tiskových zařízení

Tiskové služby Windows Server dovolují několik variant připojení společných tiskáren. Při konfiguraci tisků si musíme rozmyslet, která z variant bude pro naše podmínky ta pravá.

Vzdálené místní tiskové zařízení

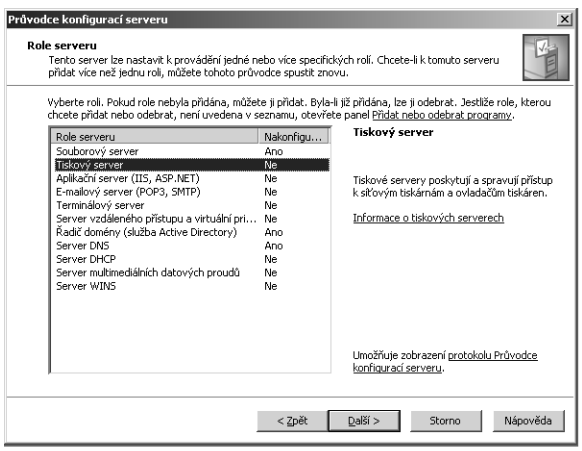
Řešení klient/server nabízí výhodu v tom, že všechny tiskové úlohy, mířící na tiskový server jsou řazeny do centrální tiskové fronty. Je možná centrální správa tisků (přidělování oprávnění pro práci s tiskárnou). K tiskovému serveru je možné připojit i více tiskových zařízení (záleží na počtu USB či paralelních portů, kterými je server vybaven). Nevýhoda je jen jedna, ale podstatná: společná tisková zařízení musejí být umístěna u serveru, což často nebývá možné.

Vzdálené síťové tiskové zařízení

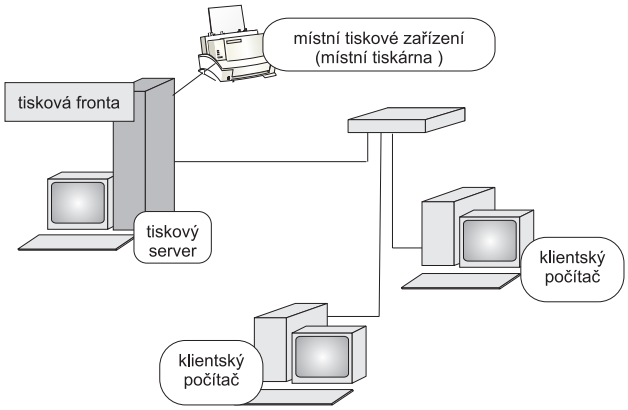
Takovéto řešení má také všechny výhody tiskového serveru (společná tisková fronta, oprávnění). Tiskové zařízení je však možné připojit kamkoliv do sítě, musí však být vybaveno vlastní síťovou kartou, ale funkci tiskového serveru plní Windows Server. Tiskový server může spravovat jedno, nebo více tiskových zařízení (na obrázku vidíme dvě společná tisková zařízení).

Konfigurace tiskových služeb – přidání role Tiskový server

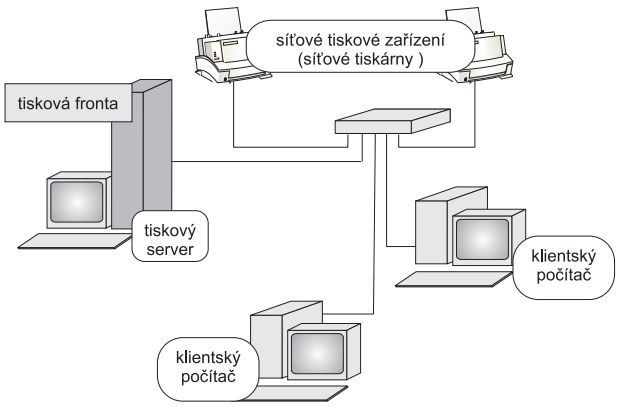
Nyní již víme, jaké varianty tisků můžeme v síti Windows Server použít. K jejich zprovoznění je potřeba dvou zásadních kroků. Nejdříve musíme tisková zařízení připojit k tiskovému serveru (jak hardwarově, tak softwarově) a pak se ke společnému tiskovému zařízení připojit z klientské stanice.



Obrázek 4.60: *Volba role Tiskového serveru*



Obrázek 4.58: *Společná tiskárna připojená k tiskovému serveru*

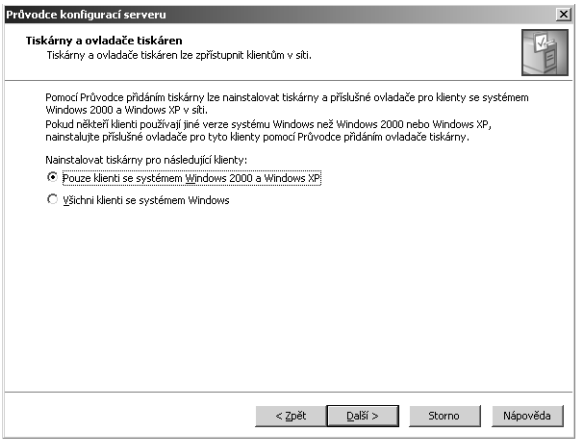


Obrázek 4.59: *Společná tiskárna připojená ke kabeláži sítě*

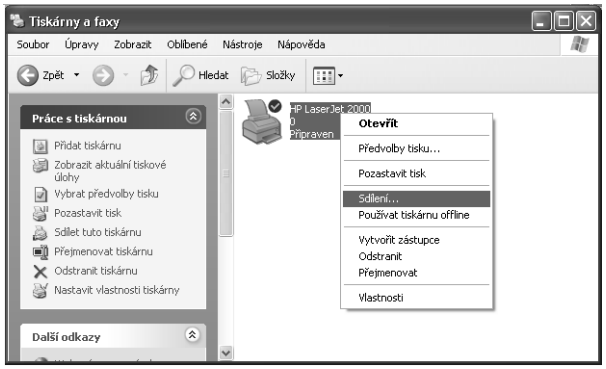
Již jsme se setkali s programem *Správa Serveru,* jehož prostřednictvím můžeme přidávat role (služby) Windows Serveru 2003. Roli tiskového serveru přidáme právě jeho prostřednictvím. Program se spouští po startu operačního systému, nebo přes tlačítko *Start.* V jeho horní části klepneme na zelenou šipku *Přidat nebo odebrat roli,* a v *Průvodci konfigurace serveru* (jenž jsme takto spustili) zvolíme *Tiskový server.*

V další obrazovce *Průvodce* sdělíme jaké operační systémy v naší síti používáme. Následně bude spuštěn *Průvodce přidáním tiskárny.* Toho jsme si již ukázali v kapitole o sítích peer to peer, a tak se jeho popisem zabývat nebudeme, jenom upozorním na důležitost jeho druhé

obrazovky, kde rozhodujeme o tom, zda tiskárna bude připojena k počítači místně, nebo vzdáleně. Po přidání ovladače tiskárny je tiskový server nakonfigurován.



Obrázek 4.61: *Volba role Tiskového serveru*



Obrázek 4.62: *Rozhodnutí o tom, zda budeme připojovat místní, nebo vzdálenou tiskárnu*

Budeme-li k tiskovému serveru připojovat vzdálené tiskové zařízení (tiskárnu s vlastní síťovou kartou), bude nutné vytvořit si její místní port. Postup byl opět již popsán v kapitole o sítích peer to peer (přesně *Ovladače tiskáren připojených k print serveru).*

Ovladač další tiskárny obsluhované print serverem můžeme přidat prostřednictvím *Správy Serveru*

Obrázek 4.63: *Role serveru*

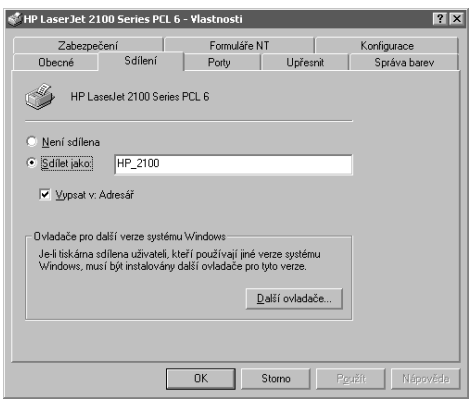
Sdílení a zabezpečení tiskového zařízení

Tiskárna připojená k tiskovému serveru je objektem Active Directory, který můžeme sdílet (to jsme udělali během konfigurace role Print server) a samozřejmě jí můžeme přidávat oprávnění a ovlivňovat tak kdo bude moci tiskárnu používat. Tato základní nastavení provádíme podobně jako u oprávnění složek. Otevřeme ovládací panel *Tiskárny a faxy* (*Start/Tiskárny a faxy*), klepneme pravým tlačítkem myši na ikoně tiskárny a vybereme poslední řádek *Vlastnosti.* Na obrazovce vlastností tiskárny nás zajímají dvě karty *Sdílení* a *Zabezpečení.*

Karta sdílení

Zde bude zatrženo políčko *Sdílet jako.* Do stejnojmenné řádky můžeme vepsat název tiskového zařízení. (Tím se bude identifikovat klientům v síti a zároveň bude pod tímto názvem uložena v Active Directory).

Políčko *Zobrazit v adresáři* necháme zatržené. Tím umožníme zveřejnění (publikování) tiskárny v Active Directory.



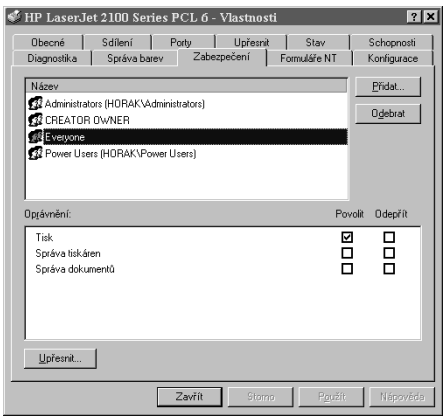
Obrázek 4.64: *Sdílení tiskárny*

Karta zabezpečení

Význam této obrazovky je stejný jako při sdílení složek. Přidělujeme zde oprávnění k práci s tiskárnou (viz tabulka). Ve výchozím tvaru má systémová skupina *Everyone* přiděleno oprávnění *Tisk*.

V horním okně prostřednictvím tlačítka *Přidat* přidáváme skupiny, či uživatele, jejichž oprávnění chceme měnit. Tlačítkem *Odebrat* můžeme tisková oprávnění rušit.

Tip: Stejně jako u oprávnění NTFS má odepřené oprávnění přednost před přiděleným oprávněním. Pokud zaškrtneme políčko Odepřít u oprávnění Tisk skupině Everyone, nebude moci nikdo na tiskárnu tisknout. (Do skupiny Everyone patří všichni momentálně přihlášení a políčko odepřít má vždy přednost!)



Obrázek 4.65: *Oprávnění k práci s tiskárnou*

Tabulka 4.9: Oprávnění pro tisky

Akce	Tisk	Správa dokumentů	Správa tiskáren
Tisk dokumentů	X	X	X
Pozastavení, obnovení, restartování a zrušení tisku vlastního dokumentu uživatele	X	X	X
Připojení k tiskárně	X	X	X
Řídicí nastavení úlohy pro všechny dokumenty		X	X
Pozastavení, restartování a odstranění všech dokumentů		X	X
Sdílení tiskárny			X
Změna vlastností tiskárny			X
Odstranění tiskárny			X
Úprava tiskových oprávnění			X

Připojování síťových tiskáren (přesněji tiskových zařízení)

Instalací tiskového zařízení na tiskový server a jeho nasdílením je vše připraveno k síťovým tiskům. Posledním krokem je připojení klientské stanice ke sdílenému tiskovému zařízení (tj. fyzické tiskárně).

V podstatě jde o instalaci síťové tiskárny, kterou provádíme úplně normálním způsobem – pomocí *Průvodce přidáním tiskárny*. Postup je popsán v kapitole o sítích peer to peer.

Ochrana dat

Data jsou největším pokladem naší sítě. Přestože je soustřeďujeme na server a pomocí oprávnění chráníme před zneužitím, je navíc nutné jejich zabezpečení před havárií serveru. Ochrana se skládá ze dvou metod:

- Automatické ochrany s pomocí diskových polí
- Ručního zálohování dat

Disková pole

V kapitole *Server* jsou popsána disková pole RAID. Windows Server 2003 nabízí dva způsoby ochrany dat - RAID 1 a RAID 5.

- **RAID 1:** (Zrcadlení) kopíruje v reálném čase data jednoho disku na druhý
- **RAID 5:** část diskového prostoru (tvořícího svazek RAID) je vyčleněna pro paritní informace. Pokud některý disk havaruje, jsou jeho data obnovena z paritních záznamů zbývajících disků.

Porovnání metod RAID dostupných ve Windows Server ukazuje tabulka.

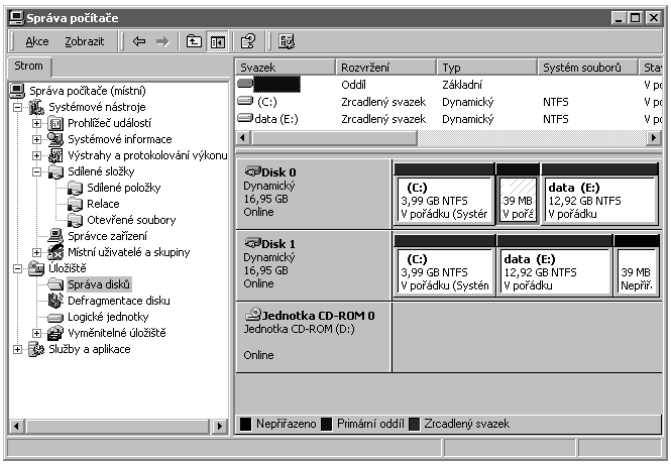
Tabulka 4.10: Porovnání technologií RAID

RAID 1 (zrcadlení)	RAID 5 (paritní informace)
Dovoluje zrcadlit spouštěcí oblast (z ní systém startuje) a systémovou oblast (jsou v ní uloženy soubory operačního systému)	Neumí prokládat systémové ani spouštěcí svazky.
Jsou potřeba minimálně 2 disky	Jsou potřeba minimálně 3 disky (maximum je 32)
50 % využití diskového prostoru	Využití diskového prostoru je závislé na počtu disků ve svazku. U 3 dvougigových disků (celková kapacita svazku 6 GB) se pro data využije 64 % diskového prostoru. U 5 dvougigových disků (s celkovou kapacitou 10 GB) bude pro data použitelných 80 % prostoru svazku.
Vyšší cena za megabajt uložených dat	Nižší cena za megabajt uložených dat
Menší nároky na systémovou paměť	Vyšší nároky na systémovou paměť

Zapnutí zrcadlení je poměrně složitý proces a nebudeme se jím podrobně zabývat. Informace o použitém stupni RAID získáme v konzole Správa disků (*Start/Nástroje pro správu/Správa počítače*).

Na obrázku vidíme, že v počítači jsou nainstalovány 3 disky. Jeden z nich je CD-ROM a dva pevné jsou zrcadleny. Na obou pevných discích jsou shodné dynamické svazky. Že jde o zrcadlení je také patrné ze sloupečku Rozvržení.

Poznámka: Hardwarové řadiče polí RAID jsou standardním vybavením serverů. Pokud jimi je náš server vybaven, je výhodnější vytvořit pole RAID tímto způsobem.



Obrázek 4.66: *Instalované disky*

Zálohování (archivace) dat

Během zálohování dat uložíme data na jiné místo a po případné havárii je odtud obnovíme. Příčin vedoucích ke ztrátě dat může být více: havárie disků serveru, viry, výpadky energie, živelná pohroma atd.

K zálohování je určen program Zálohování (*Start/Všechny Programy/Příslušenství/Systémové nástroje*). Než přistoupím k jeho popisu, musíme si vysvětlit základní postupy a obecná pravidla zálohování.

Plánování zálohování

Co zálohovat – Kapacita zálohovacích médií není nevyčerpatelná, a tak si musíme rozmyslet, která data zálohovat. Vždy zálohujeme data jednotlivých aplikací (účetnictví, záznamy o prodeji, zákaznících atd.). Dále je důležité zálohovat soubory registrů a úložiště služby Active Directory. Naopak je celkem zbytečné zálohovat programy, které můžeme nainstalovat z instalačních médií (např. adresář Program Files).

Určení frekvence zálohování – Data zálohujeme podle toho, jak často se mění. U dat měněných každý den bude nutná záloha denní, naopak denní záloha dat měněných týdně bude zbytečně zabírat místo na zálohovacím médiu.

Výběr média pro uložení zálohy – Zálohovat můžeme na pásku, nebo jiné vyjímatelné médium (např. Iomega Zip), nebo na pevný disk. (Zálohování jinam než na pásku se v programu Zálohování označuje jako zálohování do souboru.)

Obecně je bezpečnější zálohovat na vyjímatelné médium, které pak ukládáme odděleně od počítačů. Je tak možné předejít ztrátě dat způsobené zničením počítačů (krádež, živelná pohroma). Při zálohování na pevné disky jiných PC chráníme data pouze před poruchami počítačů (ale i to je lepší nežli žádná záloha, nehledě na to, že nejvíce problémů vzniká právě poruchami PC).

Místní nebo síťové zálohování – rozhodnutí o tom, zda budeme zálohovat data jen z jednoho počítače (typicky serveru), nebo i jiných strojů, záleží na způsobu práce s daty. Pokud jsou důležitá data ukládána pouze na server, bude stačit místní záloha serveru. Jsou-li důležitá data uložena také na stanicích, je dobré zálohovat i stanice. Pak se zálohování soustředí do jednoho bodu (např. na páskovou jednotku v serveru).

Typy zálohování

Zálohovací program Windows 2000 nabízí pět typů zálohování. Pro jejich činnost je důležitý atribut A (Archive), který je součástí popisu souboru i složky. Každý zápis do souboru znamená změnu jeho atributu A na 1. (Jestliže má atribut A hodnotu 1, je nutné soubor zálohovat). (O atributech se dočtete v kapitole Atributy.)

Normální (úplné) – zálohuje všechny soubory a složky. U zálohovaných souborů přepíše hodnotu atributu A z 1 na 0. Obnova dat je rychlá, záloha obsahuje všechny údaje nutné pro obnovu. Zálohování je však nejpomalejší a zabírá nejvíce místa na disku.

Kopie – pracuje stejně jako normální zálohování. Jediný rozdíl spočívá v tom, že u zálohovaných souborů a složek nemění atribut A.

Rozdílové – ze souborů a složek určených k zálohování zazálohuje pouze ty, jejichž atribut A má hodnotu 1. (Jde o soubory, které se od posledního zálohování změnily.) Zálohováním se atribut A nemění. Rychlost zálohování je střední. Pokud budeme chtít provést obnovu dat z rozdílové zálohy, musíme nejdříve použít poslední normální zálohu a až poté poslední rozdílovou zálohu.

Přírůstkové – stejně jako rozdílové zálohování zálohuje pouze soubory a složky s hodnotou atributu A = 1. Zálohováním se však hodnota atributu změní na 0. Zálohování je velmi rychlé (druhá přírůstková záloha v pořadí pracuje jen se změněnými soubory), ale obnova dat pomalá. Při obnově dat musíme nejdříve použít poslední normální zálohu a pak postupně všechny zálohy přírůstkové.

Denní – zálohuje všechny soubory a složky, které se během dne změnily. Tato záloha s atributy vůbec nepracuje.

Kombinace základních zálohovacích metod

Skutečné zálohování většinou používá kombinace základních způsobů, některé z nich popisují následující odstavce.

Normální a rozdílové – v pondělí provedeme normální zálohu a od úterka do pátku zálohujeme rozdílově. Rozdílové zálohování nemaže atribut A, takže každá záloha obsahuje všechny změny od pondělka. Dojde-li k poruše dat v pátek, stačí obnovit normální zálohu z pondělka a poslední rozdílovou ze čtvrtka. Tato metoda potřebuje více místa na zálohovacím médiu, více času při zálohování, ale méně času pro obnovu dat.

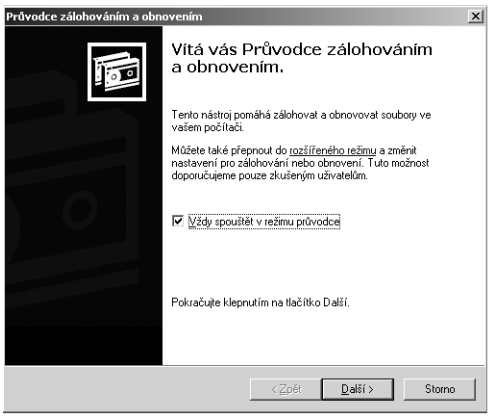
Normální a přírůstkové – v pondělí provedeme normální zálohu a od úterka do pátku zálohujeme přírůstkově. Přírůstkové zálohování mění hodnotu atributu A, a tak se zálohují pouze ty soubory, které se od poslední zálohy změnily. Dojde-li k poruše dat v pátek, musíme nejdříve obnovit první normální zálohu z pondělka a pak postupně všechny přírůstkové zálohy od úterka do čtvrtku. Tato strategie je nejrychlejší při zálohování, potřebuje také méně místa na zálohovacím médiu než předešlá metoda. Při obnově dat je však pomalejší a pokud se některá z přírůstkových záloh zničí, není obnova dat možná!

Tip: V kapitole Obecné zásady archivace (kapitola Síť Novell NetWare) je uveden zajímavý koloběh pásek při zálohování. Obecným zásadám zálohování je i zde věnováno několik odstavců, které doporučuji přečíst také správcům sítí Windows Server.

Zálohování dat

Aby bylo zálohování účinné, je nutné provádět je pravidelně. Program *Zálohování* umožňuje plánování a automatické spouštění zálohovacích úloh. My si ukážeme, jak s pomocí *Průvodce zálohováním* takovou úlohu definovat. Musíme stanovit co se bude zálohovat, kam se bude záloha ukládat, kdy se bude spouštět a pak zálohovací úlohu uložit.

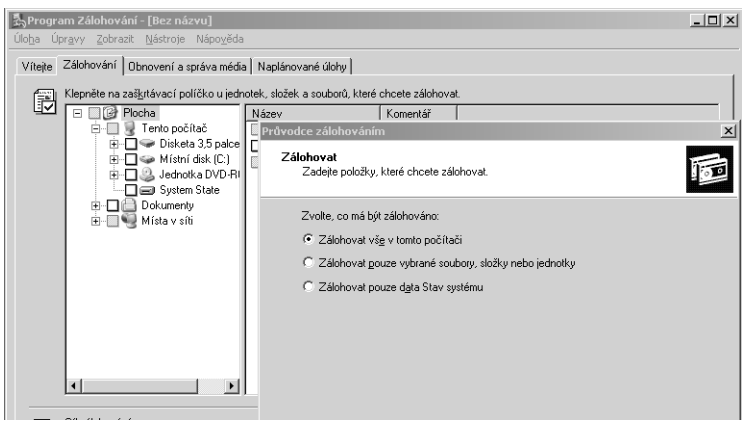
Program spustíme stiskem *Start/Všechny Programy/Příslušenství/Systémové nástroje*. Přivítá nás úvodní obrazovka *Průvodce zálohováním a obnovením*. *Průvodce* se snaží zálohování ulehčit, ale my přejdeme do rozšířeného režimu *Průvodce*. Použijeme HTML odkaz na obrazovce.



Obrázek 4.67: *Obrazovka Průvodce zálohováním*

Na následující obrazovce stiskneme tlačítko *Průvodce zálohováním (rozšířený režim)*. Vrátíme se tak zpět do *Průvodce zálohováním*, ale tentokrát budeme pracovat v rozšířeném režimu. *Průvodce* nás tradičně přivítá a hned ve druhé obrazovce se zeptá na rozsah naší zálohy. Většinou použijeme druhou možnost: *Zálohovat pouze vybrané soubory, složky nebo jednotky*. (Zálohovat vše je většinou zbytečné a drahé – potřebujeme více prostoru na záložním médiu).

Následující obrazovka slouží k výběru složek a souborů, které budeme zálohovat. Práce je velmi snadná, k dispozici je ikona *Tento počítač* a *Místa v síti*. Klepnutím na + vlevo od ikony si položku rozvineme, stejně rozbalujeme i obsah disků a složek. Složky a soubory určené k zálohování zatrhneme ve čtverečku vlevo od složky (souboru). Po výběru všech dat k zálohování stiskneme tlačítko *Další*.

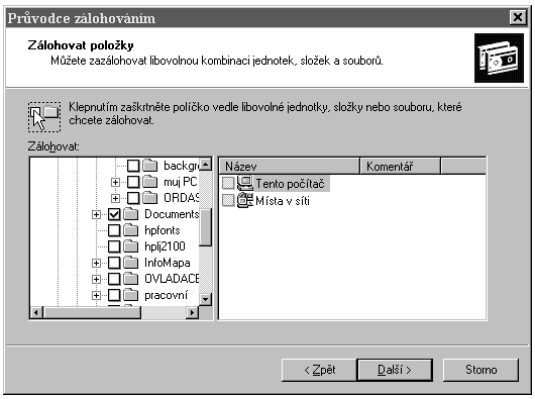


Obrázek 4.68: *Obrazovka Průvodce zálohováním*

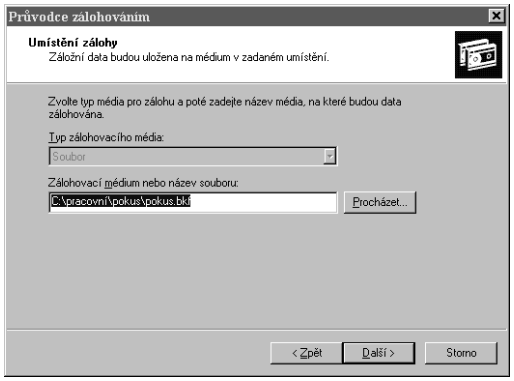
Postoupíme do obrazovky *Umístění zálohy*. Zde nejdříve zvolíme typ zálohovacího média:

- Soubor – umožní uložení dat na jakékoliv diskové médium, ve spodním řádku pak musíme zadat cestu a jméno souboru, do něhož se bude zálohovat

(přípona tohoto souboru musí být .bkf). Soubor může být uložen také na jiném počítači sítě. Pro usnadnění práce je k dispozici tlačítko *Procházet*.



Obrázek 4.69: *Výběr složek a souborů k zálohování*



Obrázek 4.70: *Umístění zálohy*

• Páska – je určena k ukládání dat na pásková média. V případě této volby musíme o řádek níž zapsat jméno pásky.

Tlačítkem *Další* přejdeme do závěrečné obrazovky první fáze zálohování. Vidíme zde všechny zvolené parametry. Tlačítkem *Upřesnit* přejdeme do druhého definičního stadia zálohování, složeného z několika obrazovek.

Nejdříve určíme typ zálohování (Normální, Přírůstkové…).

Následuje obrazovka *Způsob zálohování* s dvěma zaškrtávacími políčky:

- *Po dokončení zálohování ověřit data* zaškrtnutím bude vytvořená záloha přečtena a porovnána s originálem (tzv. verifikována). Tato činnost prodlouží zálohování, ale zkontroluje bezchybnost uložených dat. Verifikaci bychom měli alespoň občas provádět.
- *Zakázat stínovou kopii svazku*. Stínová kopie je jednou z nových funkcí Windows Serveru 2003. Umožňuje zálohování souborů i tehdy, když se do souboru zapisuje. Většinou nemáme důvod toto měnit.

Poté se objeví obrazovka *Možnosti média* s volbami:

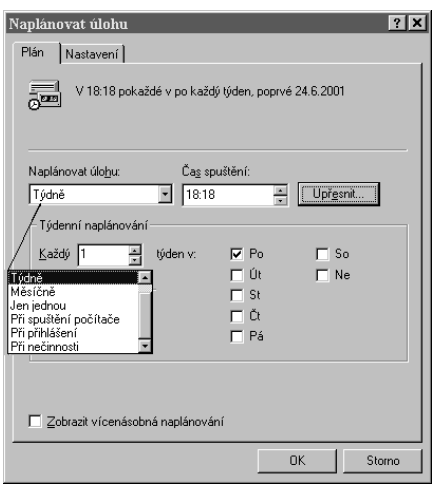
- *Přidat tuto zálohu k existujícím zálohám* – záloha bude zapsána za existující zálohu.
- *Nahradit existující zálohy* – starší záloha na médiu bude přepsána zálohou novou.

V příští obrazovce můžeme změnit název zálohy.

Další obrazovkou – *Čas zálohování,* začneme definici spouštěcího času zálohy. Máme na ní dvě volby:

- *Nyní* – jejím stiskem zahájíme zálohu okamžitě.
- *Později* – odsuneme start zálohy na pozdější dobu, a navíc budeme moci naplánovat pravidelné spouštění úlohy.

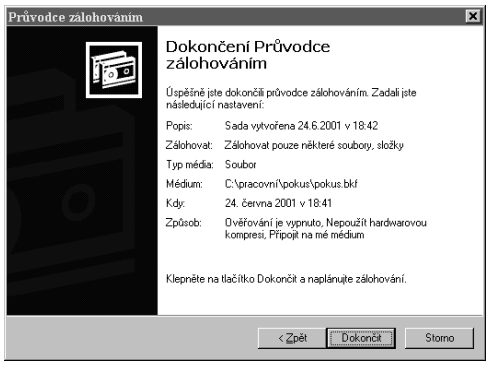
Po výběru *Později* musíme nejdříve přiřadit úlohu určitému uživatelskému účtu (zadat jméno účtu a jeho heslo). Poté úlohu pojmenujeme a stiskem tlačítka *Naplánovat* zahájíme plánování spouštěcího času úlohy. V políčku *Naplánovat úlohu* stanovíme interval opakování, který můžeme ještě upřesnit v dalších částech obrazovky. Tlačítkem *Upřesnit* zpřesníme provádění úkolu.



Obrázek 4.71: *Plánování času spouštění*

Tlačítkem *OK* se vrátíme do obrazovky *Čas zálohování*, tlačítkem *Další* opět uvidíme přehled naplánovaných úkolů. Tlačítkem *Dokončit* pak úlohu uložíme a zároveň přiřadíme do *Naplánovaných úloh*.

Poznámka: *Na záložce Naplánované úlohy programu Zálohování uvidíme vytvořené zálohovací úlohy (jsou součástí systémového modulu Naplánované úlohy – Start/Všechny Programy/Příslušenství/Systémové nástroje). Přejdeme-li do záložky Zálohování, můžeme v menu Úloha/Načíst výběr otevřít dříve vytvořené zálohovací úlohy.*

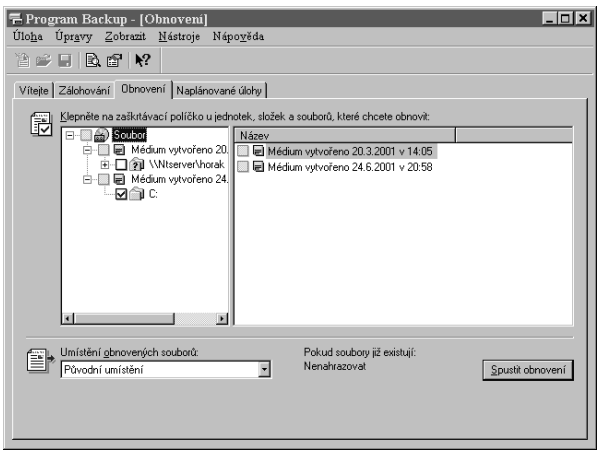


Obrázek 4.72: *Přehled o naplánované úloze*

Obnova dat

Úspěšná obnova dat je cílem veškerého zálohování. Proto bychom měli dodržovat následující pravidla:

- Provést pokusnou obnovu dat, abychom si celý zálohovací řetězec vyzkoušeli.
- Udržovat dokumentaci o zálohovacích úlohách. Každá zálohovací úloha vytvoří soubor BACKUPxx.LOG, v němž jsou uloženy základní údaje o zálohování. Soubor nejsnadněji najdeme přes *Start/Hledat*.



Obrázek 4.73: *Katalog záloh*

- *Původní umístění*, data se zapíší na původní místo (používá se při obnově poškozených dat).
- *Alternativní*, zapíše data do jiné složky disku (např. při cvičné obnově). Pro jednodušší nalezení složky je k dispozici tlačítko *Procházet*.
- *Jediná složka*, soubory ze stromové struktury (vnořené složky) obnoví do složky jediné. Neobnoví tedy hierarchickou strukturu souborů a složek.

Druhá obrazovka upřesňuje způsob obnovení:

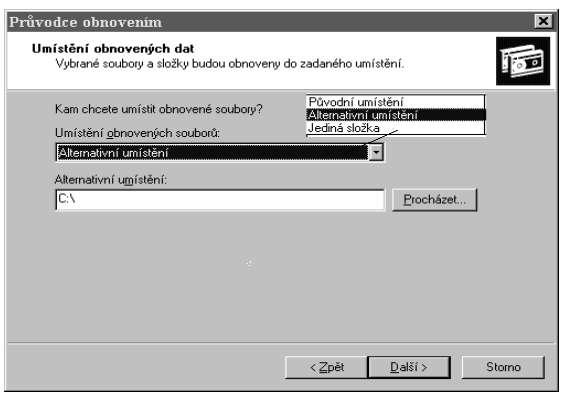
- *Nepřepisovat existující soubory* – pokud je ve složce, do níž data obnovujeme, soubor stejného jména jako obnovovaný, program jej nepřepisuje.
- Vést si přehled o vícenásobných zálohách. Vědět který den jsme zálohovali a jakým typem zálohy. (Při obnově na sebe jednotlivé zálohy navazují).

K obnově opět použijeme program *Zálohování*, nejsnáze pomocí *Průvodce obnovením*.

Ten nám na své první obrazovce ukáže katalog provedených záloh (v okně *Obnovit*), my si jednu z nich vybereme a klepneme na tlačítko *Další*.

Přejdeme do obrazovky, v níž uvidíme souhrnné údaje o obnovovaném souboru. Pokud bychom klepli na tlačítko *Dokončit*, budou soubory obnoveny a uloženy do původní složky.

Stiskem tlačítka *Upřesnit* můžeme obnovu dat přesněji definovat. V první obrazovce vybíráme místo, do něhož budou soubory obnoveny. Máme možnosti:



Obrázek 4.74: *Určení kam se budou obnovovat soubory*

- *Nahradit soubor na disku, pouze je-li starší než záložní kopie.* Je-li v adresáři, do něhož data obnovujeme, soubor stejného jména jako obnovovaný, program jej přepisuje pouze tehdy, pokud je v záloze novější verze souboru.
- *Vždy přepsat soubor na disku* – Je-li v adresáři, do něhož data obnovujeme, soubor stejného jména jako obnovovaný, program jej přepíše.

Zatrhneme-li v poslední obrazovce *Upřesnit možnosti obnovení* možnost *Obnovit zabezpečení*, budou při obnově dat obnovena i oprávnění a vlastnictví.

Pak následuje obrazovka s přehledem navolených parametrů obnovovacího procesu. Tlačítkem *Dokončit* provedeme obnovu dat.

Zálohování dat prostřednictvím ASR

„Klasické" zálohování bylo popsáno v předešlé kapitole. Systém ASR je dostupný od verze Windows Server 2003 (a ve Windows XP Professional), je novým prvkem, složeným ze dvou částí:

- *Zálohování* pomocí ASR. To se provádí pomocí *Průvodce automatickým obnovením systému*, který je součástí zálohovacího programu *Zálohování*. Průvodce zálohuje stav systému, systémové služby a veškeré disky, které jsou spojeny se součástmi operačního systému. Vytváří rovněž soubor obsahující informace o záloze, konfiguraci disku (včetně běžných a dynamických svazků) a o způsobech obnovení.
- *Obnovení* pomocí nástroje ASR. To přečte z dříve vytvořeného záložního souboru konfiguraci disku a obnoví veškeré podpisy, svazky a oddíly alespoň na discích, které jsou vyžadovány pro spuštění počítače. Pak nainstaluje Windows a automaticky zahájí obnovení systému s využitím zálohy (vytvořené *Průvodcem automatickým obnovením systému*).

Vytvoření zálohy ASR

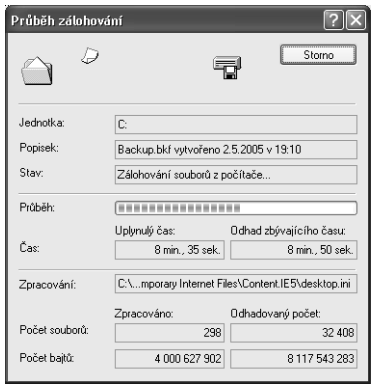
Vytvoření kompletní zálohy (všech dat) je relativně snadné, ale pro uložení zálohy je nutné mít:

- Zařízení s dostatečnou kapacitou (kam budeme záložní data ukládat). Záložní soubor se komprimuje, ale jeho zmenšení oproti originálu se podle typu zálohovaných dat pohybuje zhruba mezi 1/2 a 1/3 originálu.
- Záložní data musejí být navíc umístěna na médiu, které bude dostupné během instalace Windows XP. Není tedy možné použít ani síťové disky (na vzdálených PC), ani média CD a DVD (navíc je kapacita médií CD z hlediska ASR velmi malá). Pro zálohu ASR se jako vhodné zařízení ukazuje pásková jednotka, která je u mnoha serverů často k dispozici.
- Dále budeme potřebovat disketu, kam si ASR uloží údaje nutné ke spuštění procesu obnovy ASR.

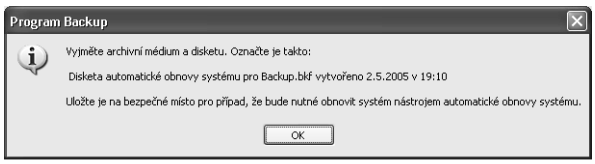
Nejdříve je tedy nutné rozvážit, zda je ASR tím správným řešením, zda neprovést pouze částečnou zálohu (která je kapacitně méně náročná). Pokud se pro použití ASR rozhodnete, vytvoříte základní zálohu ASR následujícím způsobem:

- Spustíte program *Zálohování*. Stačí otevřít ikonku *Tento počítač*, klepnout pravým tlačítkem myši na ikoně disku (který chceme zálohovat), přejít na kartu *Nástroje* a stisknout tlačítko *Zálohovat*. Druhou možností je „klasické" spuštění programu *Start / Všechny programy / Příslušenství / Systémové nástroje / Zálohování*.
- *Zálohování* se většinou spouští v *Režimu průvodce*, my však přejdeme do *rozšířeného režimu*. Provedeme to na první obrazovce průvodce (viz předešlá kapitola).
- Na kartě *Vítejte* stiskneme odkaz na *Průvodce automatickým obnovením systému*, čímž ASR nastartujeme a spustíme *Průvodce přípravou automatického obnovení systému*.
- Ve druhé obrazovce *Průvodce – Cíl zálohování* musíme vybrat místo, kam zálohu ASR uložíme. Samozřejmě to nesmí být na disk, který chceme zálohovat, nesmí to být ani na síťové disky, ani CD či DVD média. Zbývá tedy pásková jednotka nebo druhý pevný disk.

Obrázek 4.75: *Výběr místa pro uložení zálohy*



Obrázek 4.76: *Informace o průběhu zálohy*



Obrázek 4.77: *Vytvoření Diskety automatické obnovy*

- Tím v podstatě práci s vytvářením zálohy ASR ukončíme, na poslední obrazovce *Průvodce* shrne naši dosavadní činnost a upozorní nás na nutnost mít k dispozici disketu a zálohování se spustí.
- O postupu zálohování jsme průběžně informováni. Od velikosti zálohovaných dat se odvíjí doba trvání zálohy (počítejte od desítek minut až po hodiny). Odhadovaný čas, velikost záložního souboru a počet zálohovaných souborů najdeme v okně *Průběh zálohování*.
- Zálohu ASR zakončíme vytvořením spouštěcí *Diskety automatické obnovy*.

Obnovení ze zálohy ASR

Zálohu ASR používáme v případě havárie systému, kdy s její pomocí můžeme rychle vrátit systém do původního stavu. K úspěšné obnově potřebujeme:

- Instalační CD Windows Serveru 2003
- Disketu automatické obnovy, vytvořenou během ukládání zálohy ASR
- Vlastní zálohu ASR na dostupném médiu

Obnova ze zálohy spočívá v několika krocích, které na sebe navazují a musejí se provést ve správné posloupnosti. Pro ty, kdo již Windows Server někdy instalovali to nebude velký problém, úplní začátečníci by raději měli požádat o pomoc někoho zkušenějšího.

Příprava obnovy ASR

Prvním krokem při obnově ze zálohy ASR je instalace Windows Serveru 2003. Ta probíhá vždy z instalačního CD, odkud se spouští automaticky během startu počítače.

- Nejdříve se ujistíme, že máme v BIOSu povoleno bootování z CD mechaniky a do mechaniky vložíme instalační CD Windows Serveru 2003.
- Zapneme počítač a zahájíme běžnou instalaci Windows Serveru 2003 z instalačního CD.

Start ASR během instalace Windows Serveru 2003

Instalaci Windows Serveru pečlivě sledujeme, protože se na jejím začátku objeví dotaz na to, zda chceme spustit *automatické obnovení systému (ASR).* (Instalační program s námi komunikuje prostřednictvím spodního řádku obrazovky). Stiskem klávesy *F2* tak učiníme.

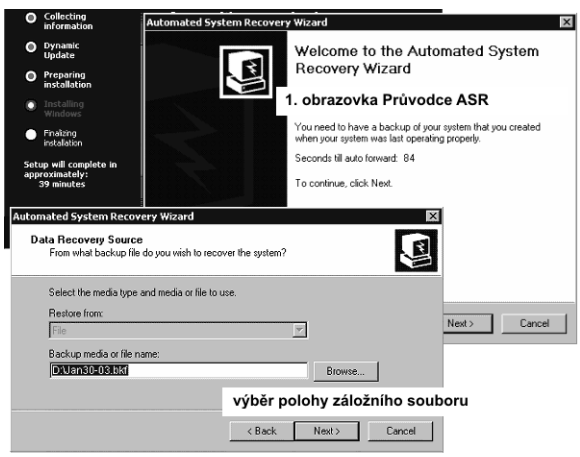
Poté si instalační program vyžádá *Disketu automatické obnovy* (vytvořenou zálohou ASR), kterou vložíme do disketové mechaniky.

> ***Poznámka**: Servery bývají vybaveny řadičem diskových polí RAID, pro nějž musíme během instalace nahrát správný ovladač. Na to jsme upozorněni při startu instalačního procesu (opět ve spodním řádku obrazovky), kdy jsme vyzváni ke stisku klávesy F6. Tato výzva předchází upozornění na ASR!*

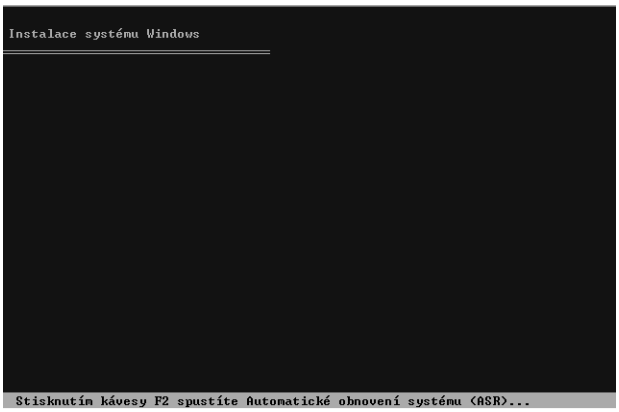
Spuštění průvodce ASR během instalace Windows Serveru 2003

Instalační program začne instalovat Windows Server:

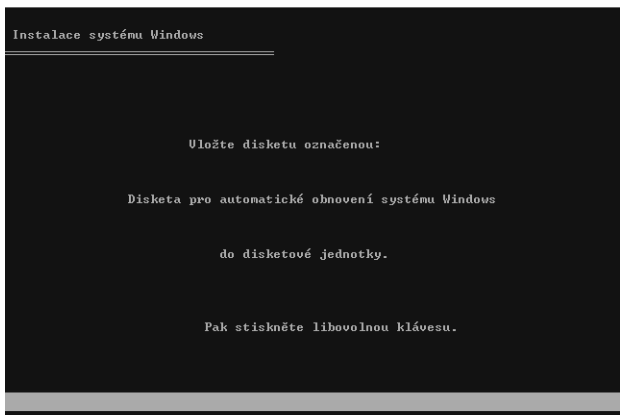
- Naformátuje disky, vytvoří zde oddíly (proto záloha ASR nemůže být uložena na zálohovaném pevném disku!)
- Pak se PC restartuje. Během nového startu již nesmíme během dotazu na start z CD (*Press any key to boot from CD*) stisknout klávesu. Instalace již pokračuje z pevného disku a stiskem klávesy bychom zahájili novou instalaci.



Obrázek 4.80: *Obnova Windows Serveru 2003 ze zálohy*



Obrázek 4.78: *Výzva instalačního programu ke spuštění ASR ve spodním řádku obrazovky*



Obrázek 4.79: *Výzva instalačního programu ke spuštění ASR*

- Po restartu se automaticky spustí *Průvodce ASR*. Instalace Windows Serveru 2003 se tak přeruší a bude probíhat obnova ze zálohy ASR.
- V druhé obrazovce si *Průvodce* vyžádá potvrzení polohy záložního souboru *.bkf, který jsme vytvořili zálohou ASR. Chceme-li použít jiný soubor, můžeme stisknout tlačítko *Procházet* a vyhledat jej. Zde se ukazuje nutnost uložit zálohu ASR na médium přístupné během instalace Windows XP. Již víme, že jím může být u serverů častá pásková jednotka.

Vzdálená plocha

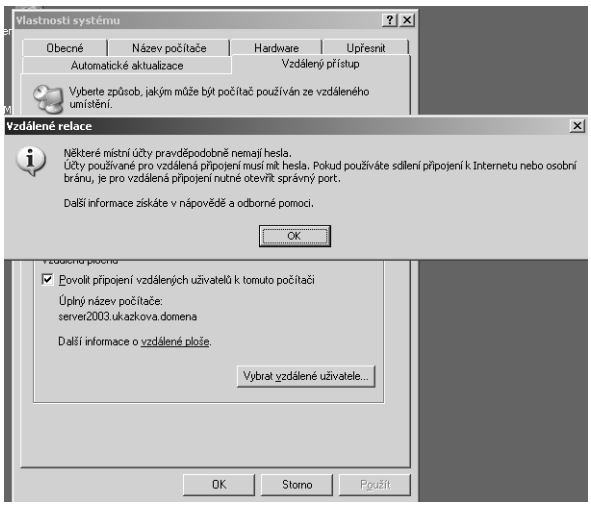
Windows Server 2003 nabízí „promítnutí“ své (serverové) vzdálené obrazovky na náš monitor (v podstatě jde o terminálový přístup k PC). Na dálku je tak možné spravovat server, který bývá často umístěn v oddělených místnostech. Na druhou stranu představuje *Vzdálený přístup* bezpečnostní riziko – ovládnout plochu Windows pod administrátorským účtem je určitě snem každého hackera. Vzdálený přístup je dostupný prostřednictvím funkce *Vzdálená plocha*. Úplně stejná funkce je k dispozici také ve Windows XP Professional a můžeme ji tedy použít v síti peer to peer.

Mezi vzdáleným počítačem a tím naším se vytváří relace vzdáleného připojení. Přístup ke *Vzdálené ploše* je možný jen po standardním přihlášení *k Windows Serveru*. Uživatel tedy musí zadat přístupové jméno a heslo některého z existujících účtů vzdáleného počítače (ale tento účet musí být zařazen do skupiny povolující vzdálené připojení – viz dále). Zabezpečení přístupu spočívá opět v přihlašovacích jménech a heslech – pro účty vzdáleného připojení určitě použijeme silná hesla.

Povolení Vzdálené plochy

Potenciálně je *Vzdálená plocha* nebezpečná a po instalaci Windows Serveru 2003 není povolena. Její zakázání je nejlepším bezpečnostním opatřením proti zneužití. Při občasném využití *Vzdálené plochy* ji povolíme pouze tehdy, když to bude potřeba.

Povolení provedeme na kartě *Vzdálený přístup* obrazovky *Vlastnosti Systému* (pravé tlačítko myši na ikoně *Tento počítač,* nebo *Start / Ovládací panely / Systém*). Zaškrtneme zde políčko *Povolit připojení vzdálených uživatelů…* Od této chvíle závisí ochrana před neoprávněným připojením pouze na přihlašovacím jménu a heslu. (Trochu odbočím od tématu: je-li síť chráněna firewallem, bude navíc potřebné otevření portu 3389). Pokud nemáme některé účty kryty heslem, budeme na to upozorněni (viz obrázek).

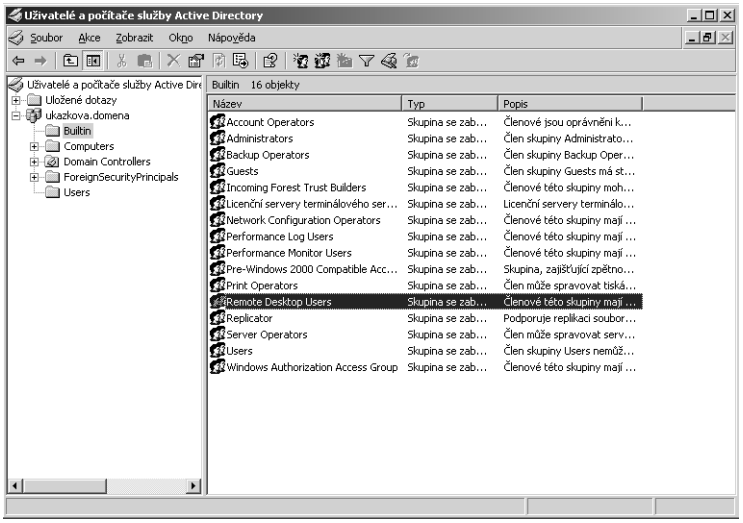


Obrázek 4.81: *Povolení vzdálené plochy*

Výběr uživatelů pro vzdálené připojení

Vzdálený přístup k serveru mají povolen všichni členové skupiny *Administrators*. Ale my již víme, že pro běžnou práci není vhodné pracovat jako administrátor. Měli bychom používat některý účet ze skupiny *Power Users* nebo *Users*. Vzdálené připojení (na rozdíl od administrátorů) však musíme těmto účtům povolit.

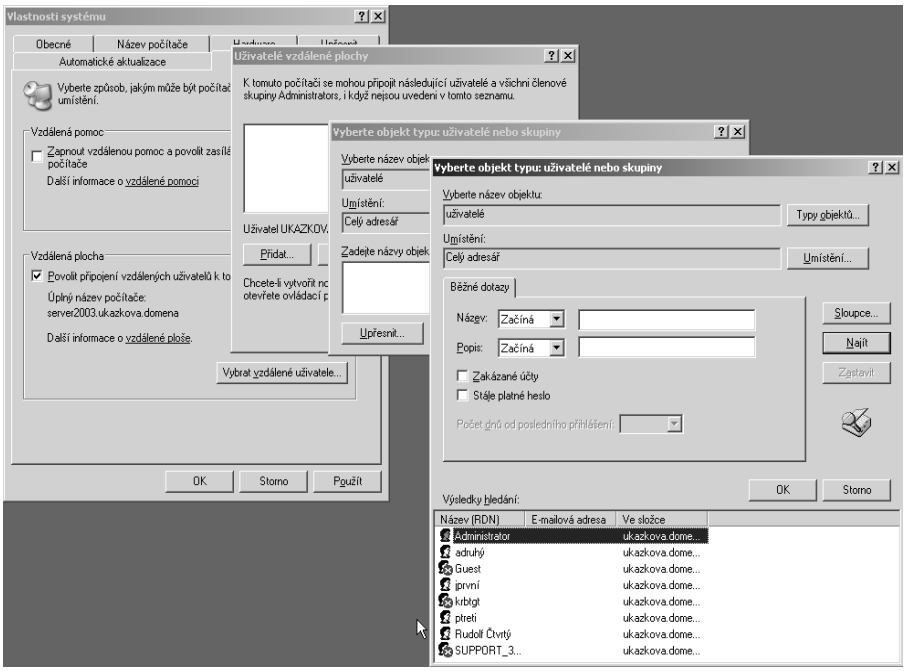
Windows Server 2003 má předdefinovánu skupinu *Remote Desktop Users*, jejíž členové mají povoleno použití vzdálené plochy. Přístup ke vzdálené ploše tedy povolíme přiřazením účtu do skupiny *Remote Desktop Users*. Můžeme to provést



Obrázek 4.82: *Skupina Remote Desktop Users*

v nám již známé obrazovce *Uživatelé a počítače služby Active Directory (Start / Nástroje pro správu)*. Zde budeme pracovat v kontejneru *Builtin*.

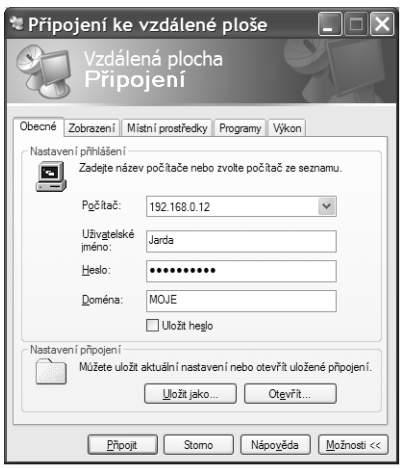
Druhou možností je samotný panel *Vzdálený přístup*, kde stiskem tlačítka *Vybrat vzdálené uživatele* otevřeme okno *Uživatelé vzdálené plochy*. V podstatě jde o pohled na členy skupiny *Remote Desktop Users*. Postup přidání nového účtu jsme již popisovali (postupný stisk tlačítek *Přidat*, *Upřesnit* a *Najít* …).



Obrázek 4.83: *Přidání vzdáleného uživatele*

Připojení ke vzdálené ploše

Je možné ze stanice Windows XP Professional, přes *Start / Všechny programy /Příslušenství / Komunikace / Připojení ke vzdálené ploše*. Příslušnou obrazovku ukazuje obrázek. Důležité je vyplnění řádku *Počítač*, kam zapisujeme IP adresu (nebo jméno) serveru, k němuž se připojujeme. Ostatní řádky vyplňovat nemusíme (budeme na ně během připojování dotázáni). Pokud se však k serveru připojujeme často, je výhodné si přihlašovací údaje předvyplnit.



Obrázek 4.84: *Připojení ke vzdálené ploše*

Poznámka: *Pro vzdálené připojování je nutné splnění několika podmínek, které ještě jednou shrnu:*

- *Přístup ke Vzdálené ploše je možný nejen z Windows XP, ale také z Windows 2000, ty však musejí mít nainstalovaného Klienta služby Terminal Services.*
- *Přistupovat může pouze účet ze skupiny Administrators nebo Remote Desktop Users.*
- *Vzdálený přístup probíhá ze sítě protokolem TCP/IP. Ke vzdálenému PC je možné připojení z libovolné sítě (např. Internetu), prostřednictvím portu 3389, který může být blokován firewallem.*

Přehled činností Windows Server 2003

Následující tabulka ukazuje stručný přehled jednotlivých postupů při správě serveru.

činnost	prostředek	postup
Komprese dat složky	Průzkumník, nebo přes ikonu Tento počítač/Disk/Složka	Klepnout pravým tlačítkem myši na složce, vybrat Vlastnosti, v záložce Obecné stisknout tlačítko Upřesnit. Zaškrtnout políčko „Komprimovat obsah…“
Komprese dat svazku	Průzkumník, nebo přes ikonu Tento Počítač/Disk	Klepnout pravým tlačítkem myši na svazku, vybrat Vlastnosti, v záložce Obecné zaškrtnout políčko „Komprimovat obsah…“
Vypnutí serveru	Start/Vypnout	Před vypnutím zkontrolovat, zda se serverem nikdo nepracuje! Konzola Sdílené složky (Start/Nástroje pro správu/Správa počítače.) Složky Otevřené soubory a relace by měly být prázdné. Před vypnutím je nutné zadat důvod vypnutí.
Diskové kvóty	Pravé tlačítko myši na disku / Vlastnosti / karta Přidělená kvóta (Nezapomenout přidat roli Souborový server)	Musí být zatrženo Povolit správu přidělování kvót, pak je možné ovlivňovat další vlastnosti.
Přidání modulu do konzoly MMC	Start/Spustit/MMC	Menu Konzola/Přidat nebo odebrat modul snap-in. Na obrazovce s přehledem již nainstalovaných modulů stisknout tlačítko Přidat, vybrat modul a zavřít okna Průvodce.
Uložení konzoly	Konzola MMC	Menu Konzola/Uložit. Vybrat režim ukládané konzoly. Soubor konzoly má příponu *.msc. Novou konzolu najdeme v Start/Nástroje pro správu.
Vytvoření uživatelského účtu	Modul Uživatelé a počítače služby Active Directory (Start/Nástroje pro správu)	Pravým tlačítkem myši klepneme na kontejner Users a v menu vybereme Nový/Uživatel. Vyplnit jednotlivé obrazovky Průvodce.
Vytvoření účtu počítače	Modul Uživatelé a počítače služby Active Directory (Start/Nástroje pro správu)	Pravým tlačítkem myši klepneme na kontejner Computers a v menu vybereme Nový/Počítač. Účet počítače se vytváří automaticky při konfiguraci Klienta sítě Microsoft pro připojení do domény.
Přiřazení uživatelského účtu do skupiny	Modul Uživatelé a počítače služby Active Directory (Start/Nástroje pro správu)	Klepnout pravým tlačítkem myši na uživatelský účet, vybrat Vlastnosti a kartu Je členem. Tlačítky Přidat, Odebrat měnit členství ve skupinách.
Přiřazení skupiny k jiné skupině (zanoření)	Modul Uživatelé a počítače služby Active Directory (Start/Nástroje pro správu)	Klepnout pravým tlačítkem myši na účet skupiny, vybrat Vlastnosti a kartu Je členem. Tlačítky Přidat, Odebrat měnit členství ve skupinách.
Přihlašovací parametry u počítače s Windows 98	Klient sítě Microsoft. Klepnout pravým tlačítkem myši na ikoně Okolní počítače, pak Vlastnosti, poklepat na řádku Klient sítě Microsoft	V horní části obrazovky zaškrtnout políčko „Přihlásit se do domény Windows NT“ a do řádku zapsat jméno domény.

Přihlašovací parametry u počítače s Windows 2000 Professional	Ikonka Tento počítač, pravým tlačítkem myši na ikonku „Tento počítač" a vybrat Vlastnosti.	Zde karta Identifikace v síti, tlačítko ID sítě, na jednotlivých obrazovkách volit „Tento počítač je součástí podnikové sítě a je používán ... „ pak „Společnost používá síť s doménou", zadat uživatelské jméno a heslo pro přihlášení k účtu v doméně. Pokud počítač ještě není členem domény, musíme vyplnit název počítače a jméno domény, do níž bude počítač přiřazen.
Definice sdílené složky	Průzkumník nebo Tento počítač. (Nezapomenout přidat roli Souborový server.)	Pravým tlačítkem na složku, Vlastnosti, na kartě Sdílení zatrhnout políčko Sdílet tuto složku. Tlačítkem Oprávnění zadat základní oprávnění pro přístupy ze sítě, na kartě Zabezpečení je případně zpřísnit a zpřesnit prostřednictvím oprávnění NTFS.
Definice oprávnění	Průzkumník nebo Tento počítač. (Nezapomenout přidat roli Souborový server.)	Pravým tlačítkem na složku, Vlastnosti, na kartě Zabezpečení přidáváme (odebíráme) do horního okna Název uživatele a skupiny, jimž budeme měnit oprávnění NTFS. Ve spodním okně Oprávnění povolujeme, zakazujeme nebo měníme oprávnění. Důležité je zaškrtávací políčko „Povolit šíření dědičných oprávnění...", jímž můžeme zakázat dědění oprávnění z nadřazených složek. Základní oprávnění pro přístupy ze sítě jsou definována na kartě Sdílení (tlačítko oprávnění).
Změna vlastnictví	Průzkumník nebo Tento počítač	Pravým tlačítkem na složku, Vlastnosti, na kartě Zabezpečení stisknout tlačítko Upřesnit a vybrat kartu Vlastník. Umístit kurzor na některého z možných vlastníků a převzít vlastnictví tlačítkem Nahradit vlastníka v....
Změna atributů	Průzkumník, nebo Tento počítač	Pravým tlačítkem na složku (soubor), Vlastnosti, na kartě Obecné jsou dole dvě okénka (Skrytý, Jen pro čtení) pro práci s atributy. Po stisku tlačítka Upřesnit můžeme měnit (přečíst) hodnotu archivačního atributu.
Mapování	Okolní počítače, Místa v síti	Pravým tlačítkem na složku, vybrat „Připojit síťovou jednotku". Mapování přiřadit logické jméno (v prvním řádku), podle potřeby zaškrtnout okénko „Znovu připojit při přihlášení".
Konfigurace tisků: Instalace místního tiskového zařízení	Ovládací panel Tiskárny (na PC – tiskovém serveru)	Klepnout na ikonu Přidat tiskárnu a nainstalovat ji standardním postupem.
Konfigurace tisků: Instalace síťového tiskového zařízení	Ovládací panel Tiskárny, případně software dodaný výrobcem tiskárny (na PC – tiskovém serveru). (Nezapomenout přidat roli Tiskový server.)	Spočívá ve vytvoření portu zastupujícího tiskové zařízení: – Software k jeho vytvoření je buď součástí instalace tiskárny a dodá jej výrobce tiskárny. – Nebo port vytvoříme pomocí tlačítka Přidat port na kartě Porty.

Konfigurace tisků: Nastavení sdílení tiskového zařízení	Ovládací panel Tiskárny (na PC – tiskovém serveru) (Nezapomenout přidat roli Tiskový server)	Klepnout pravým tlačítkem myši na tiskárně (sdíleném tiskovém zařízení), Vlastnosti a karta Sdílení. Zde zatrhnout políčko Sdílet jako. Na kartě zabezpečení můžeme definovat oprávnění uživatelů tisků.
Konfigurace tisků: Instalace síťové tiskárny z Windows 98	Ovládací panel Tiskárny (na PC – klientské stanici tiskového serveru)	Klepnout na ikonu Přidat tiskárnu a nainstalovat ji standardním postupem, v třetí obrazovce Průvodce vybrat možnost Síťová tiskárna. Budeme připojovat tiskárnu připojenou k tiskovému serveru (ten je fyzicky spuštěn na PC s Windows 2000 Server)
Konfigurace tisků: Instalace síťové tiskárny z Windows 2000	Ovládací panel Tiskárny (na PC – klientské stanici tiskového serveru)	Ikonka Přidat tiskárnu, na druhé obrazovce je několik možností jak tiskárnu najít: – přes Active Directory (Oblast hledání tiskárny...) – podobně jako u Windows 98, procházením mezi počítači v síti (Zadat název tiskárny nebo...)
Konfigurace tisků: Instalace síťové tiskárny z Windows XP	Ovládací panel Tiskárny (na PC – klientské stanici tiskového serveru)	Klepnout na řádek Přidat tiskárnu, ve druhé obrazovce musíme zaškrtnout řádek Síťová tiskárna nebo tiskárna připojená k jinému počítači. Ve třetí obrazovce ponechat zaškrtnutý řádek Vyhledat tiskárnu a dále postupovat podle pokynů průvodce.
Role serveru	Správa počítače (otevře se po startu, nebo Start/Nástroje pro správu)	V horní části – Správa rolí tohoto serveru, klepnout na zelené tlačítko Přidat roli.
Stav disků (např. stupeň RAID)	Konzola Správa počítače (Start/Nástroje pro správu)	Vybrat složku Správa disků. V horní pravé třetině vidíme ve sloupečcích: – Svazek: jména svazků – Rozvržení: stupeň použitého RAID – Typ: dynamický nebo základní typ svazku – Systém souborů: použitý souborový systém (u serverů NTFS)
Zálohování dat	Program Zálohování Start/Programy/Příslušenství/ Systémové nástroje/Zálohování	Na první obrazovce vybrat tlačítko Průvodce zálohováním. Na druhé obrazovce použít možnost „Zálohovat pouze vybrané soubory...". Na další obrazovce vybrat soubory k zálohování. Klepnutím na + vlevo od ikony (složky, počítače). Složky a soubory k zálohování zatrhneme ve čtverečku vlevo od složky (souboru). Na další obrazovce vybrat typ média, kam se bude soubor ukládat. Bude to soubor (všechny typy disků), nebo páska (pro pásková zařízení) Pak tlačítko Upřesnit a volit tyto parametry (postupně na obrazovkách): – Zvolit typ zálohování Normální, Přírůstkové... – Rozhodnout, zda budou zazálohovaná data kontrolována s originálem (verifikace). – Rozhodnout, zda se budou zálohy ukládat jedna za druhou (Přidat tuto zálohu na médium), nebo se bude starší záloha přepisovat novou (Nahradit data na médiu touto zálohou).

		– Stiskem tlačítka Později zadat čas, v němž se bude záloha pravidelně opakovat: přiřadit úloze účet a jeho heslo a pojmenovat ji, stiskem tlačítka Naplánovat stanovit interval opakování úlohy.
Obnova dat	Program Zálohování Start/Programy/Příslušenství/ Systémové nástroje/Zálohování	Na první obrazovce tlačítko Průvodce obnovením. Poté z katalogů záloh vybrat ten, v němž jsou obnovovaná data. Stiskem Dokončit se soubory obnoví a uloží do původní složky. Stiskem Upřesnit ovlivňujeme obnovu: – 1. obrazovka kam se budou data obnovovat: „Původní umístění" – na původní místo, „Alternativní": do námi definované složky, „Jediná složka" všechny soubory se obnoví do jediné složky (zničí se stromová struktura obnovovaných dat). – 2. obrazovka upřesňuje způsob obnovení s možnostmi: Nepřepisovat existující soubory. Nahradit soubor na disku, pouze je-li starší než záložní kopie. Vždy přepsat soubor na disku. Zatrhneme-li v poslední obrazovce možnost „Obnovit zabezpečení", budou při obnově dat obnovena i oprávnění a vlastnictví.

Kapitola 5

Síť Novell NetWare

Firma Novell má ve vývoji svého síťového operačního systému NetWare dlouholeté zkušenosti, jedná se tedy o rozsáhlý a důkladně propracovaný systém. Během života NetWare docházelo (a dochází) k jeho inovacím. Při výkladu budeme vycházet z momentálně standardních verzí 6 a 6.5.

Další důležitou skutečností je nutnost striktního rozlišení jednotlivých činností. Jde o to, že mnoho operací a příkazů je možné provádět pouze na obrazovce serveru, jiné pouze z pracovní stanice. Při výkladu tedy vždy upozorním na to, odkud (ze serveru, stanice) jsou úkoly proveditelné. Pohodlnější (a mnohem častější) je práce ze stanice. Pro připojení stanice k serveru slouží *Klient sítě NetWare*. Ten je dostupný ve dvojím provedení – od firmy Microsoft (je součástí operačních systémů Windows) a od firmy Novell (najdeme ho na instalačních CD NetWare, případně je volně dostupný na Internetu). Klient NetWare od Novellu nabízí daleko lepší podmínky pro administraci sítě. Proto ve svém výkladu budu používat pouze klienta od Novellu (a pro praxi jej doporučuji).

Síťový operační systém NetWare je typickým představitelem sítě klient server. Soustřeďuje veškeré údaje o síťových prvcích do centrální databáze eDirectory. K ochraně spravovaných dat uživatelů má důkladný systém definice přístupových práv k souborům a složkám.

NetWare je operační systém, který je možné použít jak v malých, tak rozsáhlých sítích. Má k dispozici mnoho nástrojů určených pro velké sítě (časové servery, kopie eDirectory, složitě členěné databáze eDirectory,…), mnoho prostředků zaměřených na Internet (DHCP servery, WWW servery, DNS servery…) či programy pro pokročilou správu sítě – např. ZEN Works. Jejich popis však v této knize nenajdete. Zaměříme se především na „klasické“ (a nejčastěji používané služby): práci s uživateli a jejich přístupovými právy k souborům složkám a objektům (službu souborový server) a na činnosti související se síťovými tisky.

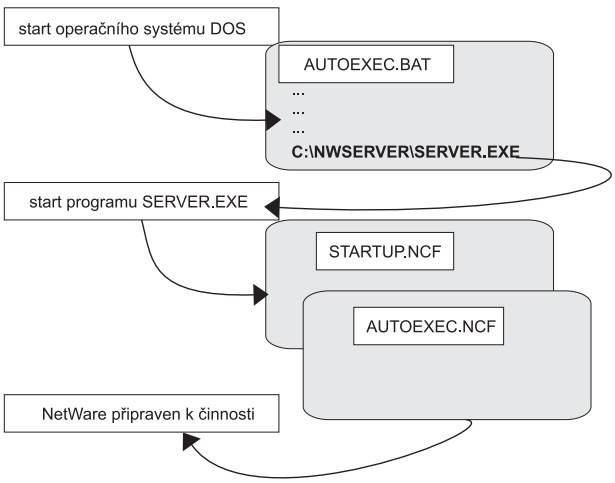
Základy systému NetWare

Síťový operační systém je vždy nahraný na serveru a spolupracují s ním ostatní síťové stanice. Pro další výklad je důležité pochopit posloupnost kroků při startu serveru a seznámit se se základními prvky operačního systému. Na rozdíl od serverů Microsoft Windows pracuje NetWare na dedikovaném serveru (jeho klávesnice o obrazovka jsou použitelné pouze pro konfiguraci serveru, nikoliv pro práci s aplikačními programy).

Start serveru

Startování serveru Novell NetWare probíhá v několika krocích. Nejdříve se do operační paměti zavede operační systém DOS (s novellskými servery je dodáván *Caldera DOS*). Důvodem tohoto kroku je spuštění programu *SERVER.EXE*, který je jádrem operačního systému NetWare. Automatický start je zajištěn vložením příkazu *SERVER* do souboru *AUTOEXEC.BAT*.

Tady si dovolím malou odbočku: DOS je starý operační systém, který už nemusí každý znát. Pro naše účely stačí jedna z jeho vlastností – po startu provádí



Obrázek 5.1: *Start serveru Novell NetWare*

příkazy, zapsané v textovém souboru *AUTOEXEC.BAT*. Jedním z takových příkazů je povel pro nastartování serveru NetWare.

Pokračujme ve startu serveru. Vlastní program *SERVER.EXE* bývá standardně umístěn do složky *C:\NWSERVER* operačního systému DOS. V této složce je také spousta jiných souborů potřebných při startu serveru, mezi nimi i textový soubor *STARTUP.NCF*. V něm *SERVER.EXE* hledá ovladače pro svůj hardware (např. pevné disky a jejich řadiče). *STARTUP.NCF* je tedy automaticky přečten a jeho prostřednictvím jsou do operační paměti serveru načteny hardwarové ovladače.

Dalším důležitým souborem je *AUTOEXEC.NCF*. Ten je již uložen na diskovém prostoru NetWare (z DOSu není přístupný). *SERVER.EXE* automaticky přečte také tento soubor a provede příkazy, které zde najde (jsou to ovladače síťových karet, nastavení časového prostředí, start programových modulů…). Rozběhnutím programu *SERVER.EXE* (z oblasti operačního systému DOS) nastartuje operační systém NetWare. Od tohoto okamžiku se oblast DOS nepoužívá, NetWare začne „vidět" data a programy uložené v netwarových oblastech disku.

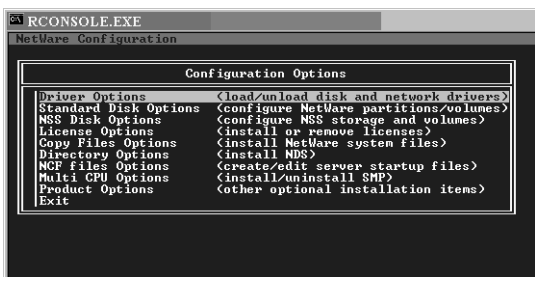
Poznámka: *Ještě jednou zdůrazním to, co vyplývá z předešlých řádků. Jeden z disků serveru NetWare musí mít dvě oblasti: oblast DOS (o velikosti zhruba 250 MB), která zajišťuje start systému (a po nastartování již potřeba není) a oblast NetWare (většinou obhospodařovanou systémem NSS), v níž server pracuje.*

Tip: Jestliže se start serveru nedaří, je možné načíst operační systém DOS z diskety a nastartovat server ručně (příkazem SERVER ve složce C:\NWSERVER). Příkaz SERVER je možné zadat s parametrem -NA, SERVER.EXE pak nebude načítat soubor AUTOEXEC.NCF (v některém z jeho řádků bude pravděpodobně příčina potíží.) Po nastartování systému pak můžeme provést úpravu v AUTOEXEC.NCF. (Přesná syntaxe příkazu je: **server -na**)

Programové moduly

Vlastní jádro systému (program *SERVER.EXE*) je možné rozšiřovat o programové moduly. Jsou to soubory s příponou *NLM*. Jejich spuštěním zavedeme novou službu (například modul *PSERVER.NLM* souvisí s tiskovým prostředím). Nastartování modulu provedeme napsáním jména modulu na obrazovce (konzoly) serveru. (U starších systémů NetWare 4.x bylo nutné před jméno modulu napsat příkaz *LOAD*.)

Jestliže chceme spouštět některé moduly automaticky, vložíme jejich spouštěcí příkaz do souboru *AUTOEXEC.NCF*. Uděláme to tak, že spustíme modul *NWCONFIG*, vybereme volbu „*NCF Files Options*" a v ní řádek „*Edit AUTOEXEC.NCF file*". Modul *NWCONFIG* slouží k základní hardwarové konfiguraci serveru. Této problematice se nebudeme věnovat, a tak s jednotlivými volbami programu nijak neexperimentujte, mohli byste znemožnit start serveru, v horším případě smazat všechna data! (U starších verzí NetWare 4.x se modul se stejnými funkcemi nazýval *INSTALL*).



Obrázek 5.2: *Obrazovka modulu NWCONFIG*

Moduly, příkazy, utility

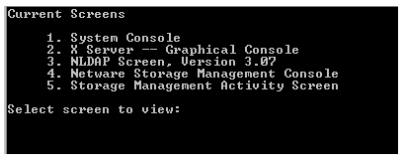
Programové moduly nejsou jedinými prostředky pro práci se serverem. Při správě serveru můžeme použít několik typů konfiguračních programů:

- **Loadable modules:** Moduly *NLM*, spouštějí se příkazem zapsaným z klávesnice serveru na obrazovku serveru. Jejich volbami procházíme opět klávesnicí serveru. Patří sem například moduly *PSERVER*.NLM, *MONITOR*.NLM.
- **Console commands:** Příkazy konzoly jsou příkazy, jimiž ovlivňujeme práci serveru. Opět se zadávají klávesnicí serveru a jejich výstup je zobrazován na konzole serveru. Jde např. o příkazy *CONFIG*, *DISABLE LOGIN*.

- **Command line Utilities**: jsou řádkové příkazy zapisované z pracovní stanice. S těmi se v knize nesetkáme, protože jsem se snažil je vůbec neuvádět. Stejných výsledků totiž dosáhneme grafickými utilitami, které jsou uživatelsky příjemnější.
- **Menu utilities**: Dialogové utility, spouštěné ze síťové stanice jsou programy, které ovládáme klávesnicí prostřednictvím menu. I těm jsem se snažil v knize vyhnout.
- **Graphical utilities:** jsou graficky (myší) ovládané programy. Na tento způsob ovládání jsme zvyklí z Windows a i já jsem se jej snažil preferovat. Jde například o program NetWare Administrator, či činnosti spojené s klientem sítě NetWare.

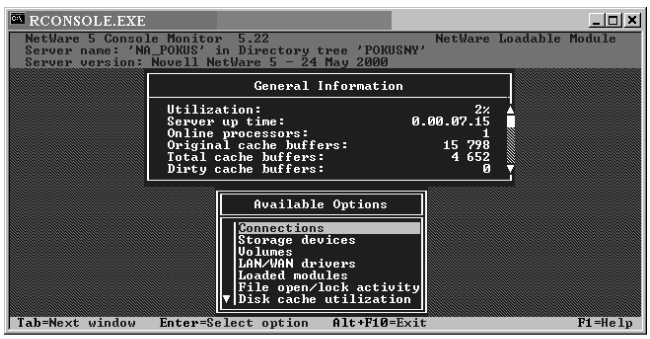
Loadable modules a Menu utilities mají shodné ovládání klávesami klávesnice:

- Šipky se používají pro pohyb mezi položkami menu
- Page Up, Page Down posunou kurzor na první, respektive poslední položku menu
- Enterem se položka vybírá, případně přecházíme do podmenu
- Insert přidává položku
- Delete maže vybranou položku
- F1 vyvolá nápovědu
- F3 modifikuje
- F5 označí položku (na označené položky můžeme aplikovat příkaz)
- F10 vybere položku, potvrdí volbu
- Esc – přechod v menu o úroveň zpět, ukončení utility.



Obrázek 5.3: *Moduly spuštěné na serveru (po stisku Alt + Esc)*

Na serveru NetWare je pravidelně spuštěno několik modulů, mezi nimiž se potřebujeme přepínat. Windows tento problém řeší pomocí oken. Jejich tlačítka pak vidíme na systémové liště a přepínání mezi okny spočívá ve stisknutí tlačítka myší. Na obrazovce serveru NetWare je přepínání mezi okny nejsnazší pomocí klávesové kombinace *CTRL + Esc*. Po současném stisku obou kláves uvidíme na obrazovce seznam všech spuštěných modulů. Do konkrétního z nich se přepneme stiskem příslušné číselné klávesy. Mezi jednotlivými moduly se můžeme také cyklicky přepínat kombinací kláves *Alt+Esc*.



Obrázek 5.4: *Úvodní obrazovka modulu Monitor*

Vypnutí serveru

Práci serveru není možné uzavřít jednoduchým vypnutím počítače! Je nutné nejdříve ukončit všechny činnosti systému, ten pak zaparkovat a až potom vypnout počítač. K tomuto účelu slouží příkaz konzoly *DOWN*.

Před vypnutím serveru je navíc potřeba zjistit, zda na serveru nepracují uživatelé (nečekaným vypnutím serveru mohou přijít o rozpracovaná data, mohou také havarovat některé aplikační programy, či moduly samotného NetWare). Za tím účelem použijeme modul MONITOR a jeho volbu *Connections*, v ní vidíme připojené uživatele. Umístíme-li na některého z nich kurzor a zmáčkneme klávesu *Enter*, spatříme ještě soubory, s nimiž uživatel pracuje. Pokud nemá otevřeny žádné soubory, můžeme uživatele odpojit klávesou DEL. Pokud vypínáme server, na jehož discích některý z uživatelů pracuje, budeme na to serverem upozorněni.

Tip: Aby se nám na vypínaný server nepřihlašovali noví uživatelé (zatímco odhlašujeme jiné), je možné přihlášení zakázat příkazem **DISABLE LOGIN**. K povolení přihlašování dojde restartem serveru nebo příkazem **ENABLE LOGIN**.

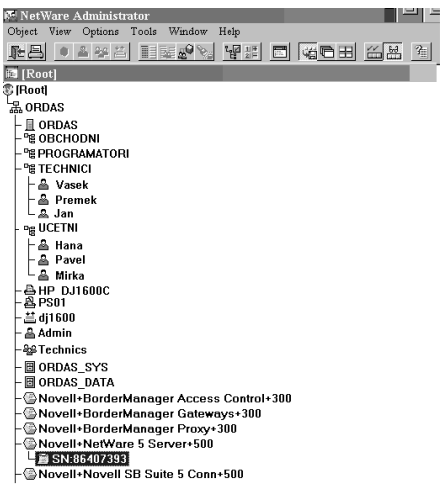
Databáze eDirectory

Je jedním ze základních pilířů NetWare. Jde o databázi, v níž jsou zapsány všechny informace týkající se objektů sítě. Je zde seznam všech uživatelů (i s jejich přístupovými jmény a hesly), informace o serverech v síti (těch může být více), údaje o tiskárnách (a tiskových serverech a frontách) a spousta dalších dat (o počítačích v síti a programech zde nainstalovaných, o zdrojích UPS, o licencích…). Databáze síťových objektů byla poprvé použita u verze NetWare 4, tehdy ještě pod jménem *NDS* (*Novell Directories Services*)

Informací o síťových objektech je mnoho, a tak pro ně platí přesně definovaná pravidla. Nebudeme se jim věnovat detailně, ale některá z nich (nutná pro pochopení práce NetWare) nemůžeme ignorovat.

Základním znakem eDirectory je její **globálnost**: Mějme velkou síť, tvořenou několika servery, okolo nichž jsou vybudovány lokální sítě. Pro celou síť bude operačním systémem vytvořena jen jedna databáze eDirectory. Svým přihlašovacím jménem se tady můžeme přihlásit z kterékoliv stanice v síti, vždy se přihlásíme do stejné (a jediné) databáze eDirectory. Globálností tedy rozumíme to, že eDirectory je jen jedna, pro libovolně velkou síť. To značně usnadňuje správu sítě.

Další důležitou vlastností je **hierarchičnost** eDirectory. Všechny objekty databáze jsou řazeny do stromové struktury, pro niž platí pravidla, která přibližuje následující kapitola.



Obrázek 5.5: *Databáze eDirectory*

Objekty eDirectory

Při výkladu použiji obrázek databáze eDirectory tak, jak jej vidíme v programu *NetWare Administrator*. S tímto základním programem pro práci v eDirectory se ještě mnohokrát setkáme a blíže si jej popíšeme. V příštích odstavcích si vysvětlíme, že v eDirectory jsou kontejnerové objekty. Poklepáním na jejich symbol otevřeme kontejner a uvidíme jeho obsah. (Na obrázku všechny kontejnery pochopitelně otevřeny nejsou.)

Základem eDirectory je kořenový objekt **[Root]**. Ten musí mít každá eDirectory.

Dále můžeme použít nepovinný objekt **Country**. V menších sítích LAN není obvykle používán (není ani v naší databázi na obrázku). Pokud by použit byl, musí být umístěn pod objektem [Root].

Důležitý je povinný objekt **Organization**. V každém eDirectory stromu musí být minimálně jeden. Na našem obrázku jím je objekt ORDAS. Pod něj se již umísťují koncové objekty, nebo objekty Organizational Unit.

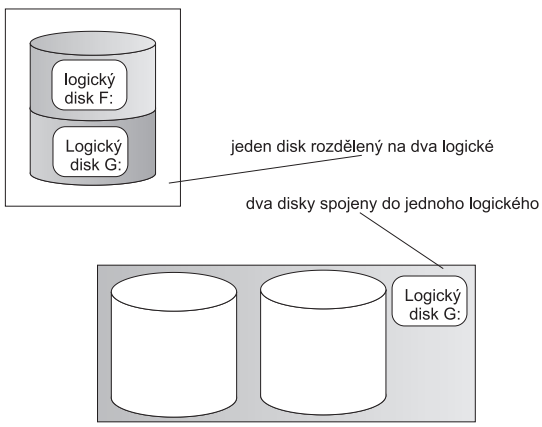
Organizational Unit je dalším možným typem. Představuje hlavní prostředek pro větvení databáze. Umožňuje zachycení struktury organizace a její převedení do eDirectory. Zpravidla odpovídá samostatným skupinám v podniku, odloučeným pracovištím či pobočkám podniku. V naší ukázkové databázi vidíme čtyři objekty *Organizational Unit* (samostatných pracovních skupin): OBCHODNICI, PROGRAMATORI, TECHNICI, UCETNI.

Všechny dosud uvedené objekty měly jednu společnou vlastnost – databáze se v nich větvila. V terminologii eDirectory se pro ně používá termín **kontejner, kontejnerový objekt**. Kromě větvení mají kontejnerové objekty

ještě jednu důležitou funkci, umožňují dědění práv a vlastností. Přidělíme-li kontejneru nějaké právo, bude se toto dědit na celý obsah kontejneru (všechny objekty v něm obsažené).

Při správě sítě nejvíce pracujeme s **koncovými objekty**. Jde o prvky, které popisují skutečně existující součásti sítě. Koncových objektů je velmi mnoho a s každou novější verzí eDirectory přibývají. My si ukážeme pouze objekty s nimiž se při běžné správě sítě setkáme nejčastěji:

- Objekt typu **User** zastupuje uživatele, kterému je dovoleno pracovat v síti. Mezi jeho typické vlastnosti patří jméno a heslo, kterým se do sítě hlásí, práva popisující povolené (či nepovolené) činnosti ve složkách, souborech nebo vztazích k jiným objektům. S tímto objektem pracuje správce sítě velmi často. Na obrázku vidíme uživatele v kontejnerech TECHNICI a UCETNI. Dalším je uživatel Admin umístěný přímo v objektu Organizational unit.
- Objekt typu **Server** se instaluje automaticky. Představuje síťový server (v jedné eDirectory jich může být více). Obsahuje především popisné informace (umístění serveru, jeho síťovou adresu apod.).
- Pro práci s tisky existují tři základní síťové objekty. Práci s nimi si vysvětlíme v kapitole Síťové tisky, takže stručně: *Print server* – tiskový server (na obrázku PS01), *Print Queue* – tisková fronta (dj1600) a *Printer* – tiskárna (HP DJ1600).
- Objekt typu **Group** představuje skupinu uživatelů, jimž je možné delegovat stejná práva. Stejnou funkci umožňuje kontejnerový objekt. Group je v podstatě přežitkem z doby bindery (databáze uživatelů z verzí NetWare 3.x), v níž kontejnery nebyly k dispozici. Na obrázku vidíme skupinový objekt *Technics*.
- Objekt **Volume** (logický disk) reprezentuje logický disk serveru. V NetWare je možné na jednom fyzickém disku vytvořit několik disků logických, nebo z několika fyzických disků vytvořit jeden disk logický. S logickým diskem (představovaný logickým jménem) pak pracujeme. V naší databázi vidíme dva logické disky ORDAS_SYS a ORDAS_DATA. (Disk vždy nese jméno serveru + vlastní jméno disku).



Obrázek 5.6: *Logické a fyzické disky*

Pod objekty Volume vidíme zvláštní kontejnerové objekty, určené pro správu licencí. Jde o **License container objects** (na obrázku např. *Novell NetWare 5 server + 500).* Do tohoto objektu se vkládají **License certificate objects** (licenční certifikáty), nesoucí informaci o vlastní licenci. (Licenční certifikáty byly poprvé zavedeny v NetWare 5.)

Dalším objektem vymykajícím se běžným pravidlům je objekt **[Public]**. Vytváří se automaticky, při první instalaci serveru. Souvisí s objektovými právy, práva jemu přidělená platí pro všechny uživatele sítě.

Na závěr krátké shrnutí: eDirectory se skládá z kontejnerových objektů, v nichž jsou vloženy jiné objekty kontejnerové nebo koncové. Hierarchie kontejnerových objektů je přesně stanovena. Koncové objekty vkládáme do kontejnerů. Pro popis objektů eDirectory se používají anglické termíny, často se však setkáme s jejich českými ekvivalenty. Jejich souvislost ukazuje tabulka

Tabulka 5.1: Anglické a české názvy objektů eDirectory

Anglický název objektu	**Český ekvivalent**	
Container objects	***Kontejnerový objekt***	***zkratka***
[Root]	Kořenový objekt	
Country	Země	C
Organization	Organizace	O
Organizational Unit	Organizační jednotka	OU

Anglický název objektu	Český ekvivalent
Leaf object	***Koncový objekt***
User	Uživatel, uživatelský účet
Server	Server
Group	Skupinový objekt
Print server	Tiskový server
Print Queue	Tisková fronta
Printer	Tiskárna
Volume	Logický disk

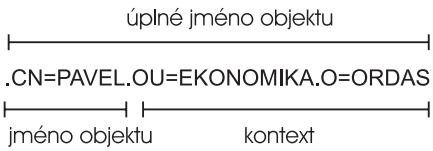
Kontext a jméno objektů

Při práci s objekty je nutné objekt pojmenovávat tak, aby se v jeho jménu odrazila poloha objektu ve struktuře eDirectory. Tato potřeba není sice častá, ale její nerespektování může způsobit značné potíže. V souvislosti s pojmenováním objektu musíme rozlišovat tyto pojmy:

Kontext objektu (object context) vyjadřuje polohu objektu ve stromu eDirectory, určuje tedy kontejner, v němž se objekt nachází. Ve skutečnosti jde o výčet kontejnerových objektů, přičemž se začíná od kontejneru, v němž je objekt obsažen, až ke kořenovému objektu [Root]. Uveďme příklad: kontext objektu Pavel je *.UCETNI.ORDAS* (používám stále obrázek databáze eDirectory z předešlé kapitoly). V kontextu se často používají symboly indikující o jaký objekt se jedná. Se symboly bude stejný kontext vypadat takto: *.OU=UCETNI.O=ORDAS*. Všimněte si povinných teček mezi objekty kontextu a tečky první, kterou je kontext uveden. Zkratky jsou odvozeny ze jmen kontejnerových objektů – vidíte je v tabulce.

Jméno objektu (*object name*) je množina znaků, popisující konkrétní objekt. Jméno většinou zadává správce sítě.

Úplné jméno objektu (complete name) vznikne spojením jména objektu a kontextu. Pro objekt Pavel bude úplné jméno: *.PAVEL.UCETNI.ORDAS*, použijeme-li variantu se zkratkami: *.CN=PAVEL.OU=UCETNI.O=ORDAS*. Koncový objekt je zastoupen zkratkou CN (*Common Name*).

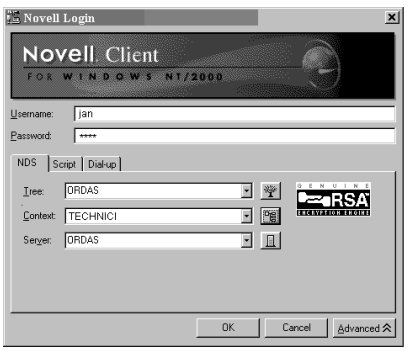


Obrázek 5.7: *Jména objektu eDirectory*

Při přihlašování k serveru je jedním z přihlašovacích parametrů i kontejner, kam se přihlašujeme. Pokud nastavíme, že uživatel Pavel se bude přihlašovat přímo do kontejneru *UCETNI*, bude jeho aktuální kontext *.OU=UCETNI.O=ORDAS*. Jestliže uživatel Pavel bude pracovat s objektem *Hana*, může použít tzv. **current context**. Z hlediska *Pavla* je *Hana* ve stejném kontextu a její relativní úplné jméno (vzhledem k Pavlovi) je *.CN=Hana*.

Přihlášení do sítě (přesněji ke stromu databáze eDirectory)

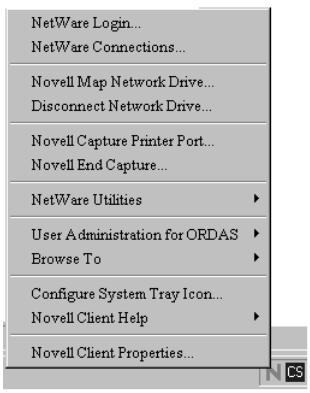
Při přihlášení do sítě se uživatel musí přihlásit do stromu a kontextu, v němž je umístěn jeho uživatelský objekt. Většina uživatelů se přihlásí do svého kontextu a již jej nepotřebuje měnit. Nejčastěji se kontext vkládá při prvním přihlášení uživatele. (Na obrázku přihlašovacího okna vidíme uživatele *Jan*, hlásícího se do kontextu TECHNICI stromu ORDAS.)



Obrázek 5.7: *Přihlašovací okno Klienta sítě NetWare od firmy Novell*

Červené okno novellského klienta má ve standardním zobrazení pouze dva řádky: *Username* (sem píšeme jméno, jímž se do sítě hlásíme) a *Password* pro zadání hesla. K dispozici je také tlačítko „*Advanced*". Jeho stiskem rozšíříme obrazovku klienta o další upřesňující možnosti. My se zaměříme na kartu *NDS*. V jejím prvním řádku je vepsáno jméno stromu databáze eDirectory, k níž se hlásíme (jde o název objektu *Organization*), v druhém řádku je kontext, do něhož se přihlašujeme a v posledním řádku najdeme jméno serveru. Všechny údaje je nutné sem zapsat při prvním startu klienta. S tím nám pomohou tlačítka vedle jednotlivých řádků. Jejich stiskem prohlédneme síť a získáme možnosti volby. Vše pracuje v grafickém režimu, nemusíme se starat o syntaktická pravidla zápisu. (Podrobný popis konfigurace klienta je v kapitole *Klient systému NetWare*.)

Tip: Jestliže se nám nedaří přihlášení do sítě, stiskneme tlačítko Advanced a zkontrolujeme správnost údajů v jednotlivých řádcích karty NDS. Pokud je vše v pořádku, chyba bude v nesprávném hesle nebo přihlašovacím jménu.



Obrázek 5.8: *Menu klienta sítě NetWare*

Během práce se můžeme připojit k další databázi eDirectory (i když to nebývá obvyklé). Klepneme pravým tlačítkem myši na ikonu *N* novellského klienta (pravý dolní roh systémové lišty). Rozevře se menu, jehož první řádek *NetWare Login…* je určen k přihlašování. Po jeho výběru se otevře obrazovka klienta. V ní musíme vyplnit (případně vyhledat) přihlašovací údaje k dalšímu stromu eDirectory (jde o *username*, *password*, *NDS Tree*, kontext a jméno serveru).

Tip: Budete-li pracovat s několika novellskými sítěmi, použijte druhý řádek v menu klienta – NetWare Connections. Nabízí přehled novellských zdrojů, k nimž jsme přihlášeni.

Odhlášení od serveru

Od serveru se odhlásíme automaticky, legálním ukončením Windows. Navíc seznam připojených uživatelů je operačním systémem pravidelně aktualizován. Když některý z přihlášených uživatelů neodpovídá, je od serveru odpojen.

Pokud se chceme od serveru odpojit, aniž bychom ukončovali Windows, využijeme novellského klienta. Poklepeme na položku Místa v síti a vybereme síť NetWare, v níž uvidíme ikonu serveru. Na ni ťukneme pravým tlačítkem myši a v menu použijeme řádek *Logout*.

Uživatelé sítě

Na serveru bývá vytvořeno více uživatelů (uživatelských účtů). Jeden z uživatelů je správcem sítě (administrátorem), který vytváří objekty eDirectory (mezi nimi rovněž ostatní uživatele) a stanovuje, co tito uživatelé mohou dělat – jaká budou mít práva. Ve větších sítích může na některé uživatele převést část svých oprávnění – udělat z nich administrátory ve větvi databáze eDirectory apod. V podstatě rozeznáváme dva základní typy uživatelů:

- správce sítě, v NetWare má jméno *Admin* a instaluje se automaticky.
- „*částečný*" správce, uživatel na něhož *Admin* převedl část práv.
- *běžný uživatel*, který používá server jako jeden z datových zdrojů. Jeho práva jsou definována některým z výše uvedených administrátorů.

Zabezpečení sítě

NetWare, jako klasický síťový systém client server, má důkladné zabezpečení proti zneužití. Prvním bezpečnostním krokem je to, že se k serveru může přihlásit pouze uživatel, který zde má svůj účet (objekt v databázi eDirectory). Uživatel se může hlásit pouze svým jménem, a navíc je možné přihlašovací proces zpřísnit dalšími požadavky:

- *Heslem*, sice není povinné, ale je používáno téměř vždy.
- Zpřísněním požadavků na heslo.
- *Restrikcemi*: omezením času, kdy může uživatel na serveru pracovat.
- Omezením proti vetřelcům (jak se má systém zachovat, pokud se k němu opakovaně a neúspěšně někdo hlásí).

Konkrétní zadání těchto hodnot je uvedeno v následující kapitole.

Tip: Chceme-li účet dokonale zabezpečit heslem, je nutné dodržet určité podmínky, o nichž jsme se již zmínili v kapitolách o Windows Serveru. Heslo nesmí být krátké (min. 7 znaků), nemělo by být snadno odvoditelné (křestní jméno, jména dětí apod.), mělo by se pravidelně měnit. Požadavky na heslo však nesmíme přehnat. Donutíme-li uživatele používat nezapamatovatelné heslo složené z mnoha písmen a číslic, tak si je poznamená (někde u počítače) a bezpečnost je ta tam.

NetWare Administrátor

K administraci databáze eDirectory je určen program *NetWare Administrátor*. Najdeme jej na logickém disku *SYS* ve složce *PUBLIC* a jeho podsložce *WIN32*. Vlastní program, kterým administrátora spustíme, se jmenuje *NWADMN32*.

Protože se s programem *NetWare Administrátor* setkáváme poprvé, dovolím si několik poznámek:

- Program spouštíme ze stanice. Správu sítě tedy administrátor provádí ze svého počítače, fyzicky k serveru nechodí.
- Umístění administrátorského programu se ve verzích NetWare liší. Původně se jmenoval *NWADMIN* a byl umístěn v několika složkách, určených pro operační systémy síťových stanic (například v *PUBLIC/WIN95* – Windows 95). U starších verzí NetWare si program musíme najít a použít verzi odpovídající operačnímu systému naší stanice.
- Při dalším výkladu budu předpokládat, že čtenář je správcem sítě. Základem správy sítě je přidělování (či odebírání) práv jiným uživatelům. Pokud nebudete mít administrátorská práva, může se snadno stát, že většinu popisovaných akcí nebudete moci provádět.
- Pro činnost programu NetWare Administrátor je nutné, abychom nainstalovali *Klienta sítě NetWare* od firmy Novell. Používáme-li Klienta sítě NetWare od Microsoftu, není možné program NetWare Administrátor (a řadu jiných utilit) spustit. Instalace tohoto klienta je popsána v kapitole Klient systému NetWare.

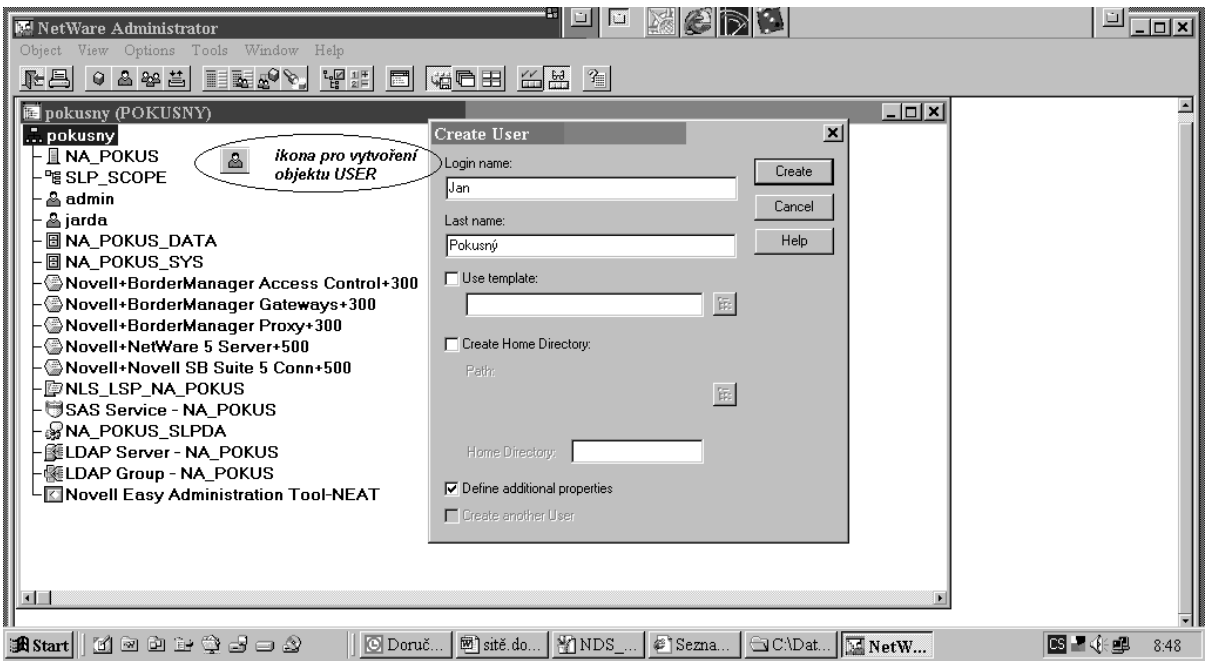
Tip: Správce sítě pracuje s programem NetWare Administrátor často, a tak se vyplatí udělat si jeho zástupce na ploše (např. ťuknout pravou klávesou myši na programu NWADMN32, vybrat řádek Vytvořit zástupce a umístit jej na plochu).

Při prvním spuštění programu bude jeho obrazovka prázdná. Je nutné v menu *Tools* vybrat funkci *NDS Browser* a zadat v kterém kontextu se bude okno administrátora otevírat (většinou vybereme objekt [Root]).

Vytvoření nového uživatelského účtu

Nového uživatele založíme takto:

- Nejdříve musíme umístit kurzor na kontejner, v němž bude nový účet obsažen.
- Pak ťukneme na symbol objektu *USER* na pracovní liště programu NetWare Administrátor.
- Na obrazovce *Create User* zadáme jméno, jímž se bude nový uživatel identifikovat systému (řádek *Login name*) a příjmení uživatele (*Last name*) – tento údaj je sice povinný, ale slouží pouze k pomocné identifikaci uživatele.
- Doporučuji zatrhnout políčko *Define additional properties*, protože po stisku tlačítka *Create* se otevře konfigurační obrazovka uživatele a budeme moci dokončit definici jeho vlastností.
- Políčko *Create Home Directory* dovoluje novému uživateli přiřadit jeho domovskou složku.

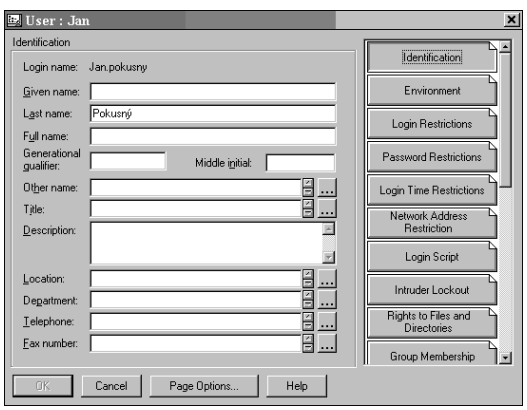


Obrázek 5.9: *Vytvoření uživatele*

> ***Poznámka:*** *K založení nového objektu v kontejneru slouží také tento postup: Klepnout pravým tlačítkem myši na kontejner a v následném menu použít řádek Create.*

Vlastnosti účtu

Po vytvoření uživatele (objektu *User*) nás systém přepne do jeho identifikační obrazovky. Tady můžeme vyplnit spoustu pomocných identifikačních údajů. Důležitá jsou tlačítka na pravé straně obrazovky. Těmi konfigurujeme účet. K některým se vrátíme ještě v následujících kapitolách, popis ostatních následuje.



Obrázek 5.10: *Identifikační obrazovka uživatele*

Login restrictions: Definuje omezení při přihlášení. Možnosti ukazuje tabulka:

Tabulka 5.2 Omezení pro přihlašování k uživatelskému účtu

Account Disabled	Účet je vypnut, není se k němu možné přihlásit
Account Has Expiration Date	Platnost účtu vyprší … (nastavuje se o řádek níže)
Limit concurrent connections	Počet současných přihlášení k účtu. Pod jedním jménem se může přihlásit více uživatelů - pokud to zde neomezíme
Last login	Informuje o posledním přihlášení

Password restrictions: popisuje vlastnosti hesla, podrobnosti opět ukazuje tabulka:

Tabulka 5.3 Vlastnosti hesla

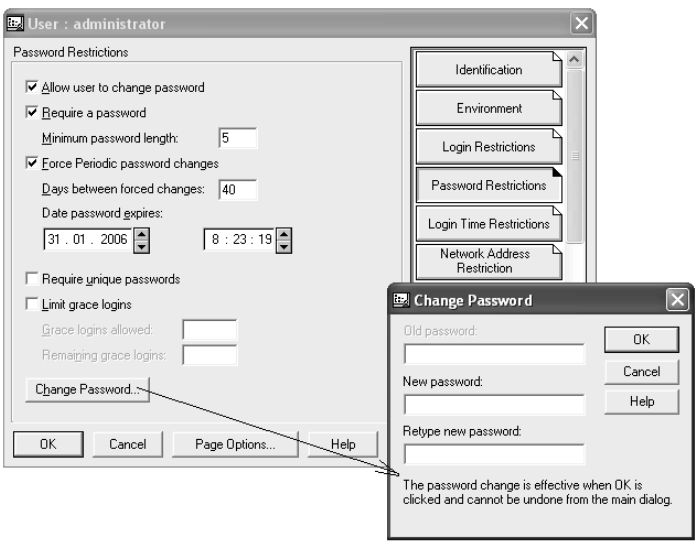
Allow User to Change Password	Uživatel si může měnit vlastní heslo
Require a Password	Heslo bude použito (jinak se bude uživatel přihlašovat bez nutnosti zadávat heslo!)
Minimum Password Length	Minimální délka hesla (myslí se počet znaků)
Force Periodic Password Changes	Zaškrtnutím vyžádáme periodické změny hesla
Days between Forced Changes	Počet dnů platnosti hesla (pak bude muset být změněno)

Tvar hesla zapíšeme po stisku tlačítka *Change Password*. Zápis hesla provádíme dvakrát – oba tvary hesla musejí být shodné. Při práci s heslem samotné heslo nikdy nevidíme, je nahrazeno hvězdičkami.

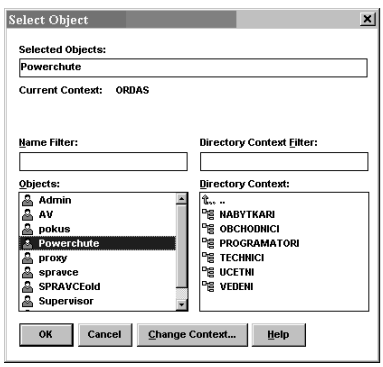
Login Time Restriction: Omezení doby, kdy se uživatel může přihlásit. Myší zabarvíme ta políčka, v nichž je přihlášení zakázáno.

Rights to Files and Directories: Přístupová práva ke složkám a souborům, jde o velmi důležité nastavení, vrátíme se k němu v kapitole *Přístupová práva a NetWare Administrátor*.

Group membership: Přiřazení účtu k uživatelské skupině. Ťukneme na tlačítko *ADD* a vybereme skupinu, do níž bude uživatel přiřazen.



Obrázek 5.11: *Nastavení hesla*



Obrázek 5.12: *Vyhledávací okno objektů eDirectory*

Security Equal to Me: Ekvivalence s jiným objektem. Pokud chceme, aby nový uživatel měl stejná práva jako některý z již existujících, provedeme to tímto tlačítkem. Když však „vzorový" objekt smažeme, vše se ruší – ekvivalence zanikne. Ekvivalenci přiřadíme ťuknutím na tlačítko *ADD*. Pak vybereme objekt k němuž požadujeme ekvivalenci.

Při výběru objektu (např. po stisku tlačítka *ADD*), máme k dispozici obrazovku *Select Object*. V její pravé části se přepínáme mezi kontexty a v levé vybíráme hledaný objekt.

Poznámka: Vlastnosti účtu je možné měnit kdykoliv. Stačí poklepat na účet a otevřeme identifikační obrazovku s výše popsanými tlačítky.

Tip: Každý uživatelský účet je možné smazat. Jde to dokonce i s účtem Admin (jeho smazáním ztrácíme kontrolu nad administrací sítě). Proto Novell doporučuje vytvořit dva administrátorské účty. Ten druhý – náhradní nepoužívat, ale jeho vlastnosti si zapsat a použít je v případě ztráty prvního administrátorského účtu. (Postup najdete v kapitole Objektová práva a NetWare Administrator.)

Souborový systém

Při správě serveru musíme znát jeho souborový systém a z něho vyplývající souvislosti. Od verze NetWare 5 jsou k dispozici dva souborové systémy: klasický (použitý u předešlých verzí) a nový *NSS* (*Novell Storage Services*), jehož použití se především ve verzích 6.x preferuje.

Typ souborového systému (*klasický* či *NSS*), velikosti, jména a počty disků jsou záležitostí instalace. Tu běžně správce sítě neprovádí a ani v této knize není popsána. Běžný uživatel, přistupující k serveru ze sítě, nepozoruje mezi souborovými systémy žádný rozdíl. Přesto by správce měl mít představu o vlastnostech svého souborového systému. Pokusíme se tedy porovnat několik parametrů obou souborových systémů.

Tradiční souborový systém

Klasický souborový systém má dlouhou tradici, byl použit ve všech starších síťových operačních systémech NetWare. Šlo o verze 3.x, 4.x, verze 5.x přinesla možnost použití nového systému *NSS* a ve verzích 6.x má již přednost nový systém *NSS*. Ve všech verzích je však stále starý souborový systém k dispozici. Mezi jeho podstatné parametry patří:

- Na jednom serveru může být maximálně 64 logických disků.
- Logický disk může být rozprostřen maximálně přes 32 segmentů.
- Na jednom fyzickém disku může být maximálně 8 logických disků.

Tradiční souborový systém je organizován podobně jako u jiných operačních systémů: Základem je diskový oddíl (oblast) NetWare, v ní jsou vytvořeny logické disky a zde pak složky a soubory.

Souborový sytém NSS

NSS je novým systémem, který přinesl vylepšení v mnoha směrech. Především se zvětšily limity jeho maximálních hodnot:

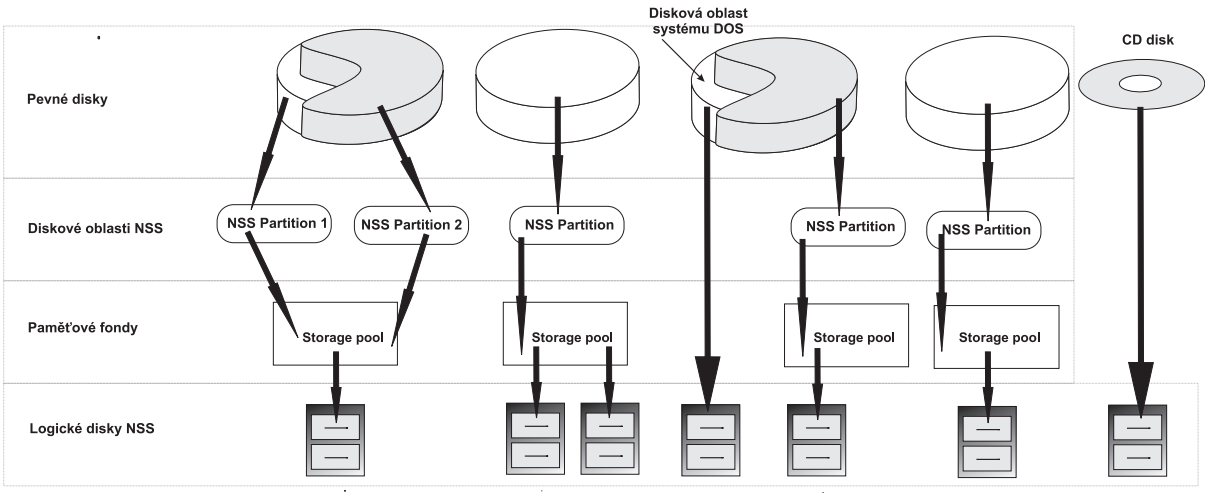
- Maximální počet současně namontovaných logických disků na serveru je 255
- Maximální počet souborů na logickém disku je 8 trilionů
- Maximální velikost jednotlivých disků a složek je 8 EB
- Maximální velikost jednoho souboru může být až 8 TB
- Maximální počet současně otevřených souborů na serveru je 1 milion

Kromě zvýšení maximálních limitů přináší *NSS* další výhody: Velmi rychle montuje logické disky, potřebná velikost operační paměti nezávisí na kapacitě připojovaného disku, je možné namontovat také CD disky (a následně je sdílet s ostatními uživateli jako běžné logické disky), zrychlil se přístup k datům na discích, zrušený logický disk NSS je možné do určité doby opravit, je umožněno zálohování otevřených souborů...

Koncepce NSS

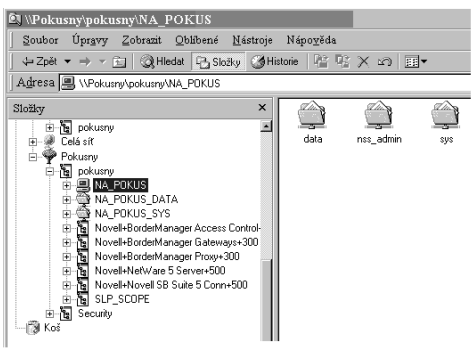
Organizace dat v souborovém systému NSS je odlišná od běžných principů, a proto si její základní zásady přiblížíme. Jednotlivé části struktury NSS ukazuje obrázek *Koncepce NSS.*

- Oblast NSS je přirozeně umístěná na pevných discích. Na každém disku se vytvářejí diskové oblasti NSS (*NSS partitions*), přičemž je možné vytvořit na jednom disku několik NSS oblastí.
- Na diskové oblasti navazují paměťové fondy (*storage pools*). Paměťový fond může být vytvořen pro jednu nebo několik oblastí NSS. Není však možné definovat v jedné diskové oblasti více jak jeden paměťový fond. Kapacitu paměťového fondu je možné postupně zvyšovat přidáváním nových diskových oblastí NSS.



Obrázek 5.13: *Koncepce NSS*

- Uživatel sítě vidí až logické disky NSS (*NSS logical volume*). V jednom fondu může být umístěn jeden, nebo několik logických disků. Velikost logického disku může být pevná, nebo proměnná. Disk proměnné velikosti dynamicky vyplňuje celý volný prostor paměťového fondu. Pokud fond rozšíříme o další diskovou oblast, zvětšíme kapacitu logického disku. Odpadají nám tak starosti s postupným zaplňováním diskového prostoru.
- Obrázek ukazuje také možnost připojení CD disku. Jako zvláštní oblast NSS je možné připojit rovněž diskovou oblast operačního systému DOS (která slouží ke startování NetWare). Praktický význam to má hlavně při správě serveru.



Obrázek 5.14: *Logické disky serveru*

To jaké disky na serveru máme, zjistíme např. přes *Průzkumníka*. V něm si otevřeme *Okolní počítače*, poklepeme na jméno stromu databáze *eDirectory*. V něm již vidíme server *NetWare* a jeho logické disky.

Na obrázku vidíme databázi *eDirectory* s názvem *Pokusny*. Zde je kontejner typu *Organizational Unit OU=Pokusny* a v něm server s jménem *NA*_POKUSY. Na něm vidíme dva logické disky *SYS* a *DATA*, (*NSS_ADMIN* je část diskového prostoru, rezervovaná pro správu disků systému NSS. Automaticky se vytváří při instalaci).

Poznámka: *Pro logický disk se také používá termín svazek či volume.*

Systémové složky

Základem souborového systému je logický disk. Podle toho jak vytvoříme diskové oblasti a uspořádáme paměťové fondy, může být na jednom fyzickém (tj. skutečném) disku několik disků logických, nebo naopak jeden disk logický může být rozprostřen přes více disků fyzických. NetWare musí mít alespoň jeden logický disk se jménem SYS. Zde jsou uloženy veškeré systémové soubory a systémová databáze eDirectory. Další logické disky slouží pro ukládání dat.

Tip: NetWare je možné nainstalovat i tak, že bude mít jen disk SYS, na který se budou kromě systémových souborů rovněž ukládat data. Tento postup však nedoporučuji. Pokud dojde k havárii disku, je to velmi často právě disk SYS a my přijdeme o všechna data. Jsou-li data uložena ve vyčleněné diskové oblasti (na zvláštním logickém disku), dá se tento disk po opětovné instalaci připojit a data zachránit.

Pokud však používáte ochranu prostřednictvím polí RAID, je nebezpečí diskové chyby eliminováno polem RAID a počet logických disků je dán spíše organizačními potřebami konkrétní sítě.

Na disku SYS jsou vytvořeny systémové složky nutné pro správu disků, mezi nejdůležitější patří:

Složka **SYSTEM** obsahuje souborové systémy vlastního NetWare a některé programy pro konfiguraci. Do této složky má přístup pouze správce sítě (*Admin*).

PUBLIC je složka určená všem uživatelům. Je tedy veřejná (public) a všem přístupná. Jsou zde soubory a příkazové utility, které mohou používat všichni uživatelé sítě. V této složce jsou ještě podsložky s utilitami spustitelnými z jednotlivých operačních systémů klientských stanic.

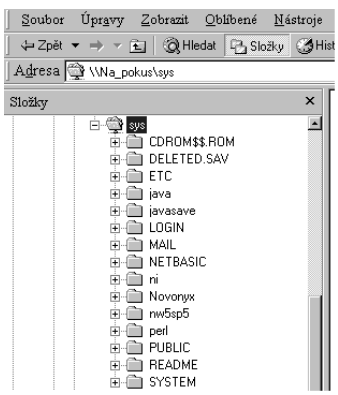
LOGIN zde jsou soubory související s přihlášením uživatelů do sítě. Je to jediná složka serveru, kam mají přístup i nepřihlášení uživatelé. Uživatelé pak používají zdejší soubory pro přihlášení k síti.

Složka **MAIL** je určen pro síťovou poštu. Běžně je prázdná, využijí ji hlavně poštovní programy kompatibilní s NetWare.

JAVA je určena pro moduly související se softwarovou technologií JAVA, s níž je NetWare kompatibilní a kterou také sám používá.

Složka **DELETED.SAV** používá samotný systém, my uživatelé si jí nebudeme všímat. Je určena pro logicky smazané soubory, konkrétně se sem ukládají ty soubory, jimž byl také smazána jejich složka. Mazání souborů a jejich případné obnově je věnována příští kapitola.

Další složky jsou již záležitostí správce serveru a uživatelů. Bývá zvykem, že na datovém svazku má svoji složku každá aplikace a také každý uživatel.



Obrázek 5.15: *Systémový disk SYS*

Obnova smazaných souborů

Mezi další speciality souborového systému NetWare patří způsob mazání souborů a složek. Běžné smazání souboru (či složky), které provedeme z libovolného souborového manažeru, označujeme jako logické. Takto smazaný soubor totiž zůstane dále (tj. fyzicky) ve složce, pouze není vidět. Zrušená složka se přesune do systémové složky *DELETED.SAV*, která je na každém logickém disku. Fyzicky tedy nezmizí ani smazaná složka.

Protože jsou smazané složky i soubory na disku fyzicky stále přítomné, je možné je zviditelnit – obnovit. NetWare pro obnovení používá termín *SALVAGE*.

Logicky smazané soubory a složky zabírají stále místo na disku. Pokud je toto pro nás problematické (potřebujeme uvolnit diskový prostor pro jiná data), můžeme logicky smazané objekty vymazat fyzicky – odstranit je z disku nenávratně. Pro fyzické mazání používáme termín *PURGE*.

Velikost prostoru disku pro smazané soubory je pevně stanovena, vymazané soubory nemohou tedy disk nikdy zaplnit. Pokud se prostor pro smazané soubory zaplní, jsou fyzicky odstraněny (*purge*) nejstarší smazané soubory.

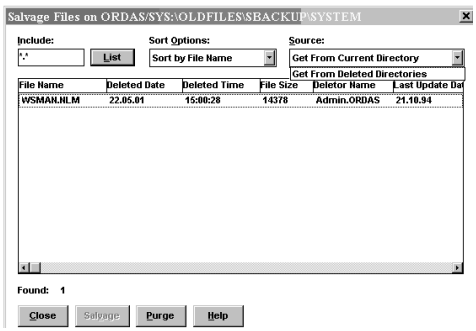
Obnova, či trvalé odstranění smazaných souborů NetWare Administrátorem

Praktickou obnovu můžeme provést programem *NetWare Administrátor*. Nejdříve otevřeme objekt typu *Volume* (tj. logický disk na serveru) a vybereme složku, v níž je umístěn smazaný soubor. Pak použijeme menu *Tools* a volbu *Salvage*. Systém nabídne obrazovku pro obnovu souborů:

Tlačítko *List* je určeno pro vypsání seznamu obnovitelných souborů. Pokud necháme v sousedním okénku *Include* zapsánu hvězdičkovou konvenci, vypíší se všechny obnovitelné soubory. Můžeme také rovnou napsat jméno souboru, či specifikovat výpis pouze pro některé typy souborů (např. *.bat – bude hledat pouze soubory s příponou bat apod.). Důležité je také okénko *Source*, v němž můžeme nastavit dvě možnosti:

- *Get from Current Directory* bude vyhledávat smazané soubory pouze v aktuální složce.
- *Get from Deleted Directories* použijeme, pokud byly hledané soubory umístěny ve smazané složce (bude se vyhledávat ve složce *DELETED.SAV*).

Na obrazovce uvidíme seznam smazaných souborů, ty pak můžeme tlačítkem *Salvage* obnovovat, či stiskem *Purge* nenávratně odstranit.

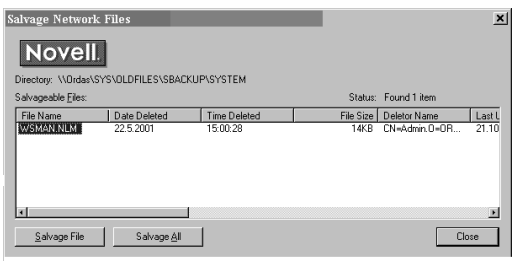


Obrázek 5.16: *Obnova (fyzické smazání) smazaných souborů*

Tip: Soubory v seznamu můžeme označovat podle běžných zvyklostí Windows:
Levé tlačítko myši + klávesa Ctrl vybírá jednotlivé soubory
Levé tlačítko myši + klávesa Shift vybírá všechny soubory mezi dvěma označenými

Smazané soubory a klient NetWare

Informace související s logicky smazanými soubory získáme snadno také prostřednictvím novellského klienta. V *Průzkumníkovi* (či v *Místech v síti*) najdeme na serveru logický disk NetWare a složku, v níž byl smazaný soubor uložen. Ťukneme na něm pravým tlačítkem myši a v menu vybereme *Salvage Files*. V okně pak vidíme všechny smazané soubory. Tlačítkem *Salvage File* můžeme obnovit kurzorem vybraný soubor, tlačítkem *Salvage All* obnovíme všechny soubory najednou.



Obrázek 5.17: *Obnova souboru*

Pokud chceme disk zbavit smazaných souborů, použijeme místo *Salvage Files* volbu *Purge Files*. Obdržíme podobné okénko jako v předešlém případě. Můžeme fyzicky mazat jeden soubor (*Purge Files*, vše ve složce *Purge All*, nebo do mazání zahrnout také podsložky *Purge Subdirectories*).

Smazané soubory a atributy

Každému souboru a složce je možné přidělit atributy (jejich seznam najdete v podkapitole *Atributy* kapitoly *Přístupová práva ke složkám a souborům*). Ty pak „vnucují" složce (souboru) některé vlastnosti. V souvislosti s mazáním souborů máme k dispozici tyto atributy:

- **Delete Inhibit** – zakazuje smazat složku nebo soubor.
- **Purge Immediate** – jeho přidělením zrušíme dvoustupňové mazání, mazaný objekt nebude mazán logicky, ale rovnou fyzicky. Bude tedy okamžitě odstraněn z disku.

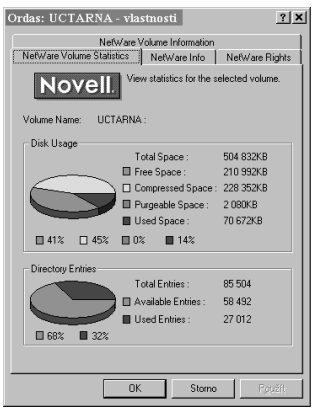
Poznámka: Pro práci se soubory a složkami je nutné definovat přístupová práva (viz kapitola Přístupová práva ke složkám a souborům). Platí to i pro obnovu souborů – pokud chceme obnovovat, musíme mít patřičná souborová práva. Nebo být rovnou přihlášeni jako uživatel Admin.

Komprese souborů (file compression)

NetWare provádí automatickou kompresi nepoužívaných souborů (implicitně je nastaveno, že se komprimují soubory, s nimiž se nepracovalo 14 dní). Komprimace (pakování) souborů spočívá v jejich zakódování speciálním algoritmem. Výsledkem je zmenšení diskového prostoru, který byl souborem obsazen. Pokud však budeme chtít soubor použít, musí jej systém rozbalit, což zabere nějaký čas. Díky automatickému pakování (provádí se denně v čase 0–6 hod) dochází k významné úspoře místa na disku. Máme-li však disk zaplněn a obsazen starými spakovanými soubory, může se stát, že nebude možné soubor rozbalit – na to nás samozřejmě systém upozorní hlášením: *„Insufficient disk space to decompress file ...".*

S komprimaci souvisejí tyto **atributy**:

- **Can't Compress –** soubor nebude komprimován, protože úspora místa by byla nevýznamná (méně jak 20%)
- **Compressed –** soubor je zkomprimován
- **Don't Compress –** soubory ve složce nebudou komprimovány
- **Immediate Compress –** zajistí okamžitou komprimaci



Obrázek 5.18: *Obsazení prostoru na disku*

Informace o souborech na disku

Souborový systém NetWare je poměrně složitý, nabízí mnoho variant. Informace o tom, jak to na disku vypadá, získáme naštěstí snadno: Pravým tlačítkem myši klepneme na logický disk a vybereme *Vlastnosti*. Na záložce *NetWare Volume Statistics* máme k dispozici údaje o logickém disku, které vysvětluje tabulka (jednotlivé části disku jsou rozlišeny barevně, proto jsem k popisu připojil i význam jednotlivých barev):

Tabulka 5.4: Rozdělení prostoru na disku

Anglický termín	Význam	Barva
Total space	Celková kapacita disku	
Free space	Volné místo na disku	fialově
Compressed space	Místo obsazené komprimovanými soubory	zeleně
Purgeable Space	Místo obsazené logicky smazanými soubory (uplatněním Purge jej lze uvolnit)	červeně
Used space	Místo obsazené nezkomprimovanými soubory	modře

Přístupová práva ke složkám a souborům

Základem práce síťového operačního systému je služba *File server*. Její součástí je ochrana složek a souborů před neoprávněným přístupem. Touto technologií je možné velmi přesně určit co kdo může dělat v konkrétní složce, případně s určitým souborem. NetWare má přidělování práv důkladně propracováno, vlastní systém se skládá z několika částí:

- **Trustee** (pověřenci) – přímo definují právo uživatele ke konkrétní složce či souboru.
- **Inherited rights filters – IRF** (filtry děděných práv) – pokud nejsou ke konkrétní složce či souboru stanovena pověření (Trustee), dědí se práva z nadřazené složky podle pravidel IRF.
- **Effective Rights** (efektivní práva) jsou výsledkem možných kombinací předešlých postupů. Je to skutečné právo, kterým uživatel disponuje.
- Každé složce i jednotlivým souborům jsou přiděleny ***atributy***. Ty je možné odebírat i přidávat a ještě více ovlivňovat vlastnosti složek a souborů.

Druhy práv

Práva, jež máme k dispozici v NetWare, ukazuje tabulka. Všimněte si, že právo je možné přidělit jak složce, tak souboru. Pro obě varianty existují drobné odchylky ve významu práv.

Tabulka 5.5: Přístupová práva

Název práva	Zkratka	Význam pro složky	Význam pro soubory
Supervisor	**S**	Poskytuje všechna práva ke složkám i k podsložkám a souborům ve složce uloženým. Právo S nelze blokovat systémem IRF.	Poskytuje všechna práva ke konkrétnímu souboru. Právo S nelze blokovat systémem IRF.
Read	**R**	Umožňuje soubory ve složce otevírat, číst a spouštět	Umožňuje daný soubory otevírat, číst a spouštět
Write	**W**	Umožňuje soubory ve složce otevírat, zapisovat do nich a modifikovat jejich obsah	Umožňuje daný soubor otevírat, zapisovat a modifikovat jeho obsah
Create	**C**	Dovoluje v dané složce vytvářet nové podsložky a soubory	Dovoluje daný soubor obnovit po jeho logickém zrušení
Erase	**E**	Umožňuje zrušit složce všechny její podsložky a soubory	Umožňuje zrušit daný soubor
Modify	**M**	Dovoluje měnit atributy a přejmenovat složku, soubory zde obsažené i podsložky. (Obsah složky a jejích souborů však měnit neumožňuje.)	Dovoluje měnit atributy a přejmenovat, soubor (Obsah souboru však měnit neumožňuje.)
File Scan	**F**	Umožňuje vidět danou složku a její soubory	Umožňuje vidět daný soubor (včetně všech jeho nadřazených složek)
Access Control	**A**	Dovoluje ke složce, podsložce a souborům v nich umístěným, přidělovat Trustee (tj. výše uvedená přístupová práva, kromě práva S) a upravovat filtry děděných práv IRF	Dovoluje k souboru přidělovat Trustee (tj. výše uvedená přístupová práva, kromě práva S) a upravovat jeho filtr děděných práv IRF.

V praxi se používají určité kombinace práv, povolující smysluplné činnosti (i když jiné kombinace jsou také možné). Všimněme si, že kombinace novellských práv se v literatuře uzavírá do hranatých závorek.

Tabulka 5.6: Nejčastěji používané kombinace práv

Kombinace práv	Dovoluje činnost
[]	Žádná práva, uživatel dokonce soubor ani složku nevidí
[RF]	Standardní kombinace práv, jejím výsledkem je možnost spouštění souborů a prohlížení obsahu složek (například je použita pro složku SYS:PUBLIC)
[RWCEF]	Rozšířená práva. Oproti předešlé variantě mohou uživatelé vytvářet, modifikovat a rušit soubory. Používá se pro běžné aplikační programy, jimiž upravujeme obsah datových souborů. Navíc si většina aplikačních programů vytváří své dočasné soubory (do nich si ukládá data) a po skončení práce tyto soubory maže – k tomu je třeba této kombinace práv!
[RWCEMFA]	Uživatel má úplnou kontrolu nad složkou
[S]	Opět plná kontrola, ta navíc není ovlivněna filtry práv (IRF)

Z tabulky vyplývá, že pohled uživatelů s různými přístupovými právy na server je odlišný. Každý z nich vidí různé složky (přesněji jen ty složky, k nimž má právo *F*). Nemá-li právo *F* k žádnému prostředku na logickém disku, nevidí dokonce ani tento disk.

Trustee (pověřenci)

Práva se vztahují k uživatelům, ale je možné je zadat i skupinám (objektu *Group*), nebo kontejneru. Je tak možné si přidělování práv zjednodušit – právo přidělené skupině uživatelů se automaticky deleguje na všechny členy skupiny, právo kontejneru platí i pro všechny objekty v kontejneru.

Objekt, jenž má přímo přidělená práva k určité složce, je pověřencem (*Trustee*) této složky (totéž platí i pro soubory).

Inherited rights filters – IRF (filtry děděných práv)

S pomocí trustee povolíme uživateli určité činnosti ve složce (či se souborem). Složky jsou seřazeny do stromové struktury a pokud bychom používali pouze *trustee*, bylo by nutné stále dokola definovat pověřence k dalším složkám. Aby k tomu nedocházelo, je systém správy souborových práv doplněn o funkci dědění práv. Podřízené složky dědí vlastnosti svých rodičů. Dědění však není automatické, je možné je omezovat. Další příjemnou vlastností je dědění práv na obsah složky – soubory. Soubory ve složce mají díky dědění stejná práva jako složka (pokud nestanovíme jinak a konkrétnímu souboru nepřidělíme *trustee*).

Princip dědění je založen na filtrech práv. Každá složka má svůj filtr práv sestávající ze všech práv – tedy [SRWCEMFA]. Pokud některé z práv z filtru vyjmeme, nebude se dále dědit – složka či soubor jej již od nadřízené složky nemůže obdržet.

Effective Rights (efektivní práva)

Práva ke složce (souboru) jsou definována dvěma způsoby (*trustee* a *IRF*). Jejich vzájemným působením obdržíme práva efektivní (skutečná), tedy ta, která uživatele opravdu omezují. Pokud o právech hovoříme, máme nejčastěji na mysli právě práva efektivní.

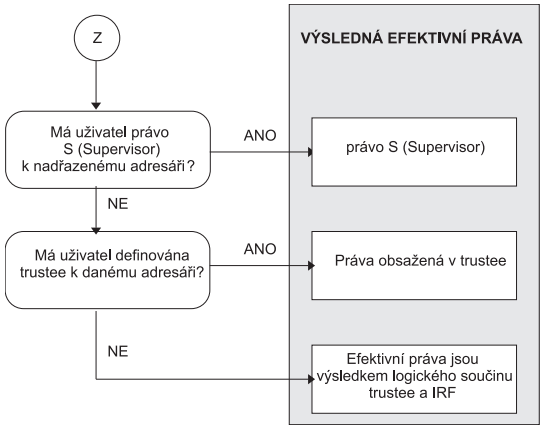
Konstrukce efektivních práv se řídí pravidly podle obrázku.

Při konstrukci práv se setkáme s termínem **logický součin**, jehož pravidla vysvětlíme na příkladu. Má-li složka masku *IRF* složenou z dílčích práv [SRWCEFA] a zděděná *trustee* jsou [RMF], jsou efektivní práva výsledkem logického součinu:

IRF adresáře	S	R	W	C	E		F	A
Trustee nadřazeného adresáře		R				M	F	
Effective Rights		R					F	

Vidíme, že efektivními zůstanou jen ta práva, která se vyskytnou ***současně*** v *IRF* a v *Trustee*.

Nejlépe práci se souborovými právy pochopíme na příkladu, který ukazuje další obrázek. V pravé části vidíme několik objektů databáze eDirectory, v levé strukturu složek na disku *DATA* serveru *ORDAS*. Je zde použito více způsobů přidělování práv:



Obrázek 5.19: *Výpočet efektivních práv*

- Objekt databáze eDirectory *GROUP TECHNICS* (skupina), jejímiž členy jsou oba uživatelé Vasek a Jan, má přiděleno trustee [RF] k objektu *VOLUME*. Pokud nebude stanoveno jinak (jiným trustee či IRF), členové této skupiny budou toto právo dědit na celém disku *DATA*.
- Objekt *ORGANIZATION UNIT Technici* má přidělena trustee [RWCEMF] ke složce *Data*. Tato trustee přecházejí také na objekty uvnitř kontejneru, tedy na uživatele *Vasek* a *Jan*.
- Každá složka má přidělenu masku IRF. Ta implicitně obsahuje všechna práva, na našem obrázku jsou IRF omezena pouze u složky *Obrazky*.

Nyní si ukážeme, jak vzniknou efektivní (skutečná) práva obou uživatelů (objektů USER) Vasek a Jan. Začneme uživatelem Vasek.

Tabulka 5.7: Efektivní práva uživatele Vasek

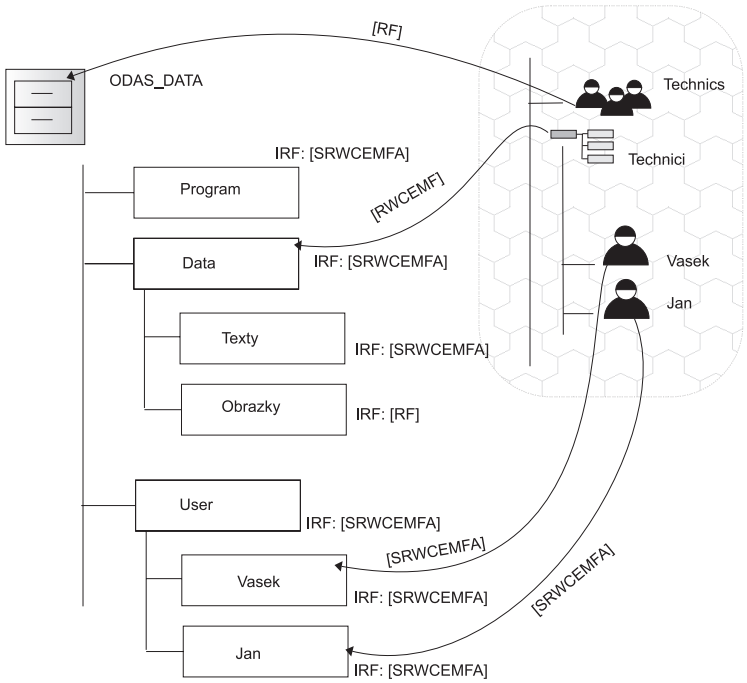
složka	Efektivní právo	Postup při výpočtu
Program	**[RF]**	Vasek je členem skupiny TECHNICS, která má přidělena trustee k disku ORDAS_DATA. Tato práva se zdědí na složku Program (logickým součinem vyjde výsledné právo).
Data	**[RWCEMF]**	Sem má Vasek přiděleno trustee objekt OU=Technici. Protože Vasek je umístěn v tomto kontejneru, přecházejí trustee i na něho.
Texty	**[RWCEMF]**	Tato práva Vasek dědí z nadřízené složky logickým součinem.
Obrazky	**[RF]**	Zde jsou práva také děděna, ale maska (filtr) práv IRF je omezen pouze na právo RF. Výsledkem logického součinu je omezení práv díky IRF.
User	**[RF]**	Vasek je členem skupiny Technics, která má přidělena trustee k disku ORDAS_DATA. Tato práva se zdědí na složku User. (Logickým součinem vyjde výsledné právo.)
Vasek	**[SRWCEMFA]**	Má úplná práva díky trustee [SRWCEMFA].
Jan	**[RF]**	Vasek je členem skupiny Technics, která má přidělena trustee k disku ORDAS_DATA. Tato práva se zdědí na složku User a odsud na složku JAN (logickým součinem vyjde výsledné právo).

Uživatel Jan má většinu efektivních práv stejných jako Vasek (vždyť oba jsou členy stejné skupiny a stejného kontejneru). Jediná odlišnost je u složek (přesněji podsložek složky *User*):

- složka *Vasek* – zde má Jan Právo [RF]
- složka *Jan* – efektivní práva Jana jsou [SRWCEMFA]

Tip: Pokud má některý uživatel potíže se spouštěním programu, zkuste se přihlásit jako administrátor a tento program spustit. Často je příčinou takovýchto problémů omezení práv. Spouštěný program si nemůže ve složce založit dočasný soubor, nebo nemůže v jiné složce otevřít pomocný program apod.

Pro práva k souborům platí stejná metodika, pouze dědění vychází z práv složky, v níž jsou programy umístěny.



Obrázek 5.20: *Příklad přidělení přístupových práv*

Atributy (attributes) složek a souborů

Kromě přístupových práv můžeme při zabezpečování souborů a složek využít také atributů, které přístupová práva doplňují o další možnosti. Ty se týkají spíše funkčnosti a vlastností složek. Většinu z nich ukazuje tabulka:

Tabulka 5.8: Atributy souborů a složek

Název	zkratka	Význam pro adresáře	Význam pro soubory
Archive Needed	**A**		Informuje o tom, že soubor byl od poslední archivace změněn
Can't Compress	**Cc**		Soubor nebude komprimován, úspora místa by byla malá
Compressed	**Co**		Soubor je zkomprimován
Don't Compress	**Dc**	Soubory v adresáři nebudou komprimovány	Zabraňuje komprimaci souboru
Delete Inhibit	**Di**	Zabraňuje smazání adresáře	Zabraňuje smazání souboru
Hidden	**H**	Adresář je neviditelný, nelze jej smazat a kopírovat	Soubor je neviditelný, nelze jej smazat a kopírovat
Immediate Compress	**Ic**	Zabezpečuje okamžitou komprimaci souborů v adresáři	Zabezpečuje okamžitou komprimaci souboru

Název	zkratka	Význam pro adresáře	Význam pro soubory
Purge Immediate	**P**	V okamžiku logického rušení je adresář a jeho soubory zrušen také fyzicky	V okamžiku logického rušení je soubor zrušen také fyzicky
Read Only	**Ro**		Soubor jen ke čtení, nelze jej rušit a modifikovat. Současně s Ro se nastavují atributy Di a Ri. Je opakem atributu Rw
Read/Write	**Rw**		Umožňuje modifikovat a mazat soubor. Opak atributu Ro
Rename Inhibit	**Ri**	Zabraňuje přejmenování adresáře	Zabraňuje přejmenování souboru
System	**Sy**	Způsobí neviditelnost adresáře, zabrání jeho mazání a kopírování	Způsobí neviditelnost souboru, zabrání jeho mazání a kopírování

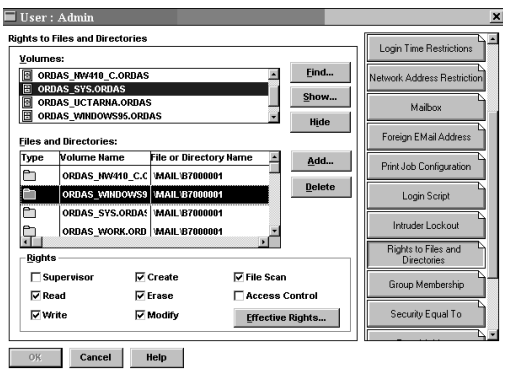
Atributy jsou „silnější“ než efektivní práva – mají tedy před nimi přednost. (Má-li uživatel efektivní právo pro zápis do souboru, ale soubor má nastaven atribut Ro – uživatel sem nic nezapíše.) Atributy může měnit administrátor a také uživatel s efektivním právem [M].

Práce s přístupovými právy a atributy

Podstatu práv i atributů již známe. V tomto odstavci si vysvětlíme jak práva přidělit. NetWare nabízí více způsobů (příkazy, programové utility např. příkaz *RIGHT*, nebo program *FILER*), my si vysvětlíme způsoby dva: Práci s NetWare Administrátorem – ta se používá při tvorbě uživatelů a práci s klientem sítě NetWare od firmy Novell. Ta je velmi jednoduchá a názorná.

Přístupová práva a NetWare Administrátor

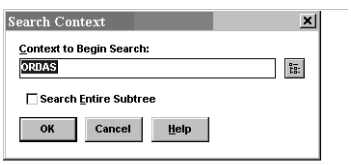
Práci s tímto programem již známe, umíme vytvořit nového uživatele. Mezi podstatné vlastnosti každého uživatele patří právě práva pro práci se složkami a soubory, schovaná pod tlačítkem *Rights to Files and Directories*. Po jeho stisku máme k dispozici obrazovku *Rights to Files and Directories*. V její horní části vidíme okno *Volumes*, v němž se zobrazují logické disky, a pod ním okno *Files a Directories*. Zde je seznam souborů a složek, k nimž máme definovaná přístupová práva. Umístíme-li kurzor na složku (soubor), vidíme dole naše práva (okno *Rights*).



Obrázek 5.21: *Přístupová práva k souborům a složkám*

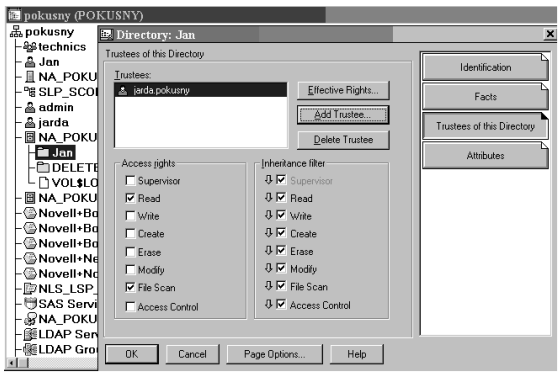
Pro práci s právy jsou k dispozici tato tlačítka:

- Stiskem **Find** budeme vyhledávat trustee vybraného uživatele. Nejdříve vyplníme okénko *Search Context*. Můžeme vybrat přímo disk a složku (pro listování je k dispozici tlačítko), snazší je zaškrtnout políčko *Search Entree Subtree*. Pak bude prohledáván celý strom, od vybraného kontextu dolů.
- Poklepnutím na **Show** se zobrazí vyhledávací okno. V něm vybereme logický disk, v jehož složkách chceme zjišťovat naše práva.
- Tlačítkem **Add** přidáváme trustee.
- **Delete** slouží k vymazání dříve přidělených pověřenců.
- Poklepáním na **Effective Rights** (úplně dole) budeme vyzváni k nalistování složky, k níž potřebujeme zjistit efektivní práva.



Obrázek 5.22: *Vyhledávání kontextu*

V předešlé obrazovce jsme přidělovali „složku uživateli“. Další možností je přidělení práv trustee přímo konkrétní složce. Složku si najdeme ve stromu databáze eDirectory (nejdříve rozbalíme příslušný kontejnerový objekt *VOLUME*). Klepnutím pravým tlačítkem myši na složku se dostaneme k oknu vlastností složky a stiskneme tlačítko *Trustee of this Directory*. V okénku *Trustees* vidíme uživatele, kteří mají ke složce přidělena práva trustee. V levé části (*Access rights*) můžeme měnit trustee, v pravé části (*Inheritance filter*) definujeme filtr (masku) práv složky. Tlačítkem *Effective Rights…* zjistíme efektivní práva uživatele ke složce, tlačítko *Add Trustee…* slouží k přidání práv dalších uživatelů. Posledním tlačítkem *Delete Trustee…* mažeme dříve zadaná práva.



Obrázek 5.23: *Přidělení přístupového práva z pohledu složky (uživatel ke složce)*

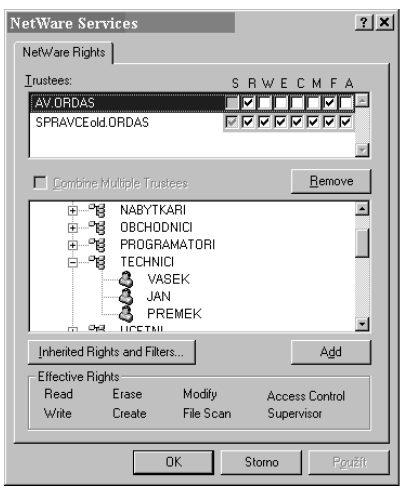
Poznámka: *Na obrázku si všimněte tlačítka Attributes, jehož stiskem uvidíme (a případně změníme) atributy souborů.*

Přístupová práva a Klient NetWare

Velmi intuitivní je práce s přístupovými právy přímo z klienta NetWare firmy Novell. Ve Windows se „proťukáme“ k disku serveru (*Volumes*), nebo konkrétní složce, klepneme na něj pravou tlačítkem myši a v menu zvolíme *Trustee Rights*.

V horní části okna vidíme *Trustee* ke složce, ve střední všechny objekty eDirectory, z nichž můžeme vytvořit pověřence ke složce. Tlačítkem *Remove* odebíráme Trustee složky, stiskem *Add* přidáme Trustee vybraného uživatele. Filtr práv upravíme pomocí tlačítka *Inherited Rights And Filters*.

Tip: Konstrukce práv není jednoduchá. Proto je vždy dobré přihlásit se jako konkrétní uživatel a nastavená práva vyzkoušet.



Obrázek 5.24: *Přístupová práva z klienta*

Složková a souborová práva přiřazovaná při instalaci NetWare

Při instalaci síťového operačního systému jsou některým složkám a objektům eDirectory přiřazena práva automaticky:

- Kontejnerovému objektu VOLUME se jménem SYS:PUBLIC jsou přiřazena složková práva *Read* a *File Scan*. Všichni uživatelé pak mohou spouštět soubory ve složce PUBLIC.
- Při vytváření je možné založit objektu *User* vlastní složku. *User* získá ke své složce automaticky všechna přístupová práva (dostane tedy *Trustee* [SRWCEMFA]). Domovskou složku uživatele vytvoříme zaškrtnutím políčka *Create Home Directory* při vytváření uživatele (viz obrázek v kapitole *Vytvoření nového uživatelského účtu*).

Přístupová práva k objektům

V databázi eDirectory je možné přidělovat práva, která definují možnosti práce jednotlivých objektů s jinými objekty. Je tak možné chránit objekty a služby databáze eDirectory. Přístupová práva k objektům pracují podobně jako přístupová práva k souborům a složkám, ale jde o odlišný zabezpečovací systém a obě služby přidělují práva k něčemu jinému! (Databáze eDirectory je něco jiného než souborová struktura disku – přestože je každý disk zastoupen v eDirectory objektem *VOLUME*.)

Pomocí tohoto zabezpečení můžeme například objektu *User* přidělit práva k práci s kontejnerovým objektem, čímž se tento *User* stane správcem ostatních objektů v kontejneru.

Analogie se složkovými a souborovými právy spočívá v metodice, opět můžeme objektu přidělit právo *Trustee*, nebo se právo zdědí z nadřazeného kontejneru. Dědění je možné ovlivňovat maskou (filtrem), podobně jako u zabezpečení složek. (Ale ještě jednou zdůrazňuji, že jde o práva k objektům, ne ke složkám.)

Druhy práv

U objektů rozeznáváme dva druhy přístupových práv:

- **Práva k objektům (object rights)**
- **Práva k vlastnostem objektů (properties rights).** Každý objekt má velké množství vlastností, jejichž popis se vymyká rozsahu naší knihy. Přesto se alespoň o základních pravidlech práce s přístupovými právy vlastností zmíním: Práva k vlastnostem se dají přidělit každé vlastnosti zvlášť, nebo všem vlastnostem najednou (je tedy možné použít dva způsoby definice *properties rights*). Právo ke všem vlastnostem nazýváme *APR (All Properties Rights).*

Možná práva ukazují následující tabulky.

Tabulka 5.9: Přístupová práva k objektům

Název	Zkratka	Význam
Supervisor	**S**	Poskytuje všechna práva k objektu a zároveň i všechna práva k vlastnostem objektu. Na rozdíl od složkových práv je u objektových práv možné právo S zablokovat filtrem děděných práv
Browse	**B**	Umožňuje vidět daný objekt ve stromu eDirectory
Create	**C**	Dá se přiřadit pouze kontejnerovým objektům. Dovoluje vytvářet nové objekty v kontejneru
Delete	**D**	Umožňuje zrušit objekt. Pokud budeme rušit kontejnerový objekt, musíme nejdříve zrušit jeho obsah. (Zrušit můžeme jen prázdný kontejner.)
Rename	**R**	Povoluje přejmenovat objekt
Inheritable	**I**	Zajišťuje dědění práv ke kontejneru i na objekty v kontejneru. (Právo I se dá použít jen na kontejnerové objekty.) Dá se aplikovat i na jednotlivé vlastnosti objektů, nebo na APR (všechny vlastnosti najednou)

Tabulka 5.10: Přístupová práva k vlastnostem objektů

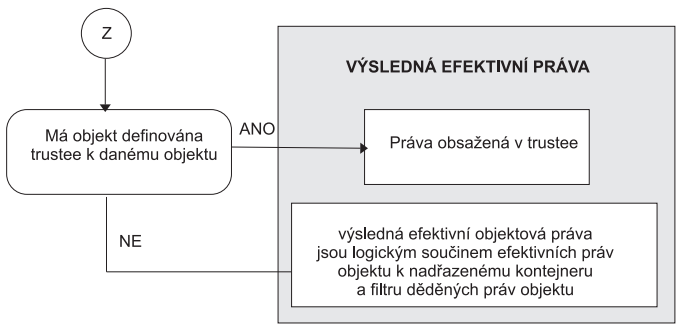
Název	Zkratka	Význam
Supervisor	**S**	Poskytuje všechna práva k vlastnosti. Právo S může být blokováno filtrem děděných práv.
Compare	**C**	Umožňuje porovnávat hodnotu vlastnosti se zadanou hodnotou. Výsledkem je buď shoda obou hodnot – True, nebo neshoda – False. (Pro přečtení hodnoty vlastnosti musíme disponovat právem R.)

Read	**R**	Umožňuje získat (přečíst) konkrétní hodnotu vlastnosti, zahrnuje v sobě i právo C.
Write	**W**	Dovoluje přidat, změnit nebo odstranit jakoukoliv hodnotu vlastnosti. Zahrnuje v sobě i právo A.
Add or Delete Self	**A**	Umožňuje pověřenci přidat nebo rušit jen tu hodnotu vlastnosti, která představuje jeho samého. Jiná změna není dovolena. (Pověřenec může např. manipulovat svým členstvím ve skupině.)

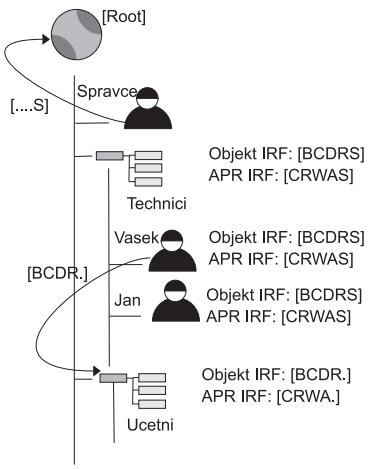
Vyhodnocování práv

Je v principu shodné s již dříve vysvětlenými právy k souborům a složkám (kapitola *Effective Rights*):

- Máme k dispozici *trustee* (*pověřence*) – každému objektu můžeme práva k manipulaci s jiným objektem přímo stanovit.
- Funguje dědění práv – každý objekt má masku (filtr) práv *IRF*. Jeden objekt však může obsahovat více práv trustee i filtrů IRF: Jedna dvojice (*trustee*, *IRF*) se vztahuje k objektovým právům, další k sumě všech vlastností APR, další může být definována pro každou vlastnost zvlášť.
- Výsledná efektivní práva vznikají logickým součinem. Jeho pravidla jsou poněkud odlišná od souborových práv. Systém nejdříve zjistí jaká efektivní práva má daný objekt k nadřazenému kontejneru. Pak teprve provede logický součin těchto práv s filtrem *IRF* objektu.
- Jednoduchý příklad práce s objektovými právy vidíme na dalším obrázku. Uživatel *Spravce* má přiděleno objektové právo *trustee S* k objektu [Root] – je tedy administrátorem. Může libovolně manipulovat s kontejnerovým objektem *Technici* i se všemi koncovými objekty v kontejneru. Odlišná je však situace pro kontejnerový objekt *Ucetni*, kde je filtrem práv IRF omezeno právo *S*. Zde se objektové právo *S* nebude dědit a objekt *Spravce* zde není administrátorem. Jeho funkci přebírá objekt *Vasek*, jemuž objektová trustee dávají maximální práva pro práci s kontejnerem *Ucetni*.



Obrázek 5.25: *Výpočet objektových práv*



Obrázek 5.26: *Příklad práce s objektovými právy*

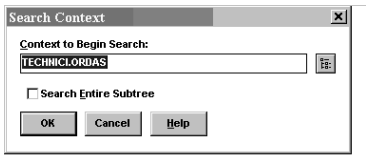
Objektová práva a NetWare Administrátor

K přidělování objektových práv používáme opět program NetWare Administrátor. Vybereme objekt, klepneme na něj pravým tlačítkem myši. V menu pak máme k dispozici dvě volby pro práci s objektovými právy:

- *Trustees of this Object*, (Pověřenci tohoto objektu) pokud chceme přidělovat, či zjišťovat práva k tomuto objektu
- *Rights to Other Objects* (Práva k ostatním objektům)

Rights to Other Objects

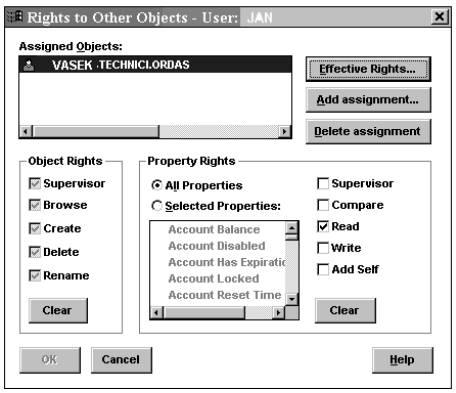
Pokud budeme pracovat s právy k ostatním objektům, objeví se nejdříve vyhledávací obrazovka, v níž zadáme objekt, s jehož právy budeme pracovat (pokud neznáme přesný kontext, můžeme hledat i v podstromu – políčko *Search Entire Subtree*).



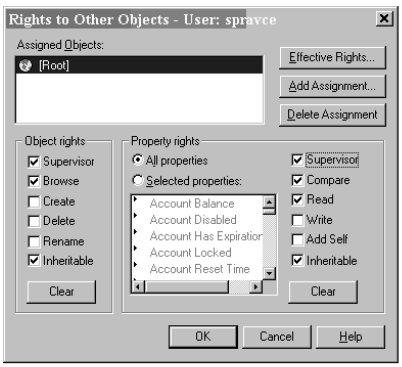
Obrázek 5.27: *Hledání objektu*

V podstatě zjišťujeme práva objektu k ostatním objektům. První objektem je ten, na něhož jsme klepli pravým tlačítkem myši (jeho jméno je napsáno v záhlaví okna), druhý objekt vidíme v okně *Assigned object* (to je ten hledaný). Objektová práva jsou zobrazena, případně je měníme v části *Object Rights*, právům k vlastnostem je vyhrazena pravá část obrazovky *Property Rights*.

Význam tlačítek je stejný jako v předešlých obrazovkách. *Effective Rights* slouží k výpisu efektivních práv k jinému objektu, *Add assignment* přidává a *Delete assignment* ruší přidělení objektových práv.



Obrázek 5.28: *Objektová práva objektu JAN k ostatním objektům*

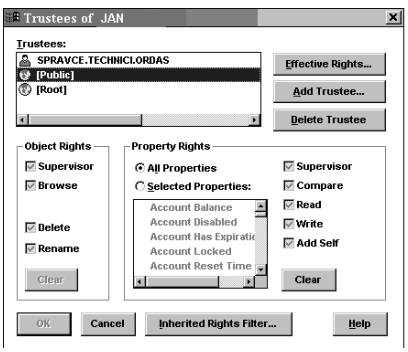


Obrázek 5.29: *Přidělení práva S uživatele Spravce k objektu [Root]*

Praktickým příkladem práce s objektovými právy je tvorba „záložního administrátora“. Již víme, že automaticky vytvářeného uživatele *Admin* můžeme omylem vymazat. Tím však ztratíme administrátorský účet a s ním i možnost administrace sítě. Účet náhradního *Admina* založíme snadno, stačí vytvořit libovolný účet a přidělit mu objektové právo *S* k objektu [Root]. Díky dědění práv pak máme právo *S* na celý strom (pokud si ho sami někde neomezíme odebráním práva *S* ve filtru práv IRF).

Trustees of this Object

Zde pracujeme s trustee k objektu, na něhož jsme klepli pravým tlačítkem myši. Obrazovka je velmi podobná předešlé. Jediný rozdíl je v okénku *Trustees* – zde vidíme pověřence objektu.



Obrázek 5.30: *Objektová práva k objektu JAN*

Objektová práva přiřazovaná při instalaci NetWare

Při instalaci systému se přidělují některá práva, potřebná pro vlastní práci systému:

- Objektu typu *User* se jménem **Admin** je přiděleno právo S k objektu [*Root*]. Díky dědění práv má pak Admin práva ke všem dalším objektům eDirectory (jak víme, [*Root*] je objektem nejvyšším).
- Objekt **[Root]** dostává přiděleno právo *Browse* ke všem objektům typu *User*.
- Objekt **[Public]** dostává přiřazeno právo *Browse* k objektu [*Root*]. Díky tomu vidí všichni uživatelé sítě všechny objekty databáze eDirectory. Pokud nechceme, aby tomu tak bylo, je účelné tuto výsadu zrušit a právo *Browse* delegovat pouze na některé kontejnery.

Ekvivalence práv (security equivalence)

Je prostředek, který zajistí přidělení stejných práv jednoho objektu *User* jinému objektu *User* (platí pouze pro objekty typu *User*). Praktické nastavení se provádí z NetWare Administratora, tlačítkem *Security Equal to Me* v identifikační obrazovce uživatele (viz kapitola *Vytvoření nového uživatelského účtu).*

Ekvivalence práv platí a je funkční po dobu životnosti obou objektů User. Nehodí se proto pro tvorbu náhradního Administrátora (smazáním původního uživatele Admin zanikne rovněž ekvivalence práv náhradního Administrátora).

Některé ekvivalence se přidělují automaticky. Každý objekt typu *User* má přidělenu ekvivalenci s objektem [*Public*] a zároveň ekvivalenci s nadřazeným kontejnerovým objektem.

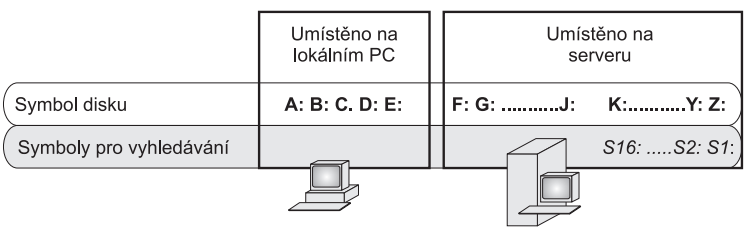
Mapování

Na serveru bývá uloženo velké množství dat, která jsou seřazena do mnoha složek a podsložek. Orientace na discích serverů je pak obtížná. A tak se také v sítích NetWare využívá mapování. Princip je stejný jako u ostatních sítí: logickým jménem disku, které momentálně nevyužíváme, nahradíme cestu ke složce síťového disku.

NetWare používá ještě další mapovací prostředek – mapování pro vyhledávání (*Search drive mapping*). Opět je celá cesta k síťovému disku nahrazena zástupným znakem. Pokud uživatel zadá příkaz ke spuštění programu, začne *Search drive mapping* prohledávat „svoje“ disky (tj. disky zařazené do vyhledávacího mapování). Tím je zajištěno automatické spouštění programů z určitých složek (zařazených do *Search drive mapping*).

Pravidla pro přidělování symbolů disků

Přidělování disků se řídí přirozenými pravidly. Část symbolů ze začátku abecedy je použita pro lokální disky (na počítači, z něhož přistupujeme k síti): *A:* a *B*: pro disketové mechaniky *C:, D:, E:* pro pevné disky a mechaniky CD-ROM. Zbytek symbolů se používá pro mapování. U sítí Novell je disk *F:* zpravidla diskem systémovým – je na něj mapován systémový disk SYS. Další jména jsou již závislá na volbě správce sítě.



Obrázek 5.31: *Přidělování mapovacích symbolů*

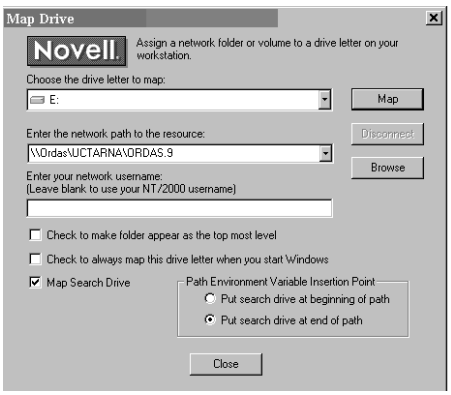
Zvláštními pravidly se řídí přidělování jmen diskům pro vyhledávání. Vyhledávací disk začíná vždy písmenem *S,* které je doplněno číslicí. Celkem máme k dispozici šestnáct vyhledávacích disků *S1:* až *S16:*. Jejich jména jsou přidělována mapovacím diskům od konce. Disku Z: odpovídá search disk *S1:*, disku *Y:* search disk *S2:* atd. Automatické prohledávání složek probíhá od disku *S1:* k disku *S16:*.

NetWare přiděluje jméno *S1* složce *SYS:PUBLIC*, čímž je zajištěno snadné spouštění všech příkazů a utilit programu (bez nutnosti zadávat cestu).

Možnosti přidělení mapovacího symbolu

Vlastní přidělení jména disku určité složce lze v principu provést dvěma způsoby:

- Umístit příkaz MAP do login scriptu. Login script je soubor, který se automaticky spouští při přihlášení uživatele do sítě. Popis login scriptů je poměrně rozsáhlý a v této knize není obsažen.
- Velmi snadné je přidělení mapování s pomocí klienta. Vybereme si složku, kterou chceme mapovat (*Průzkumníkem* či prostřednictvím ikony *Okolní počítače*, *Místa v síti*). Klepneme na ni pravým tlačítkem myši a vybereme položku *Novell Map Network Drive…*



Obrázek 5.32: *Přidělení mapování*

Mapování pomocí klienta NetWare

Výběr položky *Novell Map Network Drive…* zobrazí okno *Map Drive*. V něm máme k dispozici všechny varianty definice mapování:

- V prvním řádku (*Choose the drive…*) vybíráme logický disk (písmeno), jemuž bude mapování přiřazeno.
- V druhém řádku (*Enter the network path..*) je UNC, nebo NetWare formát zápisu cesty k mapované složce. (formát UNC již známe, formát NetWare používá zápis ve tvaru: *server\volume:\directory\subdirectory)*. Cesta se automaticky zapíše ke složce, na níž jsme klepli pravým tlačítkem myši. Tlačítkem *Browse* ji můžeme změnit.
- Použijeme-li klienta k mapování, které bude popisovat cestu ke složce na serveru Windows, musíme do třetího řádku (*Enter your network username)* zapsat jméno, kterým se na server Windows přihlašujeme. (Tento řádek má smysl v síti, v níž jsou společně umístěny servery NetWare a Windows.)
- Význam zaškrtávacího políčka *Check your folder…* je následující: jeho vyplněním se příslušná složka bude uživateli jevit jako nejvyšší složka ve stromové struktuře. Uživatel tedy neuvidí žádnou složku umístěnou nad ní. Vytvoříme tak fiktivní kořenovou složku.
- Zaškrtnutí druhého políčka *Check to always …* zajistí automatické obnovení mapování při startu Windows.
- Vyplněním posledního políčka *Map Search Drive* přiřadíme mapovacímu symbolu ještě symbol vyhledávacího disku.
- Mapování ukončíme tlačítkem *Map*. Tlačítkem *Disconnect* můžeme mapování zrušit.

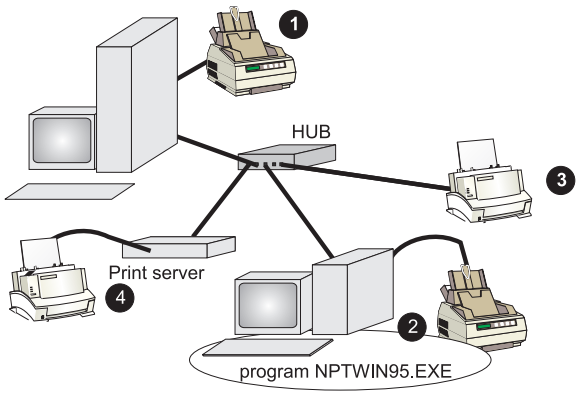
Síťové tisky

Zprostředkování tisku z více stanic na jednu sítovou tiskárnu je další častou službou sítí. U malých sítí peer to peer se používá připojení tiskárny k některé za stanic. Ve větších sítích existuje více možností (již jsme se s nimi seznámili v kapitole o Windows Serveru):

1. Připojení tiskárny přímo k serveru je nejjednodušším prostředkem. Problém je v tom, že server bývá umístěn odděleně a přístup k tiskárně je obtížný.
2. Další možností je připojení tiskárny k některé ze stanic. Pak je nutné nahrát na stanici program pro zprostředkování tisků. Pro operační systémy Windows 9.x je to program NPTWIN95.EXE.
3. Mnoho tiskáren je dnes vybaveno síťovou kartou, což umožňuje připojit tiskárnu přímo ke kabeláži.

4. Poslední možností je použití hardwarového tiskového serveru. Je to „krabička“, která má zdířku pro připojení k síti a několik zdířek na připojení tiskáren. V podstatě jde o zprostředkované připojení tiskáren (hardwarovým serverem) přímo ke kabeláži.

U dražších tiskáren určených k síťovým tiskům bývá možnost 3 a 4 sloučena. Taková tiskárna má vlastní síťovou kartu, a navíc vlastní tiskový server. Po připojení ke kabeláži je schopná nabízet své služby stanicím v síti.



Obrázek 5.33: *Možné připojení tiskáren*

NetWare nabízí dva způsoby zprostředkování tisku:

- *Klasický*, který používaly i předešlé verze operačního systému. Je kompatibilní se všemi tiskárnami, dnes je stále hodně rozšířen a my si jej také vysvětlíme podrobněji.
- *NDPS – Novell Distributed print services* je novinkou, nabízenou od NetWare 5, o níž se zmíním spíše informativně.

Klasický způsob tisku

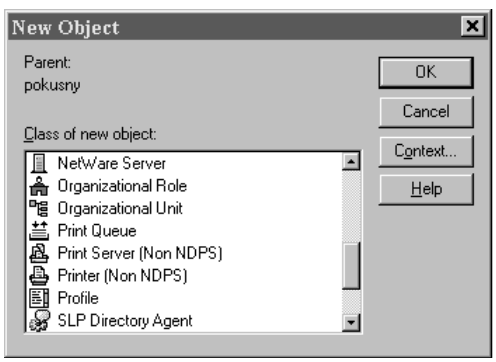
Při této činnosti se pro jednotlivé fáze tisku používá následující terminologie: Tiskové úlohy ze síťových stanic (to, co se má tisknout) nazýváme tiskovými joby. Joby jsou posílány do tiskových front. Tisková fronta je v podstatě složka na síťovém disku serveru, v níž se joby shromažďují. Pokud se sejde více jobů současně, seřadí se ve složce do fronty a na tiskárnu putují postupně, jeden za druhým. Obsluhu front a jobů provádí program (NLM modul), který se jmenuje *Print server*.

Na jednom serveru NetWare může být spuštěno několik programů *Print server* (ale každý bude mít vlastní jméno), může existovat více front a více tiskáren. Pro praxi je nejpřehlednější přiřadit jedné frontě jednu tiskárnu.

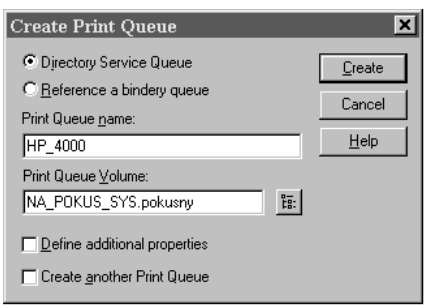
Vytvoření tiskového prostředí

K tisku je potřeba aktivovat tři typy objektů eDirectory: tiskový server (*Print Server*), tiskovou frontu (*Print Queue*) a tiskárnu (*Printer*). Na pořadí vytváření objektů nezáleží, ale mezi objekty je nutné zadat správné vazby (*assignments*).

Tiskové objekty (stejně jako jiné) umísťujeme do kontejnerů. Vybereme tedy kontejner, klepneme na něj pravým tlačítkem myši a zvolíme *Create*. Otevře se nabídka objektů, z níž si vybíráme:



Obrázek 5.34: *Objekty databáze NDS*

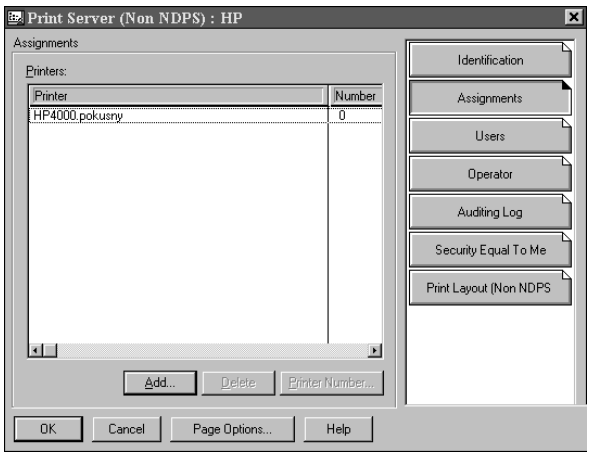


Obrázek 5.35: *Tvorba tiskové fronty*

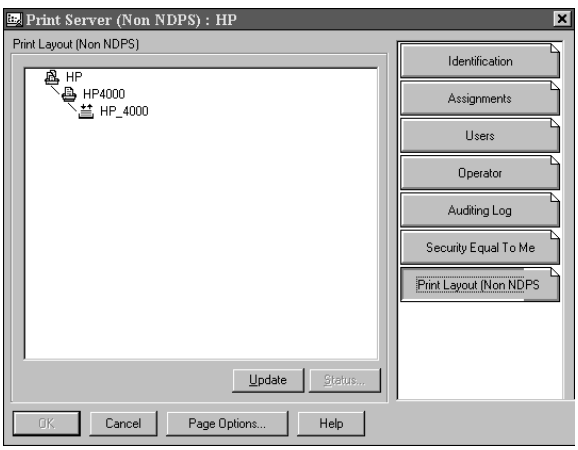
Začneme například tiskovým serverem – objektem *Print Server Non NDPS*. Po výběru objektu zapíšeme do řádku *Print Server name* jméno serveru (v našem příkladu to bude *HP*).

Dále vytvoříme tiskovou frontu – vybereme objekt *Print Queue*. Na obrazovce *Create Print Queue* vyplníme jméno tiskové fronty a jméno disku, na němž bude fronta uložena (*Print Queue Volume*). Pro zadání jména disku samozřejmě použijeme tlačítko. Na našem obrázku vidíme tvorbu fronty HP_4000, umístěné na disku *SYS* serveru *NA_POKUS*.

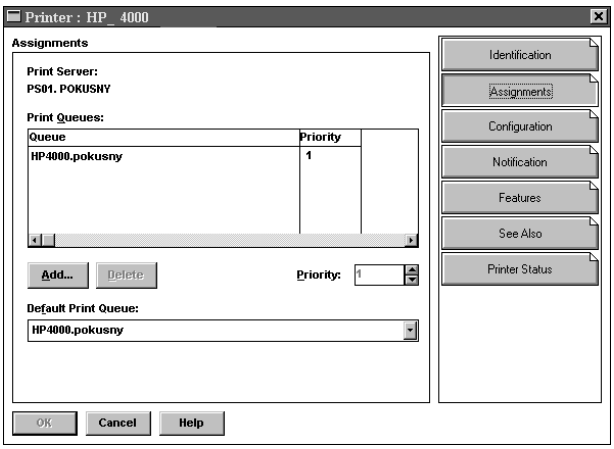
Potom vytvoříme tiskárnu – z nabídky objektů vybereme *Printer* (*Non NDPS*). Objeví se okno *Create Printer*, do něhož zapíšeme jméno tiskárny, současně zaškrtneme políčko *Define additional properties*, což nám dovolí definovat další vlastnosti tiskárny. V okně vlastností tiskárny stiskneme tlačítko *Assignments*.



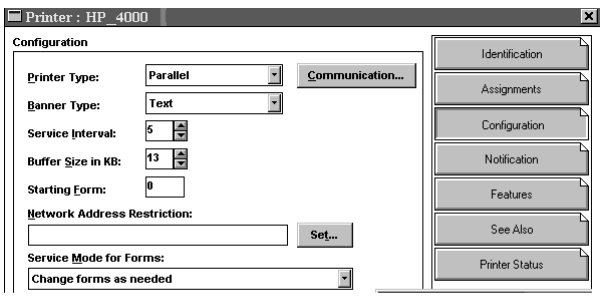
Obrázek 5.36: *Přiřazení tiskárny HP_4000 tiskovému serveru HP*



Obrázek 5.38: *Vazba mezi serverem HP, frontou HP_4000 a tiskárnou HP4000*



Obrázek 5.37: *Přiřazení tiskové fronty HP4000 tiskárně HP_4000*



Obrázek 5.39: *Konfigurační obrazovka tiskárny*

V příslušném okně pak stiskneme tlačítko *ADD*. Vyvoláme tak seznam tiskových front. K jedné z nich tiskárnu připojíme. Dále je důležitá obrazovka *Configuration* (vyvolaná příslušným tlačítkem). V ní především definujeme, ke kterému portu počítače je tiskárna připojena – řádek *Printer Type*.

Nyní máme vytvořeny vazby mezi frontou a tiskárnou, k nim je třeba doplnit vazbu na server. Klepneme pravým tlačítkem myši na objektu *Print server*, stiskneme tlačítko *Assignments*. Na příslušné obrazovce stiskneme tlačítko *ADD* a přidáme tiskárnu. Nastavení vazeb mezi objekty tisku si zkontrolujeme tlačítkem *Print Layout…*

V konfigurační obrazovce print serveru i tiskové fronty máme k dispozici tlačítka *Users* a *Operator*. S jejich pomocí můžeme měnit objektová práva k objektům *Print Server* a *Print Queue*. Tlačítkem *Users* zadáváme uživatele tiskového prostředí a *Operator* přidělí k objektům uživatele s vyššími právy (mohou například mazat tiskové joby). Na obrazovce tiskové fronty je rovněž důležité tlačítko *Job List*. Po jeho stisku uvidíme tiskové joby ve frontě. (Připomínám, že konfigurační obrazovky objektů vyvoláme stiskem pravého tlačítka myši a volbou *Details*.)

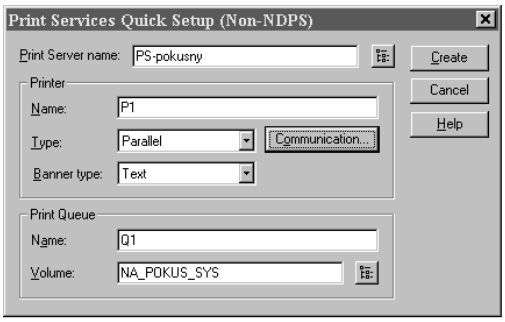
Rychlé nastavení tisků

Nastavení tisků je možné zjednodušit. V programu NetWare Administrátor máme v menu *Tools* k dispozici volbu *Quick setup*. (Před jejím použitím musíme umístit kurzor na kontejner, v němž budeme tiskové prostředí vytvářet.) Na jedné obrazovce vytvoříme print server, tiskovou frontu, tiskárnu a jejich vzájemné vazby. Jestliže však bude mít naše tiskové prostředí více tiskových objektů (např. front a tiskáren), budeme muset dokonfigurovat nastavení ručně.

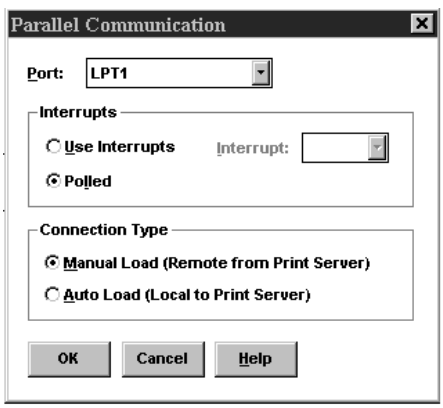
Nastavení při jiném připojení tiskáren

Výše popsaný způsob definice tisků platí pro tiskárnu připojenou přímo k serveru. U zbylých způsobů připojení dochází pouze k malým odchylkám:

- Tiskárnu připojenou do sítě vlastní síťovou kartou přiřadíme k tiskové frontě.
- Součástí dodávky hardwarového tiskového serveru (jehož prostřednictvím je tiskárna připojená do sítě) bývá software, který vytvoří vlastní tiskové prostředí na serveru NetWare. Bývá tedy vytvořen vlastní tiskový server, fronta i tiskárna.
- Je-li sdílená tiskárna připojena k některé ze síťových stanic, je nutné mít na této stanici spuštěn program NPTWIN95. Jinak je nastavení tisků standardní, s jedinou výjimkou: na obrazovce *Configuration* (objektu *Printer*) stiskneme tlačítko SET a na následné obrazovce musíme zaškrtnout políčko *Manual Load*.



Obrázek 5.40: *Quick Setup*



Obrázek 5.41: *Zadání tiskárny připojené prostřednictvím síťové stanice*

Aktivace tiskového prostředí

Tiskové prostředí je nutno aktivovat – musíme přímo na serveru načíst modul *PSERVER.NLM* (viz kapitola Základy systému NetWare). Přesná syntaxe příkazu je:

PSERVER [*kontext*] *jméno serveru*.

Pokud se objekt *Print server* nachází v jiném kontextu než objekt *Server*, musíme k němu zapsat cestu ve formě kontextu! Náš server HP je umístěn ve stejném kontextu jako server NA_POKUS, a tak spuštění tiskového modulu zajistí příkaz *PSERVER HP*.

Startovací příkaz tiskového prostředí se zapisuje do souboru AUTOEXEC.NCF. Zajistíme tak automatický start tiskového prostředí při startu operačního systému NetWare.

Tip: Nejdříve si funkčnost tisků vyzkoušíme. Nastartujeme tedy modul PSERVER z konzoly serveru a až po vyzkoušení zapíšeme příkaz do AUTOEXEC.NCF. Vyhneme se tak zbytečným restartům serveru.

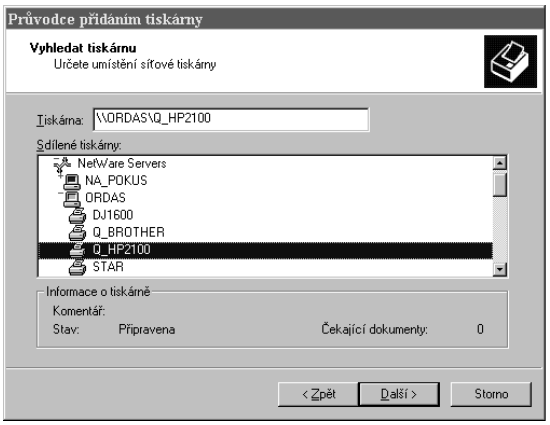
Jestliže tisk nefunguje, zkontrolujeme nejdříve vazby (tlačítko Assignments v obrazovkách jednotlivých objektů) a tlačítko Print Layout… na detailní obrazovce print serveru.

Instalace tiskárny na stanici

Nijak podstatně se neliší od instalace vysvětlené u sítí peer to peer (v kapitole *Přístup ke sdíleným tiskárnám*). Opět budeme instalovat *Síťovou tiskárnu*, při zadávání síťové cesty použijeme tlačítko *Procházet* a pak si vybereme novell-

ský server, na němž je nainstalována tisková fronta. Pokud server neuvidíme napoprvé, musíme si jej zpřístupnit poklepáním na ikonku *Celá síť*. Potom pouze vybereme příslušnou frontu.

Odlišně od instalace v síti peer to peer musíme instalovat ovladač tiskárny (buď přímo z Windows, nebo z instalačního CD tiskárny).



Obrázek 5.42: *Tiskové prostředí na NetWare serveru*

Tiskové služby NDPS

Jak jsem se již zmínil, jde o nový způsob práce tiskáren, zavedený až s verzí NetWare 5. U většiny sítí se setkáme spíše se starší variantou, nicméně alespoň základy NDPS a její architekturu se pokusím vysvětlit.

Tiskový agent (printer agents)

Jádrem tiskové služby NDPS je tiskový agent (printer agents). Každá tiskárna je reprezentována jedním agentem, jeden agent je právě pro jednu tiskárnu. Agent spojuje tiskárnu s klientem služeb NDPS a jsou v něm integrovány základní funkce klasických tiskových služeb: *print server, print queue, printer.*

Tiskový agent může být integrován přímo do tiskárny technologií NEST (Novell Embedded System Technology), nebo může být realizován softwarově, v podobě zaveditelného modulu NLM na serveru. V případě modulu NLM musí být tiskový agent doplněn branou (printer gateways), která jej propojí s konkrétní tiskárnou. Navíc musí být na serveru spuštěn NDPS manager.

NDPS Manager

Je zaveditelným modulem NLM (jeho jméno je NDPSM.NLM). Používá se tehdy, pokud jsou v paměti serveru načteni tiskoví agenti ve formě NLM modulů. Je určen k ovládání tiskových agentů.

Brány k tiskovým agentům (printer gateways)

Jde o další NLM modul, který je nutný pro tiskové agenty. Je rozhraním mezi programovým tiskovým agentem a skutečnou tiskárnou.

NDPS Broker

Je po tiskovém agentu dalším prvkem tiskových služeb. Musí být načten vždy (i v případě použití tiskové brány NEST). Je realizován modulem BROKER.NLM a zajišťuje tyto služby:

- *SRS (Service Registry Service)* – nabízení se tiskáren NDPS do sítě.
- *ENS (Event Notification Service)* – posílání zpráv o událostech na tiskárněuživatelům.
- *RMS (Resource Management Service)* – instaluje prostředky tiskových služeb do prostředí NDPS (centrálně na serveru). Ty pak může distribuovat klientským stanicím a tiskárnám. Jde například o ovladače tiskáren, fonty apod.

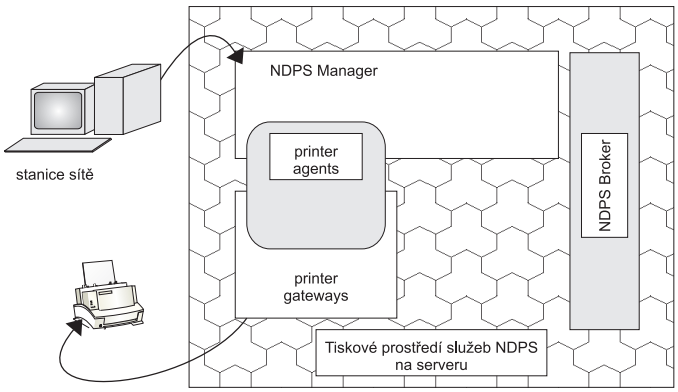
Tiskárny NDPS

Tiskárny, na něž prostřednictvím služeb NDPS tiskneme. Jak již víme, každá z nich musí mít svého agenta (printer agents). Do sítě mohou být připojeny těmito způsoby (viz obrázek *Možné připojení tiskáren*, v úvodu kapitoly o tiscích):

1. přímo k serveru
2. k některé ze stanic
3. přímo ke kabeláži sítě

Tiskárny mohou být **veřejně přístupné** – vidí je všichni v síti (dokonce i nepřihlášení k NetWare). V databázi eDirectory takováto tiskárna neexistuje, její správu provádíme z grafické utility NetWare Administrator, prostřednictvím nabídky *Tools* a volby *NDPS Public Access Printers*.

Další možností jsou **tiskárny s řízeným přístupem**. Ty lze chránit před neoprávněným použitím prostřednictvím objektových práv, protože v databázi eDirectory je každé tiskárně přiřazen objekt *NDPS Printer*.



Obrázek 5.43: *Architektura NDPS*

Instalace NDPS

Službu NDPS můžeme nainstalovat volitelně při vlastní instalaci systému, nebo kdykoliv později. (Použijeme k tomu zaveditelný NLM modul *NWCONFIG* a jeho volbu *Product Options*).

V databázi eDirectory přibudou objekty *NDPS Broker*, *NDPS Manager* a *NDPS Printer*. Do souboru AUTOEXEC.NCF je přidán spouštěcí řádek pro start modulu BROKER.NLM. V NetWare Administrátoru se menu *Tools* rozšíří o volby *Access Printer* (správa veřejně přístupných tiskáren) a *NDPS Remote Printer Management* (přidávání tiskáren pracovním stanicím uživatelů).

Pokud je tisková brána realizována softwarově, musíme načíst ještě její NLM moduly a spustit *NDPS Manager* (NDPSM.NLM).

Podporu NDPS je nutné nainstalovat rovněž na pracovní stanice sítě. Nejjednodušeji při instalaci klienta sítě Novell, nebo kdykoliv později přidáním služby od výrobce Novell. Přidání tiskárny NDPS na pracovní stanici uživatele provede správce prostřednictvím NetWare Administrátora (*Tools/NDPS Remote Printer Management)*.

Archivace a zálohování dat

Již jsem se zmínil o tom, že to nejdražší na celé síti není žádný hardware, ale data. Ačkoliv jsou servery konstruovány na trvalé zatížení, není nikdy možné vyloučit poruchu disku s daty. Zničení dat může být také výsledkem živelné katastrofy (např. požáru), nemůžeme vyloučit ani krádež serveru.

Proto jsou serverové operační systémy vybaveny službami pro zálohování dat. Zálohovacích systémů bývá samozřejmě více, v podstatě by se daly rozdělit takto:

- Zálohování vycházející z principů diskových polí RAID (viz podkapitola *Pevné disky* v kapitole *Server*). To zabezpečí data serveru před hardwarovou poruchou.
- Archivace na páskové jednotky, nahraje data na jiné, přenosné médium (pásku). Pásky se zpravidla střídají a je možné je ukládat odděleně od serveru. Tím jsou data chráněna před živelnou pohromou a krádeží.

  Poznámka: *V počítačové terminologii není mezi zálohováním a archivací činěn rozdíl. Já jej udělal pouze pro přehlednost knihy.*

Zrcadlení disků (Mirroring)

V serveru můžeme mít instalováno diskové pole s vlastní inteligencí. To provádí rozdělování a ochranu dat, nejčastěji podle metodiky RAID 1 nebo 5. Dnes je toto řešení standardně k dispozici také u malých serverů a v takovém

případě je určitě využijeme. Pokud nemáme k dispozici diskové pole vytvořené hardwarově, můžeme použít zrcadlení disků, které je součástí operačního systému NetWare. Principiálně jde o metodu RAID 1, obsah jednoho disku je v reálném čase kopírován na záložní disk. V případě poruchy systém automaticky pracuje se záložním diskem. Minimálně toto zabezpečení dat by mělo být realizováno na každém serveru!

Zrcadlení (mirroring) je možné nainstalovat a zprovoznit již při instalaci NetWare. Pokud však druhý disk dokoupíme později, je možné mirroring zapnout dodatečně. Zrcadlení je také možné kdykoliv vypnout a záložní disk připojit jako další datový svazek.

Pro správnou funkci zrcadlení musí platit, že záložní disk („zrcadlo“) je minimálně stejně velký jako disk zrcadlený. Menší být nemůže, protože by se na něj nevešel obsah originálu. Pokud by byl větší, bude zbylá část prostoru disku nevyužitá. Ideální je, když jsou zrcadleny dva stejné disky.

Práce při nastavování zrcadlení jsou velmi nebezpečné. Musíme definovat diskové oblasti a formátovat je. Přitom může velmi snadno dojít ke ztrátě dat. Proto se omezím pouze na příkazy spojené se stavem zrcadlení. Nebudu vysvětlovat ani zapnutí, ani rozpojení zrcadlených disků.

Stav zrcadlení

Stav zrcadlení nejjednodušeji zjistíme pomocí příkazu konzoly serveru MIRROR STATUS. Pokud právě probíhá prvotní sezrcadlení, ukáže procento rozpracovanosti.

Zrcadlení může být v některém z následujících stavů (což nám příkaz vypíše):

Tabulka 5.11: Stav zrcadlení vypsaný příkazem MIRROR STATUS

Being remirrored	Je v činnosti proces obnovy zrcadlení.
Fully synchronized	Plně zrcadlená.
Not mirrored	Nezrcadlená, zrcadlení není použito.
Orphaned state	Nezrcadlená, ale logické disky nebyly přejmenovány. Nemohou tedy být namontovány, dokud nebudou znovu zazrcadleny, přejmenovány nebo smazány (logické disky s těmito jmény jsou na druhém disku).
Out of synchronization	Nezrcadlená, vypadla ze zrcadlení a zrcadlení nemůže být obnoveno (např. chyba).

Archivace dat

Tato metoda spočívá v přenesení dat na jiné médium než standardní pevný disk. Výhodou je možnost archivace dat na jiném místě než PC. Data tak ochráníme před krádeží či živelnou pohromou.

Další nespornou výhodou archivace je možnost obnovy starších verzí souborů. Představme si, že přepíšeme obsah souboru a později zjistíme, že tato změna byla chybná a my se budeme chtít vrátit k předešlé verzi:

- Při zrcadlení je změna souboru okamžitě přenesena na druhý disk, takže starší verzi souboru nebudeme mít k dispozici.
- Máme-li však soubor archivován, obnovíme jej z archivačního média.

U serverů se jako archivační médium používá nejčastěji pásková jednotka. Pásky jsou vyjímatelné, běžně se v mechanice střídá několik pásek.

Obecné zásady archivace

K zálohování můžeme použít více druhů programů, nicméně existují obecná pravidla, která budeme vždy muset respektovat.

Typy archivace

Typ zálohování určuje, zda budou zálohována všechna data, nebo jen ta která se měnila. Základní tři způsoby zálohování ukazuje tabulka (stejné metody používá také Windows Server):

Tabulka 5.12: Typy zálohování

Typ zálohování	Co se zálohuje	Výhody	Nevýhody
Full backup (úplné zálohování)	Zálohují se všechny soubory.	Jednoduchost	Zálohují se i ty soubory, které se nemění. Následkem jsou velké objemy záložní kopie.
Differential backup (rozdílové zálohování)	Zálohuje jen ty soubory, které se změnily od provedení poslední úplné zálohy.	Úspora místa	Pro obnovení dat je potřeba také poslední záloha metody full backup.
Incremental backup (přírůstkové zálohování)	Zálohují se jen ty soubory, které se změnily od okamžiku provedení poslední (jakékoliv) zálohy.	Úspora místa	Pro obnovu dat je nutná poslední záloha full backup + všechny následující přírůstkové zálohy. Jestliže některá z těchto záloh bude nečitelná, nebude obnova dat možná!

Strategie archivace

Vybrat si typ zálohování je tedy na správci sítě, obecné doporučení se nedá definovat. Přesto se pokusím určitá pravidla uvést:

Je zbytečné zálohovat soubory, které máme na instalačních médiích a po havárii je budeme moci bez problémů nainstalovat. Zálohování bychom tedy měli soustředit pouze na data aplikací (ušetříme tak mnoho místa na záložním médiu).

Pokud je kapacita média (pásky) stejná (nebo větší) než kapacita zálohovaných dat, je zálohovací strategie jednoduchá – data nahrajeme pouze na jednu pásku, metodou *Full backup*. Pásky pak budeme pravidelně střídat. Např. jednu pro pondělí, další v úterý atd. Vhodné je rezervovat další pásky pro měsíční nebo roční zálohy. Cena pásek není vysoká, a tak pořízení cca 10 pásek není problémem.

Je-li kapacita zálohovaných dat větší než kapacita pásky, musíme pro jednu zálohu použít několik pásek. Zde se již budeme muset zamyslet nad úsporou místa na zálohovaném médiu, metodu *Full backup* doplnit některou z dalších, úspornějších. Musíme však mít vždy na mysli nutnost obnovy dat. V případě kombinace úplného zálohování s ostatními metodami budeme při obnově dat potřebovat více pásek (první s úplnou zálohou) a ostatní podle zvolené strategie. Čím více pásek použijeme tím vyšší je riziko toho, že některá páska bude nečitelná. Nečitelnost jediné pásky pak znemožní obnovu všech dat! Pro takovéto zálohování existuje několik metodik, jednu z možných ukazuje tabulka:

Tabulka 5.13: Možný koloběh pásek

týden	Způsob zálohování
1	Po – páska 1, Út – Ne páska 2
2	Po – páska 3, Út – Ne páska 4
3	Po – páska 5, Út – Ne páska 2
4	Po – páska 6, Út – Ne páska 4

Vidíme, že na zálohu postačuje jen 6 pásek, záloha dovoluje obnovu dat 2 týdny starých. Celou strategii je dobré doplnit ještě o měsíční zálohu.

Poznámka:

V příkladu jsem použil 7denní pracovní týden. Jestliže firma nepracuje v sobotu a v neděli, je samozřejmě záloha dat z těchto dní zbytečná.

Časové požadavky na zálohování

Zálohovat bychom měli vždy v době, kdy se se zálohovanými daty nepracuje. Pokud bychom totiž začali kopírovat otevřený soubor, nemusí se zálohování podařit a případná obnova dat nebude možná (což neplatí pro zálohovacího agenta TSA600 – viz dále).

Nejjistější je provádět zálohování mimo pracovní dobu (např. v noci). Zálohovací programy mají plánovače, v nichž je možné nastavit začátek zálohování. Při volbě začátku zálohování musíme pamatovat také na to, že pásková jednotka je pomalým zařízením a vlastní zálohování může trvat velmi dlouho. Spuštění zálohy musíme načasovat na tu dobu, kdy už nebude určitě nikdo pracovat (např. v 1 hod v noci), ale zároveň musí celé zálohování proběhnout do té doby, než začne pracovat první uživatel (např. 6 ráno).

Shrnutí

Pro bezpečné zálohování tedy musíme:

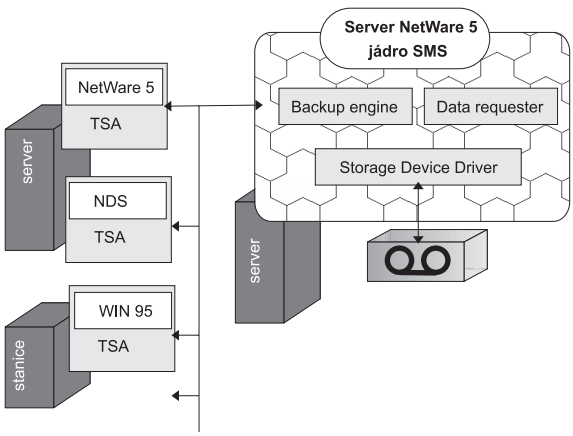
- stanovit metodu zálohování a koloběh pásek,
- zajistit ukládání pásek se záložními daty odděleně od serveru, nejlépe v jiné budově, trezoru apod.,
- spouštět zálohování v době, kdy nikdo nepracuje. Zálohovací agent NetWare 6, který se jmenuje TSA600 (viz dále), umí zálohovat (na rozdíl od svých předchůdců) také otevřené soubory. Umožňuje to nová vlastnost souborového systému NSS – *File Snapshot* snímek souborů. Jejím prostřednictvím udržuje operační systém kopie všech otevřených souborů, takže může provést jejich zálohování. Díky snímkům souborů odpadá starost se zálohováním momentálně otevřených souborů. Stále však je lepší provádět zálohování mimo pracovní dobu, tedy v čase, kdy je server nevyužit. Zálohování během plné zátěže serveru se může projevit jeho zpomalením.
- občas ověřit možnost obnovy dat ze zálohy,
- občas použít verifikaci dat (porovnání obsahu zálohovaných souborů s jejich originálem). Možnost verifikace nabízejí zálohovací programy.

Zálohovací systém Novell NetWare – SMS (Storage Management Services)

NetWare je vybaven rozsáhlým zálohovacím systémem, složeným z několika modulů. Pro pochopení práce se zálohovacím modulem je nutné vysvětlit nejdříve koncepci SMS.

Složení SMS

SMS je tvořeno několika navzájem spolupracujícími moduly. Základem jsou moduly tvořící jádro SMS, které běží na serveru NetWare (na obrázku je vidíme vpravo). Server, kde tyto moduly běží nazýváme *Host server*.



Obrázek 5.44: *Složení SMS*

Jádro je doplněno o zálohovací agenty TSA (*Target Services Agent*). Ty musí být spuštěny na tom počítači, jehož obsah chceme zálohovat. Některé z agentů ukazují tabulky:

Tabulka 14 Agenti TSA na serverech NetWare

Modul, program	Pro zálohování
TSANDS.NLM	Zálohování databáze eDirectory
TSADOSP.nlm	Zálohování oblasti DOS na serveru NetWare
TSA500.NLM	Zálohování souborů na serveru s operačním systémem NetWare 5
TSA600.NLM	Zálohování souborů na serveru s operačním systémem NetWare 6
TSAPROXY.NLM	Zajišťuje registraci zálohovaných pracovních stanic na zálohovacím pracovním serveru

Tabulka 5.15: Agenti TSA na stanicích Windows

Modul, program	Pro zálohování
W95TSA	Zálohovací agent na stanici sítě s operačním systémem Windows 95
TSAMAIN, TSAPREFS	Zálohovací agent na stanici sítě s operačním systémem Windows NT/2000/XP. (Na serveru musí být spuštěn modul TSAPROXY.NLM). (Soubory zálohovacích agentů se na stanice Windows nahrají v rámci instalace klienta sítě NetWare)

Vidíme, že jsou k dispozici klienti TSA pro operační systémy Novellu (tzn. soubory a databázi eDirectory na serveru), i pro operační systémy Microsoftu na síťových stanicích. Klient TSA se na síťovou stanici instaluje jako jedna ze služeb Klienta NetWare od firmy Novell.

Server, na němž jsou instalováni klienti TSA, je *Target serverem*. Když je v síti jen jeden Novell server, bude na něm spuštěno jádro SMS a zároveň klienti TSA. Bude tedy zároveň *host* i *target serverem*. Bude-li však v síti serverů více, poběží SMS jen na jednom z nich (tam kde je umístěna pásková jednotka). Na ostatních postačí spuštění agentů – půjde tedy o target servery.

Spouštění modulů SMS

Při startu SMS je nutné spouštět jednotlivé moduly v uvedeném pořadí. Některé z modulů si vytvářejí vlastní objekty v databázi eDirectory, je tedy nutné zadat jejich kontext.

1. *SMDR* – zajišťuje komunikaci s agenty zálohování. Při jeho prvním spuštění je nutné zadat údaje pro objekt databáze eDirectory. Objekt má jméno SMS SMDR Group, musíme stanovit jeho polohu v databázi eDirectory (tj. kontext), zadat jméno a heslo správce zálohování. Tím může být administrátor, nebo jím pověřený uživatel.
2. *TSA600* – agent zálohování pro soubory na serveru (pokud potřebujeme i další agenty TSA, např. TSANDS, umístíme je za tento příkaz).
3. *SMSDI* – realizuje rozhraní vůči zálohovací jednotce.
4. *QMAN* – manažer fronty zálohovacích jobů. Podobně jako u tisků jsou i zálohovací joby řazeny do fronty – vyřeší se tím současný požadavek na více zálohování. Při prvním spuštění je nutné zadat kontext objektu fronty zálohovacích jobů (*SMS Job Queue*), jeho jméno, správce a heslo.
5. *SBSC* – komunikační modul.
6. *SBCON* je posledním modulem. Jeho prostřednictvím zálohování ovládáme a jednotlivá menu si dále popíšeme.

Asi je jasné, že zadávat takové množství příkazů je krajně nepraktické. Proto jsou v NetWare 6 k dispozici dávkové soubory, kterými můžeme služby SMS nastartovat, nebo ukončit. Jde o:

- *SMSSTART.NCF* pro start služeb SMS
- *SMSSTOP.NCF* pro ukončení služeb NCF

Stejně jako operační systémy Windows používá také NetWare příkazové (dávkové) soubory. Napíšeme-li tedy jméno souboru na konzolu serveru, odstartujeme provádění příkazů zde zapsaných. Chceme-li načítat služby SMS automaticky, můžeme zapsat příkaz SMSSTART do souboru AUTOEXEC.NCF, čímž načteme zálohování současně se startem NetWare.

Poznámka *Již výše jsem se zmínil o nové vlastnosti souborového systému NSS – snímcích souborů (File Snapshot). Pokud chceme zálohovat také otevřené soubory, musíme File Snapshot aktivovat. Provedeme to příkazem na konzole serveru:*

NSS /FileCopyOnWrite={volume name}.

- za výraz *{volume name}* dosadíme jméno disku, na němž snímky souborů povolujeme
- zapíšeme-li sem parametr *ALL*, budou snímky souborů povoleny na všech discích (přesný tvar příkazu pak bude: *NSS /FileCopyOnWrite=all*)

Obrázek 5.45: *Start SMS (po zadání příkazu SMSSTART)*

Tip: Vidíme, že start zálohování není jednoduchý, při prvním spuštění je nutné zadávat údaje pro objekty eDirectory. Je tedy dobré zahrnout první start zálohování do instalace a svěřit konfiguraci odborné firmě. Během instalace je také nutné správně nahrát ovladače páskové jednotky, bez níž zálohování není možné – to je druhým důvodem instalace SMS odbornou firmou.

Zálohování dat pomocí Enhanced SBACKUP

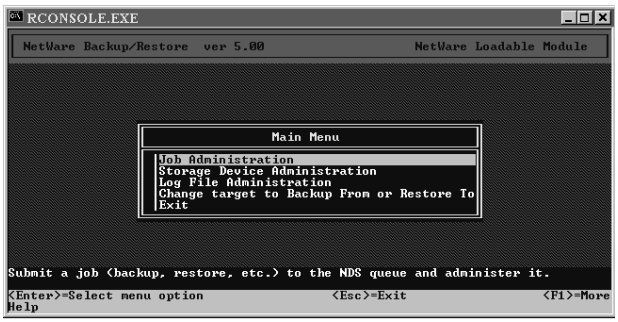
Máme-li zprovoznětnu páskovou jednotku a načteny (i nakonfigurovány) moduly SMS a zálohovací agenty, můžeme přistoupit k pravidelnému zálohování. To se ovládá z obrazovky modulu *Enhanced SBACKUP* (který startujeme příkazem *SBCON*).

Zálohování dat

Vlastní zálohování je periodicky se opakující činností. Je tedy výhodné vytvořit zálohovací úlohu (v terminologii Novellu zálohovací job), zadat parametry zálohování (co se bude zálohovat, kdy se bude zálohovat, metoda zálohování atd.) a pak pravidelně spouštět připravený job.

K definici jobu slouží první řádek obrazovky modulu *Enhanced SBACKUP* – **Job Administration.** Po jejím otevření vybereme položku *Backup* a dostaneme submenu s těmito možnostmi:

- Target Service – zde vybereme ten počítač, jehož soubory chceme zálohovat. Musí na něm samozřejmě běžet příslušný modul TSA. Pokud je v síti více



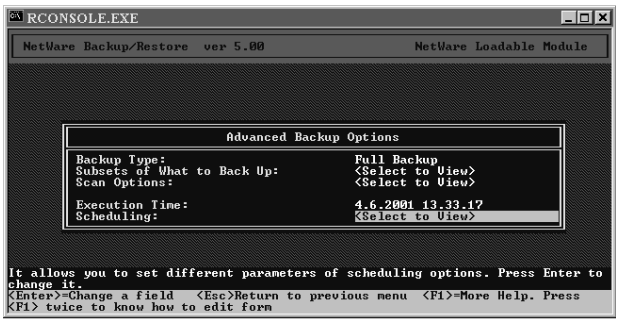
Obrázek 5.46: *Úvodní obrazovka modulu Enhanced SBACKUP*

Obrázek 5.47: *Menu pro zadání parametrů zálohovacího jobu*

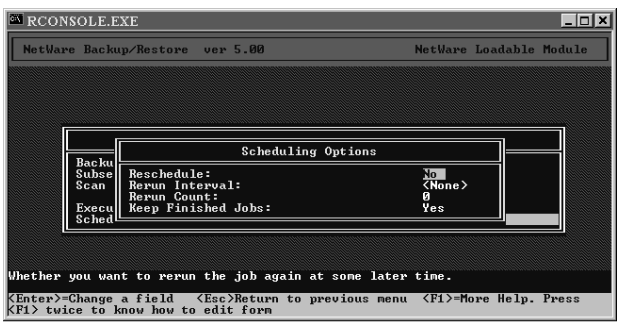
počítačů, objeví se po stisknutí *Enter* v řádku *Target Service* jejich seznam. Budeme-li zálohovat soubory ze serveru NetWare, budeme vyzváni ke vložení jména a hesla uživatele obsluhujícího zálohování. Jméno musí být zapsáno s úplným kontextem!

- What to Back Up – zde vybíráme co budeme zálohovat. Stiskem klávesy *Enter* otevřeme prázdné okno *List Resources*. Do něho pak zadáváme jednotlivé položky (celé volumes, složky, nebo soubory). Výběr položky zahájíme stiskem klávesy *Insert*, poté šipkami a *Enterem* procházíme jednotlivými logickými disky a jejich složkami. Výběr ukončíme stiskem klávesy *Esc*, (jejím stiskem přeskočí zdroj, na němž je kurzor, do okna *List Resources*).
- Description – zde zadáváme popis daného jobu. Ten nám pomůže při identifikaci úlohy zařazené ve frontě (*Job Queue*).
- Device/Media Name – slouží k určení zařízení, na něž se bude zálohovat. Má význam jen tehdy, pokud je na serveru takových zařízení více. Zvolíme-li položku *.*, bude nabídnuto zařízení, které jsme dříve určili jako implicitní. U serveru s jednou páskovou jednotkou můžeme tedy tento řádek přeskočit – zálohovat se bude na jedinou dostupnou jednotku.
- Advanced Options – sem jsou soustředěna další důležitá nastavení: *Backup Type* slouží k výběru typu zálohování (předvolen je *Full Backup*), v *Execution Time* se nastavuje čas spuštění úlohy. *Scheduling* je určen pro definici opakování úlohy: zadáme-li v řádku *Reschedule* YES, můžeme měnit parametry opakování úlohy. V *Return Interval* určujeme interval mezi opakujícími se úlohami, do *Return Count* zapíšeme kolikrát se bude úloha opakovat. YES v položce *Keep Finished Jobs* znamená, že po skončení je úloha stále dostupná pro pozdější použití.
- Append session – je poslední volbou menu Backup. Při hodnotě YES se budou nová data na pásku zapisovat za data dříve uložená, NO způsobí zapisování úlohy vždy od začátku (dřívější záloha bude přepsána novou).

Definovaný job se bude spouštět automaticky (pokud jsme tak stanovili v položce *Advanced Options/Scheduling*), nebo bude k dispozici v menu *Backup/Current Job List*. Jeho spuštění pak dosáhneme zapsáním spouštěcího času v *Advanced Options/Execution Time*.



Obrázek 5.48: *Rozšířená nastavení*

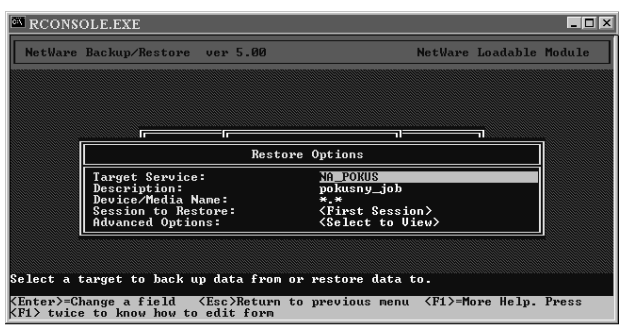


Obrázek 5.49: *Nastavení opakování úlohy*

Obnova dat

Pro obnovu dříve zálohovaných dat slouží menu *Job Administration/Restore:*

- Target Service – určuje počítač, na který budeme provádět obnovu dat. Budeme muset zadat jméno a heslo uživatele oprávněného zálohovat.



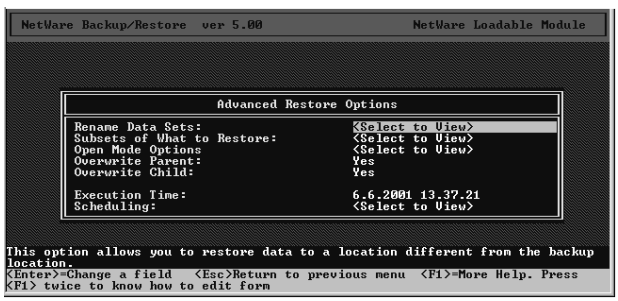
Obrázek 5.50: *Menu pro obnovu dat*

- Description má stejný význam jako při definici zálohovacího jobu.
- Device/Media Name má opět stejný význam jako při definici jobu, určujeme zde však jednotku, z níž obnovu dat provedeme.
- Session to restore zobrazí seznam dostupných úloh pro obnovu (s jejich popisem – *Description*, časem a datem zálohování a jménem stanice, kde bylo zálohování provedeno – *Source*). Při obnově si musíme dát pozor na tuto skutečnost: Agenti TSA umí zálohovat soubory nekomprimovaně i komprimovaně. Pokud však budeme obnovovat komprimovaný soubor na svazek, který komprimaci nepodporuje, soubor se naruší, aniž by o tom byla vypsána zpráva!

Obrázek 5.51: *Obnova zálohovací úlohy*

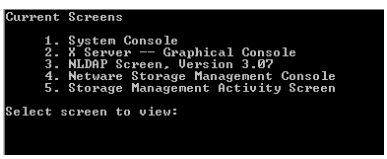
Po výběru úloh určených k obnově dat stiskneme klávesu *Esc* a v dalším okně potvrdíme spuštění úlohy (*Submit Job*). O úspěšné obnově dat obdržíme zprávu: *„The restore process was competed normally“.* Tímto způsobem se data zapíší na původní místo.

Když potřebujeme zapsat obnovená data do jiné složky (než ze které byla zálohována), máme k dispozici poslední volbu Advanced Options: Vybereme položku *Rename Data Sets*, v prázdné obrazovce stiskneme klávesu *Insert*, potvrdíme formát obnovovaných dat (*DOS* – je pouze formát jméno 8 znaků + 3 znaky na příponu, *LONG* – je formát dlouhých jmen souborů, jak je znám z Windows). Vybereme zdrojové umístění (*Source Path*) – odkud byla data zálohována a cílové umístění – kam se obnovená data zapíší. Systém pro kontrolu zobrazí obrazovku „*Restore data sets to different location*“.



Obrázek 5.52: *Rozšířené volby obnovy souborů*

Poznámka: *V předešlém odstavci je zmínka o obnovovaném formátu dat. Standardním formátem pro popis jména souboru byla dlouho norma operačního systému DOS. Ta předepisovala, že úplné jméno souboru má dvě části: vlastní jméno (obsahující maximálně 8 znaků) a příponu (s max. 3 znaky). S příchodem Windows 95 se rozšířil formát dlouhých jmen souborů (pro jméno je možné použít až 255 znaků). Pokud jsme chtěli používat dlouhá jména souborů také na serverech NetWare, bylo nutné jejich podporu doplnit. Od verze NetWare 5 se podpora dlouhých jmen instaluje automaticky. Pro obnovovaná data musíme však použít ten formát, v němž byla uložena.*



Obrázek 5.53: *Spuštěné moduly systému*

Storage Management Activity Screen

Současně se startem SBCON se rovněž spustí modul *SMS Activity Screen*. Z konzoly serveru se do něho můžeme přepnout (současným stiskem kláves *Ctrl* a *Esc* a následným zadáním čísla modulu do řádku *Select screen to view*) a zkontrolovat činnost zálohovacího programu. Uvidíme zde seznam spuštěných zálohovacích jobů a jejich úspěšnost.

Práce s páskou – Storage Device Administration

Druhý řádek utility *Enhanced SBACKUP – Storage Device Administration* je určen pro práci se zařízením, na nějž se ukládají data (většinou s páskovou jednotkou). Po jeho otevření se objeví seznam dostupných jednotek, z nichž některou vybereme. Po stisku klávesy *Insert* máme k dispozici menu *Utilities*, v němž jsou nejpoužívanější volby:

- Change the Media Label – určeno pro pojmenování pásky. Nová páska je prázdná a před zahájením zálohy ji musíme pojmenovat!
- Erase the Media – maže data na pásce. (Mazání může trvat až několik hodin!)
- Erase the Media Header – maže hlavičku pásky, v níž jsou uloženy údaje o souborech na pásce. Smazáním hlavičky se ztratí všechny údaje o souborech na pásce. Tato metoda mazání pásky je rychlejší než *Erase the Media,* ale data z pásky je možné obnovit – poskytuje tedy nižší zabezpečení mazaných dat.
- Media Status – informace o vloženém médiu.

Klient systému NetWare

Připojení stanice k serveru zprostředkovává program – síťový klient. Klienti byly postupně nabízeni pro jednotlivé operační systémy. K dispozici jsou tedy klienti pro všechny operační systémy Microsoftu (historické DOS, Windows 3.11, Windows 95/98, Windows NT) a současné Windows 2000/XP. Klienty můžeme použít dvojí:

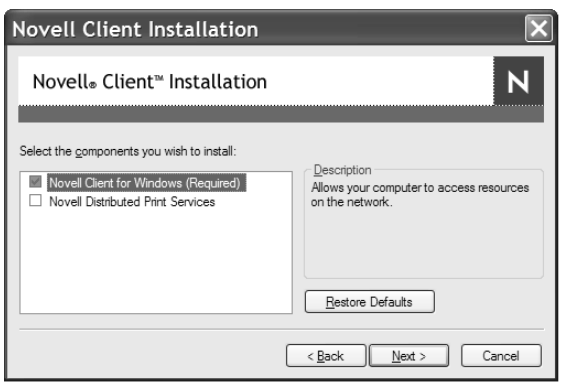
- Klienti sítě NetWare od firmy Microsoft jsou součástí Windows. Instalují se standardním způsobem popsaným v podkapitole *Načtení klienta* kapitoly *Sítě peer to peer*. Tento klient ve srovnání s klientem nabízeným firmou Novell nenabízí žádné konfigurační možnosti. Neobsahuje také podporu pro mnoho komponent NetWare (tisky NDPS, ZEN Works, zálohování, správu systému…). V dalším popisu se mu proto nebudeme věnovat.
- Klienti sítě NetWare od firmy Novell jsou těmi s nimiž se setkáváme při popisu činnosti NetWare a jim je také věnována tato kapitola. Popíšeme si klienty pro nejrozšířenější operační systém Windows XP.

Instalace Klienta

Není nijak složitá, než se jí však začneme zabývat, řekneme si, kde klienta získat. Novell jej nabízí zdarma, je součástí instalačních CD disků NetWare a samozřejmě jej lze stáhnout z www stránek firmy Novell. Novell svůj operační systém průběžně inovuje, což vyžaduje také inovaci klientů. Většina správců sítě musí tedy klienty NetWare průběžně obnovovat, nejjednodušeji prostřednictvím webových stránek.

Pokud získáme klienta prostřednictvím Internetu, bude zkomprimován a musíme jej rozbalit. Obdržíme instalační soubory, organizované do několika vložených složek. Pro Windows 2000/XP se instalační soubor jmenuje *SETUPNW.EXE*. Poklepáním myší na tento soubor spustíme instalaci, během níž klienta konfigurujeme. Nejdříve potvrdíme licenční smlouvu a poté:

Na druhé obrazovce se rozhodneme pro jednu z možností instalace: *Typical Installation* nebo *Custom Installation*. První způsob instalace je automatický, my si vysvětlíme druhou možnost, při níž můžeme instalaci klienta ovlivňovat. Zaškrtneme tedy *Custom Installation* a stiskneme tlačítko *Install*.

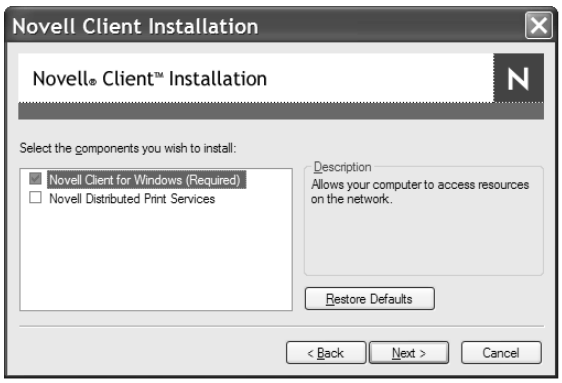


Obrázek 5.54: *Výběr komponent klienta*

Ve třetí a čtvrté obrazovce vybíráme komponenty klienta potřebné pro spolupráci se serverem. (Na obrázku vidíte třetí obrazovku, kde nám instalační program kromě klienta nabízí také možnost instalace tiskové služby NDPS).

Následující obrazovka *Protocol Preference* je určena k definici protokolů, které bude klient podporovat:

- IP only nainstaluje pouze protokol TCP/IP (stanice nebude komunikovat se serverem používajícím protokoly IPX/SPX). Protože TCP/IP je dnes standardem, je toto nejpravděpodobnější volba. Pokud jsme dříve ke komunikaci se serverem používali protokol IPX/SPX, můžeme jej odebrat zaškrtnutím políčka *Remove IPX if present.*
- IP with IPX Compatibility nainstaluje protokol TCP/IP a režim kompatibility s protokolem IPX/SPX. Pakety IPX/SPX budou převáděny na TCP/IP. Bude tak zachováno spojení stanice se servery, které pracují pouze s protokoly IPX/SPX.
- IP and IPX, stanice může komunikovat oběma protokoly. Použije ten, který používá protilehlý počítač.
- IPX pracovní stanice komunikuje pouze protokolem IPX/SPX.



Obrázek 5.55: *Výběr protokolů*

Důvod pro instalaci některé z variant protokolu IPX/SPX je dnes asi jediný – použití starého serveru (např. NetWare verze 4.x), který komunikoval protokolem IPX/SPX.

Další obrazovka nabízí pouze dvě možnosti:

- NDS (NetWare 4.x or later), kterou využijeme při spojení se všemi servery NetWare používajícími databázi eDirectory.
- Bindery (NetWare 3.x) je pro staré servery NetWare 3.x, které místo NDS používaly starší databázi Bindery.

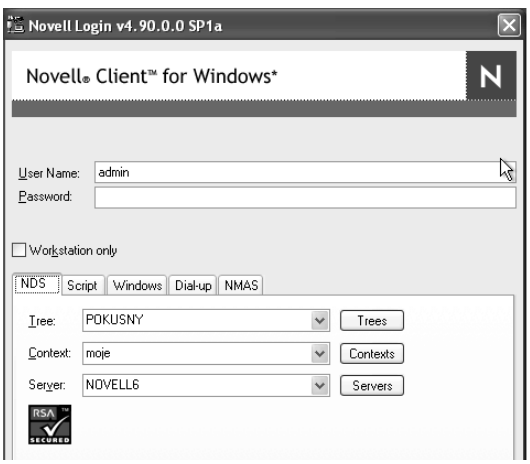
Nakonec klepneme na tlačítko *Finish*, čímž zahájíme vlastní instalaci klienta. Po jejím dokončení je nutné počítač restartovat.

Přihlášení k serveru

Po instalaci klienta a restartu počítače je nutné zadat přihlašovací údaje. Prvním přihlašovacím krokem je současný stisk kláves *Ctrl, Alt* a *Del*, k čemuž nás vyzve klient na své první obrazovce. Vstoupíme tak do přihlašovací obrazovky klienta, kde stiskem tlačítka *Advanced* rozšíříme obrazovku o detailní konfigurační možnosti. Klient Novell nabízí v rámci přihlášení několik variant, každé z nich je věnována jedna záložka obrazovky klienta. Zastavíme se u těch hlavních.

Základní záložkou je karta ***NDS***, kde zadáváme přihlašovací údaje k serveru NetWare. Všechny tři údaje doplňujeme stiskem tlačítek, umístěných vedle příslušných řádek. Po jejich stisku nabídne klient dostupné objekty, z nichž vybíráme.

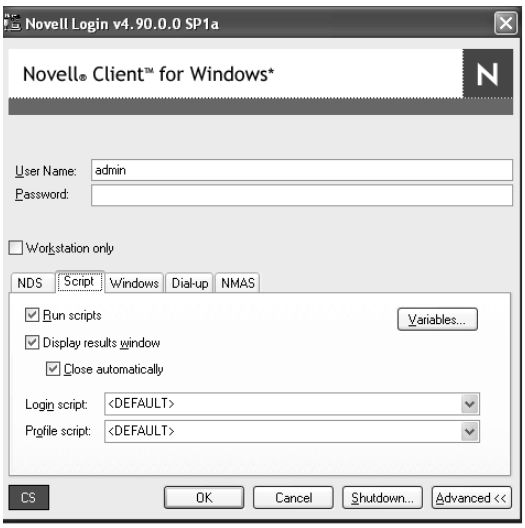
- *Tree* – jméno stromu eDirectory
- *Context* – kontext, do něhož se budeme hlásit
- *Server* – jméno serveru



Obrázek 5.56: *Přihlašovací údaje k eDirectory serveru NetWare*

Druhou záložkou je karta ***Script***. Zde se upřesňuje chování klienta během přihlašování:

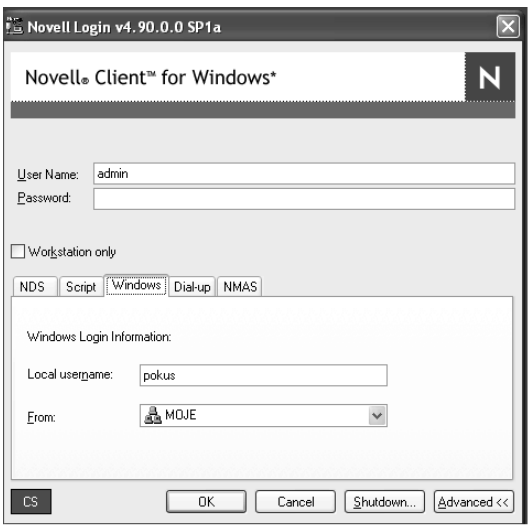
- *Run scripts* ovlivňuje spouštění přihlašovacích scriptů, vázaných na databázi eDirectory. Většinou není důvod přihlašovací skripty rušit.
- *Display results Window* zadáváme, zda se během přihlášení bude zobrazovat okno popisující průběh přihlašování (např. mapování disků atd.).
- *Close automatically* pokud během přihlášení nedošlo k žádným problémům, okno s informacemi o průběhu přihlášení se zavře. Jestliže se však problém objeví, okno zůstane otevřeno. Pokud zrušíme zaškrtnutí v tomto políčku, nebude se přihlašovací okno zavírat automaticky. Přihlašovací údaje většinou sledujeme během konfigurace sítě. Ve zkonfigurované a bezproblémové síti nemáme důvod zaškrtnutí rušit.



Obrázek 5.57: *Záložka Script*

V síti se serverem Novell se vždy hlásíme ke dvěma systémům – k Windows na lokální stanici a k NetWare na serveru. Musíme tedy dvakrát zadat přihlašovací údaje (přihlašovací jméno a heslo). Jednou k síťovému operačnímu systému NetWare (toto přihlašovací jméno a místo, kam se v eDirectory přihlásíme, jsme určili na záložce NDS) a jednou k operačnímu systému Windows. Během přihlašování jsme k tomu vyzváni dvojicí přihlašovacích oken. Třetí záložka zprava – karta ***Windows***, umožňuje ovlivnit přihlašovací údaje k Windows. Stanovíme zde, pod jakým přihlašovacím jménem se budeme přihlašovat a ke kterému počítači.

- *Local username* sem zapisujeme přihlašovací jméno, jímž se hlásíme k Windows.
- *From* zde zadáme k jaké stanici se hlásíme. Většinou se hlásíme ke svému lokálnímu PC, ale pokud v síti společně pracují servery Novellu a Microsoftu, můžeme zde vybrat počítač s operačním systémem Microsoft Server (pak samozřejmě musíme zadat také správné přihlašovací jméno).



Obrázek 5.58: *Přihlašovací údaje k Windows*

Klient Novellu nabízí možnost **sjednocení přihlašovacích údajů**, kdy se heslo přenese ze serveru NetWare na lokální stanici. Základním předpokladem je použití stejného uživatelského jména pro přihlášení k serveru NetWare a ke stanici Windows. Jsou-li obě přihlašovací jména stejná, objeví se během přihlašování okénko s nabídkou: *Change your Windows password to match your NetWare password after successful login*. Zaškrtneme-li políčko v okně, sjednotí se obě hesla. Při dalším přihlašování zadáme pouze přihlašovací údaje (jméno a heslo) k serveru NetWare. Přihlašovací údaje ke stanici Windows se doplní automaticky, což nám přihlašování zpříjemní.

Tip: Na přihlašovací obrazovce klienta vidíme políčko Workstation only. Jeho zaškrtnutím se budeme hlásit pouze k lokální stanici Windows. Používáme ho při potížích se serverem. Můžeme se tak připojit alespoň k Windows.

Dodatečná změna komponent klienta

Windows XP

Tady je nejjednodušším způsobem přeinstalování klienta a nastavení parametrů ve druhé instalační obrazovce. (Pokud doinstalováváme některou z rozšiřujících služeb, je stejně dobré použít nejnovější verzi klienta.)

Odebrání klienta

Windows XP

Odebrání klienta provedeme standardním způsobem: *Start / Ovládací panely / Přidat nebo odebrat programy.* Zde vybereme řádek *Novell Client* .

Práce s klientem

Přístup k jednotlivým menu klienta je možný těmito způsoby:

- Klepnutí pravým tlačítkem na ikonu *N* (v pravém dolním rohu systémové lišty)
- Klepnutí pravým tlačítkem na ikonu *Okolní počítače*
- Klepnutí pravým tlačítkem myši na ikonu logického disku serveru
- Klepnutí pravým tlačítkem myši na ikonu složky serveru

Pracovní postupy spojené s klientem jsme si již vysvětlili, jejich souhrn najdete v kapitole *Přehled činností v systému NetWare*. (Vyvolání shodné činnosti klienta je možné z více menu. Všechny varianty obsluhy klienta nebylo možné do knihy zahrnout – možná tedy najdete jednodušší a vám příjemnější postup.)

Vzdálený přístup

Server nebývá většinou umístěn v místnosti administrátora. Aby k němu administrátor nemusel chodit, je možný tzv. vzdálený přístup. Ten spočívá buď v prostém přenesení obrazovky serveru na pracovní stanici, nebo umožňuje prostřednictvím přístupu http vzdáleně server konfigurovat. K dispozici je několik možností, jak k serveru vzdáleně přistoupit. My si ukážeme alespoň dvě:

- *Program RconsoleJ* se používá pro připojování z místní sítě a na vzdálený počítač přenáší obrazovku serveru (je obdobou *Vzdálené plochy* Windows).
- *NetWare Remote Manager* je zástupcem webových nástrojů. Používá se pro přístup jak z vnitřní, tak vzdálené sítě (např. Internetu) a nabízí kompletní služby pro diagnostiku a správu serveru.

RconsoleJ

Je Java aplikací doplněnou poprvé do NetWare 5. Pro její správnou činnost musíme spustit příslušný modul na serveru a správný program na stanici.

Nezbytné moduly na serveru

Pro start RconsoleJ ze stanice je nutné spustit modul na serveru, který se jmenuje *RCONAG6*. Syntaxe jeho spouštěcího příkazu (z konzoly serveru) je:

RCONAG6 [heslo] [číslo_TCP] [číslo_SPX]

- *heslo* – definuje heslo, jímž se budeme muset po startu RconsoleJ přihlásit k serveru
- *číslo_TCP* – číslo portu, přes nějž bude komunikovat protokol TCP/IP. Standardní hodnota je 2034
- *číslo_SPX* – číslo portu, přes nějž bude komunikovat protokol IPX/SPX (pokud jej vůbec budeme používat). Standardní hodnota je 16800

Když parametry nezadáme, modul nás na to během svého startu upozorní a nabídne nám implicitní hodnoty, které musíme potvrdit *Enterem*. Pokud však zapíšeme startovací příkaz modulu RCONAG6 do AUTOEXEC.NCF bez parametrů, budeme muset při startu NetWare oba parametry potvrdit (čímž samozřejmě start zastavíme)! Proto zapisujeme do příkazového řádku v AUTOEXEC.NCF příkaz RCONAG6 s potřebnými parametry. Startovací řádek může například vypadat takto: *RCONAG6 heslo 2034 16800*.

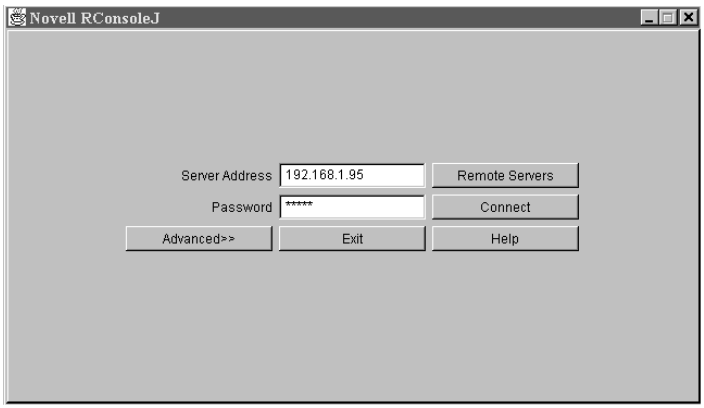
Práce na stanici

Vlastní program RconsoleJ můžeme spustit více způsoby:

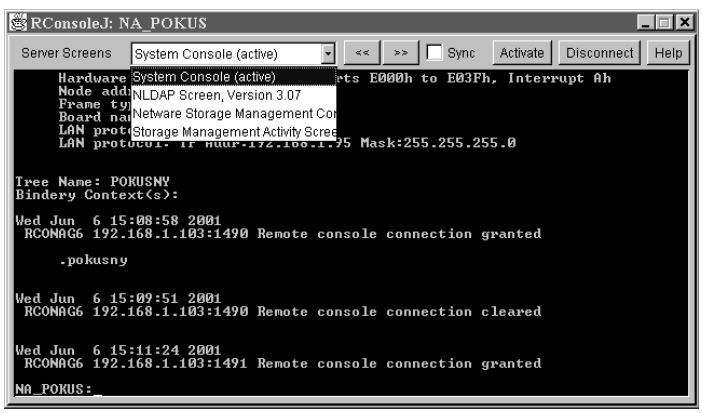
- z NetWare Administrátora přes menu *Tools* a jeho řádek *Pure IP Remote Console*.
- spuštěním souboru *RCONJ.EXE* uloženého ve složce serveru *SYS:PUBLIC*. Uložení modulu se může lišit, pokud jej tady nenajdete, použijte vyhledávání (*Start/Hledat*) na disku SYS.

Při startu se RconsoleJ zeptá na adresu serveru a heslo. Místo IP adresy serveru lze použít tlačítko *Remote Servers*, které zobrazí seznam dostupných serverů.

K ovládání konzoly je k dispozici okénko *Server Screens*, v němž si myší zobrazíme běžící moduly serveru. Myší se pak mezi nimi můžeme přepínat. Listovat mezi moduly je možné také tlačítky << a >>. Práci s programem ukončíme tlačítkem *Disconnect*.



Obrázek 5.59: *Úvodní obrazovka RConsoleJ*



Obrázek 5.60: *Obrazovka RConsoleJ*

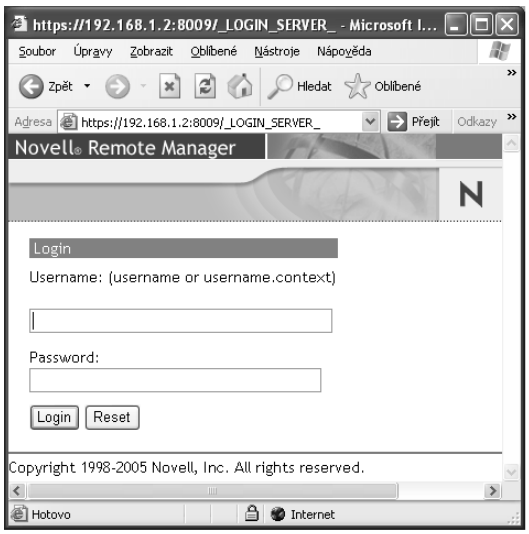
NetWare Remote Manager

Jde o moderní a velmi komplexní nástroj. Je k dispozici ve verzi NetWare 6.x, jeho předchůdcem byl *NetWare Management Portal*, dostupný ve verzi NetWare 5.1. Protokolem TCP/IP přistupujeme vždy k počítači prostřednictvím nějakého portu. Pro NetWare Remote Manager jím je port 8009. Protože jde o webovou utilitu, je další podmínkou pro úspěšný start použití webového prohlížeče (např. Internet Exploreru, či Netscape Navi-

gatoru atd.). NetWare Remote Manager spustíme z prohlížeče příkazem *https://IP_adresa_serveru: 8009* (příklad použití vidíte na obrázcích, kde IP adresa serveru byla 192.168.1.2). Podrobný popis programu by přesáhl rámec knihy, popíšeme si alespoň ovládání a některé jeho obrazovky.

Po spuštění Manageru se musíme přihlásit k serveru. Chceme-li jej spravovat, budeme se přihlašovat k účtu *Admin*.

Po správném připojení k serveru se objeví domovská stránka Manageru. V horním pruhu vidíme tlačítka, z nichž je důležité čtvrté zleva. Konfiguruje se jím samotný Manager. V levém sloupci stránky jsou k dispozici odkazy na konfigurační a diagnostické služby manažeru. Pravá, největší část obrazovky je pracovní. Odkazy jsou rozděleny do základních skupin:



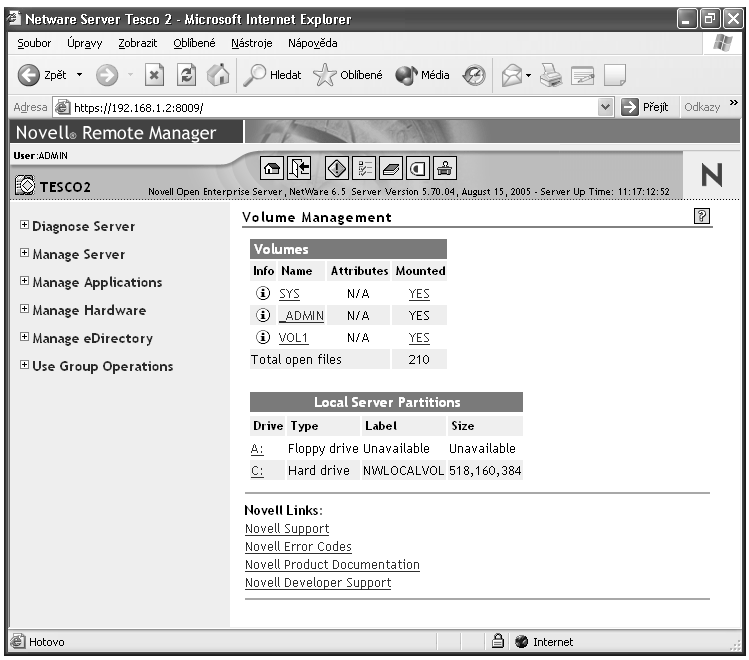
Obrázek 5.61: *Přihlášení k NetWare Remote Manageru*

Diagnose Server pro diagnostiku serveru. Zde je zajímavá obrazovka *Health monitor*, monitorující stav serveru, důležitý je především sloupeček *Status*. Ten prostřednictvím ikon informuje o momentálním stavu parametru. Ikony mají následující význam:

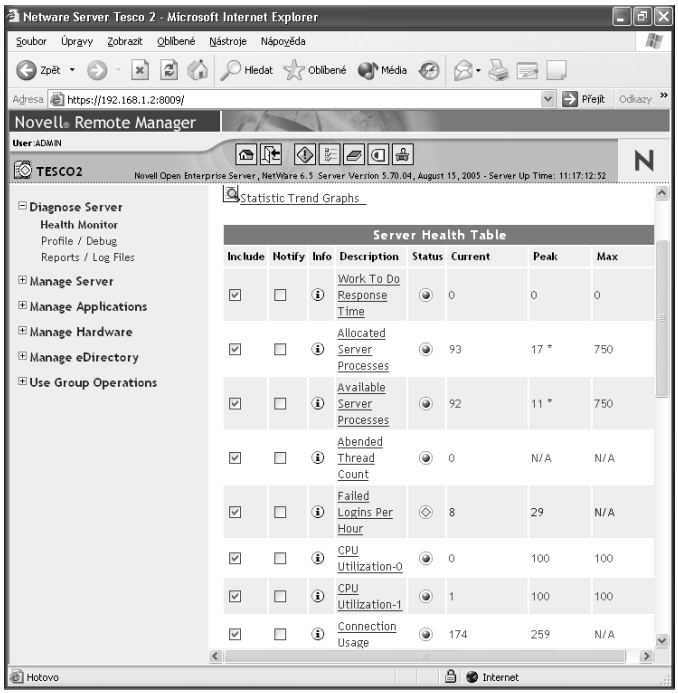
- Zelený kruh – parametr v pořádku
- Žlutý kosočtverec – podezřelá hodnota
- Červený obdélník – špatný parametr
- Černý křížek – značí přerušené spojení se serverem, parametr nemůže být načten.

Manage server pro správu serveru. Tady je soustředěno mnoho funkcí, s nimiž jsme se již na stránkách knihy setkali (vyjmenujeme alespoň některé):

- *Volumes* – přístup k logickým diskům serveru, můžeme montovat disky, spravovat diskové oblasti, prohlížet složky a soubory, přejmenovávat, mazat, kopírovat, měnit atributy atd.
- *Console Screens* – zobrazíme (ale nemůžeme ovládat) konzolu serveru.
- *Connections* – seznam aktuálních připojení, informace o nich, jejich rušení, přehled o otevřených souborech jednotlivých uživatelů, možnost rozesílání zpráv...
- *Set Parameters* – prohlížení a nastavování parametrů systému (příkaz SET).
- Schedule Tasks – umožňuje naplánovat příkazy konzoly serveru.
- *Console Commands* – seznam příkazů serveru. Můžeme si prohlédnout jejich nápovědu, případně přejít do konzoly serveru a příkazy zadat.



Obrázek 5.62: *Domovská stránka NetWare Remote Manageru*



Obrázek 5.63: *Diagnostika NetWare Remote Manageru*

- *View Statistics* – rozsáhlé statistiky o činnosti serveru.
- *Down / Restart* – vypnutí, restart nebo reset serveru.

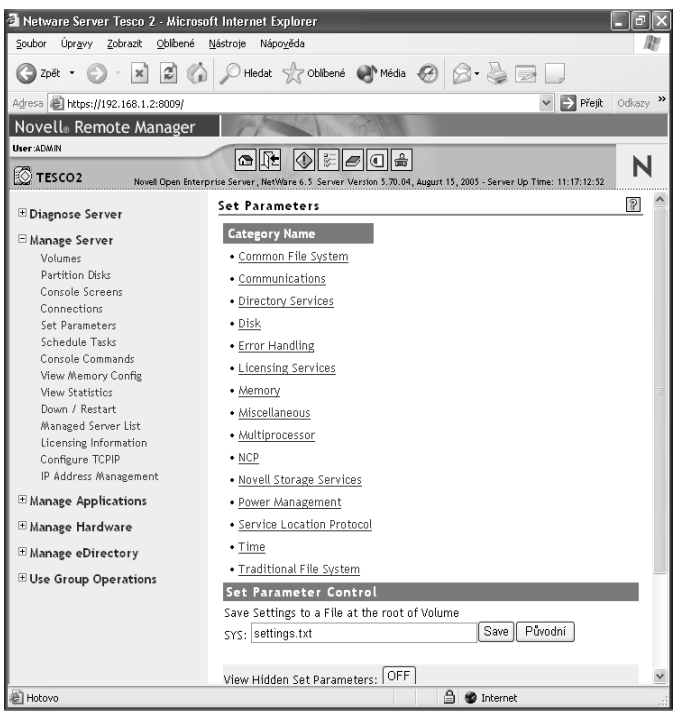
Manage Applications správa aplikací – odkazem *List modules* vyvoláme seznam spuštěných modulů, můžeme o nich získat detailní informace, případně je ukončovat a spouštět.

Manage Hardware správa hardwaru, informace o konfiguraci hardwarových prvků.

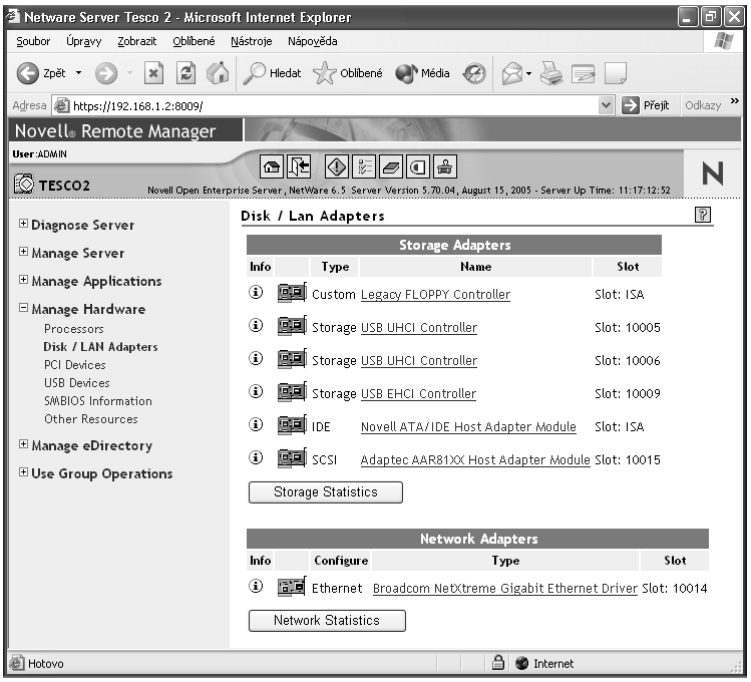
Manage eDirectory – správa eDirectory.

- *Access Tree Walker* – prohlížení stromu a objektů eDirectory, jejich vytváření a mazání.

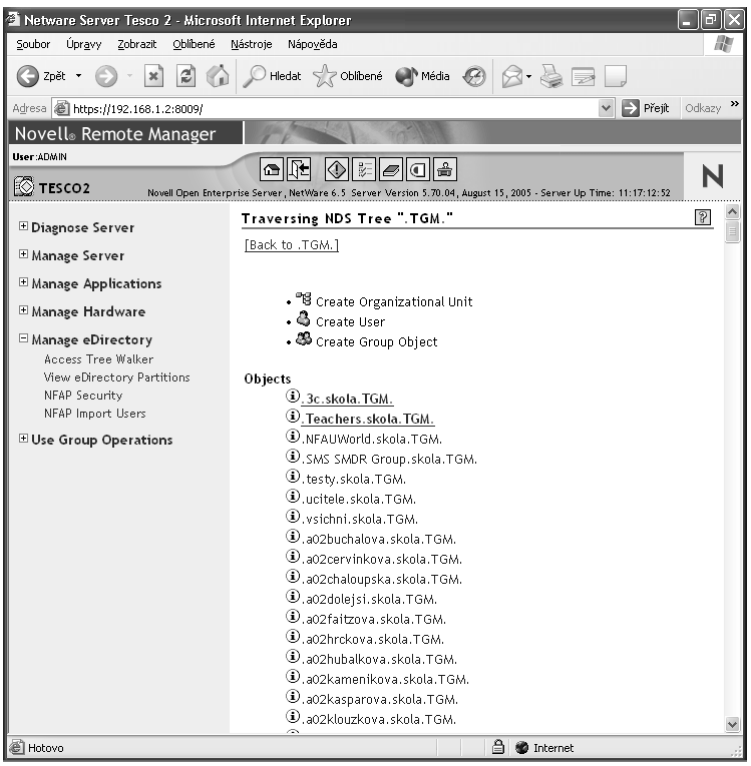
Use Group Operations se používá ke správě skupin serverů v rozsáhlých sítích



Obrázek 5.64: *Správa serveru z NetWare Remote Manageru*



Obrázek 5.65: *Správa hardwaru z NetWare Remote Manageru*



Obrázek 5.66: *Správa eDirectory z NetWare Remote Manageru*

Přehled činností v systému NetWare

V závěru kapitoly jsem zařadil stručný přehled postupů, o nichž byla řeč při popisu síťového operačního systému Novell NetWare.

Tabulka 5.16: Přehled postupů v NetWare

Činnost	Druh prostředku	postup
Start serveru	Program v DOS oblasti SETUP.EXE	Spustit program SETUP.EXE, uložený ve složce C:\NWSERVER, je možné použít parametr -na, který vyřadí automatické načítání AUTOEXEC.NCF.
Vypnutí serveru	Console Command: DISABLE LOGIN, DOWN, Utilita konzoly serveru MONITOR	1. Zakázat přihlášení nových uživatelů k serveru příkazem konzoly DISABLE LOGIN. 2. Zkontrolovat, zda někdo momentálně nepoužívá programy na serveru (na konzole serveru spustit modul MONITOR, v menu Connection vybrat uživatele, klepnout na něj, pokud má otevřené programy, upozornit jej na to, že je musí zavřít, pokud je otevřené nemá odpojit ho klávesou Delete). 3. Server zaparkovat příkazem DOWN.
Přihlášení do sítě	Klient NetWare	Po startu PC se objeví okno klienta: zapsat přihlašovací jméno (username) a heslo (password). Při prvním startu klienta zadat polohu objektu User: stisknout tlačítko Advanced a na kartě NDS vyplnit pomocí tlačítek (vedle jednotlivých řádek) přihlašovací parametry (tree, kontext, server).
Odhlášení ze sítě	Klient NetWare	Nejčastěji legálním ukončením Windows, nebo klepnout pravým tlačítkem myši na ikoně serveru (k němu přes Okolní počítače) a v menu vybrat Logout.
Vytvoření uživatele	NetWare Administrator	Vybrat kontejnerový objekt, v němž chceme účet vytvořit, klepnout (v nástrojové liště) na ikonku uživatele, vybrat objekt User a vyplnit konfigurační obrazovku, pomocí tlačítek dokonfigurovat vlastnosti. Je také možné klepnout na kontejner pravým tlačítkem myši a z menu použít Create.
Vytvoření kontejnerového objektu	NetWare Administrator	Klepnout pravým tlačítkem na objektu, v němž bude kontejner umístěn (může to být rovněž objekt [Root]). V menu vybrat Create a v následující obrazovce typ kontejnerového objektu (nejčastěji Organizational Unit OU). Vyplnit následující obrazovku vlastností.
Obnova smazaných souborů (salvage)	NetWare Administrator	Otevřít objekt Volume, najít složku, v níž soubor obnovujeme. Menu Tools/Salvage do okénka Include zadat jméno souboru, (nebo *.* zobrazit všechny obnovitelné soubory), umístit kurzor na soubor a tlačítkem Salvage obnovit. Je-li soubor ve smazané složce, použít volbu „Get from Deleted Directories“ v okénku Sources.
	Klient NetWare	V Průzkumníkovi klepnout pravým tlačítkem na složku, v níž je smazaný soubor, v menu použít Salvage Files. V okně vybrat soubor a použít tlačítko Salvage File (tlačítkem Salvage All obnovíme vše ve složce).

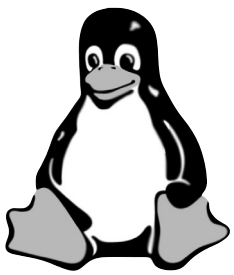
Fyzické odstranění smazaných souborů (purge)	NetWare Administrator	Stejný postup jako při obnově (salvage), ale v konečném okénku použít tlačítko Purge.
	Klient NetWare	Stejný postup jako při obnově (salvage), ale v menu vybrat Purge Files.
Práce s přístupovými právy ke složkám a souborům	NetWare Administrator	2x klepnout levým tlačítkem myši na uživatele a na obrazovce vlastností vybrat tlačítko "Rights to Files and Directories". Tlačítkem ADD přidáváme trustee uživatele ke složce, Delete trustee maže. Tlačítka Find a Show slouží k zobrazování již definovaných práv.
	Klient NetWare	Klepneme pravým tlačítkem myši na složce jejíž přístupová práva chceme měnit (dostaneme se k ní průzkumníkem, přes Okolní počítače ...). V menu použijeme Trustee Rights. Tlačítka: ADD práva přidává, Remove odebírá, "Inherited Rights And Filters" umožňuje práci s filtrem děděných práv.
Přidělování objektových práv	NetWare Administrator	Klepnout pravým tlačítkem myši na objektu databáze eDirectory, zvolit: 1. Trustees of this Object – přiděluje pověřence k tomuto objektu 2. Rights to Other Objects – přiděluje právo k práci s ostatními objekty Tlačítkem ADD Trustee přidělujeme, Delete Trustee mažeme práva. Effective Rights zjišťuje efektivní práva. Levá část obrazovky (Object Rights) je k práci s objektovými právy, pravá (Property Rights) pro práci s právy vlastností.
Ekvivalence Objektových práv	NetWare administrator	2x klepnout levým tlačítkem myši na uživateli, stisknout tlačítko "Security Equal to Me" a vyhledat uživatele, jehož práva budeme používat.
Mapování disku	Klient NetWare	Vybrat složku, kterou mapujeme, klepnout pravou klávesou myši a v menu "Novell Map Network Drive…". Následně vyplnit mapovací obrazovku.
Vytvoření tiskového prostředí	NetWare Administrator	1. na serveru vytvořit tiskové objekty: Print server, Print queue, Printer: Klepnout pravým tlačítkem myši na kontejneru v němž budeme prostředí vytvářet, použít menu Create a tvořit objekty. 2. vytvořit vazby mezi objekty: v obrazovce vyvolané tlačítkem Assignments použít tlačítko ADD, je nutné přiřadit tiskárnu frontě a tiskárnu tiskovému serveru. 3. Z konzoly serveru nastartovat modul SERVER.NLM.
Stav zrcadlení	Console Command: MIRROR STATUS	Vypíše momentální stav zrcadlení.
Zapnutí vzdáleného přístupu k serveru	NetWare Remote Manager	V internetovém prohlížeči zadat: *https://IP_adresa_serveru:8009*. Vybrat v levém sloupci z odkazů menu, v pravé části obrazovky pracovat.
	Příkaz RCONJ.EXE nebo v NetWare Administrátor Tools/Pure IP Remote Console	Komunikuje protokolem TCP/IP. Na serveru je nutné spustit NLM modul RCONAG příkazem: RCONAG6 heslo 2034 16800 (nejlépe v souboru AUTOEXEC.NCF).

Kapitola 6

Sítě Linux

Linux je v současné době fenomén, který nejde přehlédnout. Často se o něm mluví a velké společnosti, jako třeba IBM, ho berou velice vážně. Linux je operační systém, který je sice velmi mladý, ale má své nepřehlédnutelné výhody. Asi nejdůležitější je, že se dynamicky rozvíjí, je k dispozici zdarma a staví na filozofii, kterou známe pod pojmem Unix. Protože je nasazován jednak jako server v prostředí Internetu a také jako server pro lokální počítačové sítě (Intranet), budeme se jím v rámci této příručky zabývat.

Obrázek 6.1: *Linus Torvalds – strůjce Linuxu*



Obrázek 6.2: *Tučňák – logo Linuxu, autorem je Larry Ewing*

Historie Linuxu začíná v roce 1991, kdy student Linus Torvalds (viz fotografie vpravo) poprvé zveřejnil na Internetu jeho zdrojové kódy. Od té doby se na jeho vývoji podílejí nejrůznější lidé z celého světa a Linus jim dělá neformálního vůdce. Kód Linuxu je volně šiřitelný a díky Linusovi, který se o něj velmi pečlivě stará, sklízí mnoho úspěchů. Každý, kdo má zájem, může do vývoje přispět, ať už radou, nebo svým programátorským uměním.

Linux je velmi jednoduchý, snadno rozšiřitelný a univerzální. Lze ho využívat jako pracovní stanici s grafickým uživatelským prostředím, v prostředí kanceláře, ale i jako souborový nebo aplikační server. Pro nás je asi nejzajímavější projekt Samba, díky kterému může Linux nabízet disky a tiskárny v prostředí lokální počítačové sítě stejně jako Windows 98 nebo Windows 2000 (až na některé speciální služby, jako je např. Active Directory).

Základy Linuxu

Protože je Linux v podstatě Unixem, vřele doporučujeme jakoukoliv literaturu, která se Unixem zabývá. Na trhu jsou k dispozici i specializované knihy, které se Linuxu věnují výhradně. V těchto kapitolách se budeme zabývat zejména jeho možnostmi z pohledu zapojení a jeho využití v počítačové síti. Nejprve se však seznámíme se základními pojmy, které se Linuxu těsně dotýkají.

Licence

Linux a většina jeho součástí je šířena pod licencí GPL (General Public Licence), která zaručuje dostupnost zdrojových kódů, možnost jejich redistribuce a modifikace. Programy šířené pod touto licencí lze prodávat jen za manipulační poplatek a licenci nelze ze zdrojových kódů odstranit. To však nezabraňuje, aby firmy takové programy dodávaly za poplatky, které hradí poskytované služby. GPL licence pochází od sdružení GNU (GNU is Not Unix), které bylo založeno Richardem Stalmannem a jehož základní ideou je sdílení programů se zdrojovými kódy bez omezení. Díky této myšlence se mohou lidé z celého světa učit z programátorské práce jiných, podílet se společně na vývoji různých projektů a volně využívat vše, co tímto způsobem vzniklo.

Při používání Linuxu se setkáme i s jinými licencemi, než je GPL. Mezi nejznámější patří licence BSD, která není tolik restriktivní v ohledu komerčního využití kódu, který pod touto licencí vznikl (dovoluje kód použít, upravit, prodat a upravenou verzi není nutno zveřejnit). Jedno však mají společné – obě vyhovují požadavku označení jako „Otevřený kód“ (Open Source, viz *http://www.opensource.org*).

V Linuxu lze samozřejmě spouštět a používat také komerční programy, ovšem u nich ztrácíte hlavní výhodu Linuxu – totiž možnost opravovat chyby nebo se sami podílet na dalším vývoji svého oblíbeného programu (není potřeba jen programovat, stačí třeba jen oznamovat chyby nebo pomoci s ideovými nápady).

Distribuce

To, co dnes označujeme jako Linux, je obvykle obsáhlý soubor nejrůznějších programů. Ve skutečnosti je však Linux jen jádro operačního systému. Ostatní součásti, jako je například grafické uživatelské prostředí, WWW prohlížeč, program poštovního klienta, kancelářské programy (tzv. Office) a další, jsou sesbírané z celého Internetu. Lze odtušit, že poskládání a sladění kompletního funkčního systému bude poměrně obtížná práce. Proto jsou k dispozici tzv. distribuce, které vše důležité umístí „pod jednu střechu“ a koncový uživatel jen zasune instalační CD-ROM do počítače a celý komplet si snadno nainstaluje. Mezi nejznámější distribuce patří Red Hat, SuSE, Mandrake, Debian a mnoho dalších. Všechny jsou si dost podobné, s trochou nadsázky se dá říci, že obsahují totéž. Při podrobnějším pohledu však zjistíte, že každá distribuce má své charakteristické rysy, kterými si získává své příznivce (např. poskytovaná technická podpora, obsažené novinky, sladění distribuce s komerčními aplikacemi, jako je např. SQL server Oracle, dostupnost distribuce pro různé platformy, jako jsou např. počítače s procesory Sparc, Alpha, Motorola a podobně).

Konečné rozhodnutí o tom, která distribuce je pro vás nejvhodnější, je závislé na mnoha faktorech, a proto nelze říci, která z nich je nejlepší. Je to podobná situace jako třeba u výběru automobilu. Ne všichni si koupíme Jaguára nebo Škodovku a každý budeme mít pro svůj výběr jiný důvod. Většina konkrétních informací, které zde najdete, bude psána obecně s odkazy na řešení v distribuci Red Hat.

Start systému

Linux se velmi dobře snáší s ostatními systémy, a proto ho lze nainstalovat na jeden počítač například se systémem MS Windows. Mezi jednotlivými systémy pak přecházíme restartem počítače a zavedením vybraného systému. Výběr se provádí pomocí speciálního programu (zavaděč, boot loader), který se aktivuje na začátku spouštění počítače. Nepoužívanějšími zavaděči je LILO a Grub nebo třeba XOSL (*http://www.xosl.org*).

Při startu Linuxu je do paměti zavedeno jádro, které je pak v paměti trvale přítomno a zajišťuje uživatelům i programům všechny základní služby (spouštění programů, ochrana pomocí práv, možnost současného běhu více programů nebo současné práce více uživatelů, jednotné prostředí pro aplikace a přístup k hardware počítače atd.). Jádro Linuxu je modulární, což znamená, že pro ovládání nejrůznějších vstupně – výstupních zařízení stačí zavést za běhu příslušný modul (ovladač). Samo jádro poskytuje nejzákladnější služby, a proto jsou doplňky zajišťovány tak zvanými démony (tj. programy, které se spustí při startu systému a pak až do jeho vypnutí poskytují své služby) nebo uživatelskými aplikacemi. Spouštění démonů není v jednotlivých distribucích stejné, a proto je potřeba se vždy alespoň rámcově s danými zvyklostmi seznámit. Pro jednoduchou správu jsou vždy k dispozici nástroje, které poskytují příjemné rozhraní s menu (`ntsysv`, `tksysv`, `linuxconf` a podobně).

Z historických důvodů je v Unixových systémech zvykem pracovat v tzv. příkazovém řádku (shell), což je obdoba textového režimu, ve kterém pracoval DOS (avšak s mnohem většími možnostmi). V dnešní době je však obvyklejší práce v grafickém uživatelském prostředí, kde si lze spustit libovolné množství programů a shellů (terminálů) ve zvláštních oknech (obdobně jako „Příkazový řádek“ v prostředí MS Windows). Jak shell, tak grafické uživatelské rozhraní si mohou různí uživatelé volit nezávisle na sobě různě, což je v kontrastu k prostředí MS Windows, kde je k dispozici jen jeden shell (`command.com`) a jen jedno grafické prostředí.

Uživatelské účty

V Linuxu rozlišujeme uživatele a skupiny stejným způsobem, jako v ostatních Unixech. Databáze uživatelů najdeme v souboru `/etc/passwd`, kde je na každém řádku záznam o jednom účtu. Jednotlivé položky jsou odděleny dvojtečkou, po řadě jsou to: přihlašovací jméno, zakódované heslo, identifikační číslo uživatele (PID), číslo skupiny

(GID), plné jméno uživatele, domácí adresář uživatele, používaný shell. Místo hesla je dnes obvykle jen znak „x“, protože zakódovaná hesla jsou uschována před zvídavými zraky v souboru `/etc/shadow` (tento soubor nemohou obyčejní uživatelé číst). Skupiny jsou definovány podobně jako uživatelé (tedy jeden záznam na jednom řádku) v souboru `/etc/group`. Tyto soubory lze upravovat ručně, ale obvykle v systému najdeme specializované nástroje, které umožňují záznamy bezpečně přidávat i mazat (lze používat různá grafická rozhraní nebo řádkové nástroje jako např. `adduser`, `useradd`, `userdel`, `addgroup` a pod).

Příklad části souboru `/etc/passwd`:

```
kerslage:x:503:100:Milan Kerslager,,,:/home/kerslage:/bin/bash
plach:x:505:100:Pavel Lach:/home/plach:/bin/tcsh
huzva:x:507:100:Rene Huzva:/home/huzva:/bin/csh
jane:x:508:100:Jane Monkey:/home/students/jane:/bin/ksh
adamec:x:510:100:Petr Adamec, KIT:/home/adamec:/bin/sh
```

Každý uživatel je členem alespoň jedné skupiny, kterou označujeme jako primární (primární skupina je pro každého uživatele uvedena v souboru `/etc/passwd`). Pokud bude uživatelské jméno uvedeno v souboru `/etc/group` u dalších skupin, bude uživatel po přihlášení zároveň i jejich členem. Primární skupinu lze měnit pomocí příkazu `newgrp` (spustí se nový shell), a pokud zná uživatel heslo pro vstup do skupiny (nastavuje se příkazem `gpasswd`), které není přímo členem, může do ní tímto příkazem po zadání správného hesla vstoupit.

Hesla pro vstup do systému lze měnit pomocí příkazu `passwd`. Systém obvykle kontroluje, zda je zadané heslo bezpečné, tj. jestli to není obyčejné slovo, které lze snadno uhádnout. Proto obvykle vkládáme do hesel speciální znaky (středník, čárka, hvězdička, závorka apod.), kombinace velkých a malých písmen nebo čísel. Při změně hesla je nejprve nutné vložit staré heslo a pak teprve dvakrát nové heslo (pro kontrolu). Při zadávání hesla se obvykle nic nezobrazuje (ani hvězdičky).

Největší práva má v Unixech uživatel root (tj. administrátor systému), jehož heslo zadáváme obvykle při instalaci. Tento účet bychom měli využívat velmi zřídka, protože při drobné chybě můžeme poškodit systém, například nechtěným smazáním nějakého souboru. Uživatel root má v systému neomezená práva: může měnit přístupová práva k souborům, zakládat a mazat uživatele, měnit uživatelům jejich hesla, instalovat nové programy a podobně.

Přihlášení do systému

Pokud chceme pracovat v Linuxu, máme několik možností, jak do systému přihlásit. Nejjednodušší způsob přihlášení je v textovém režimu přímo na konzoli (konzolí míníme počítač, klávesnici a monitor, na kterém systém běží). V tomto případě je po vložení přihlašovacího jména a správného hesla uživateli spuštěn jeho vybraný shell (např. bash, tcsh, ksh apod.). Uživatel pak může zadávat příkazy v textovém režimu, případně si spustit grafické uživatelské prostředí. Současné systémy jsou po instalaci obvykle nastaveny tak, že po startu je rovnou spuštěno grafické prostředí, do kterého se lze přihlásit podobným způsobem jako při přihlašování do Windows NT nebo do Windows 2000.

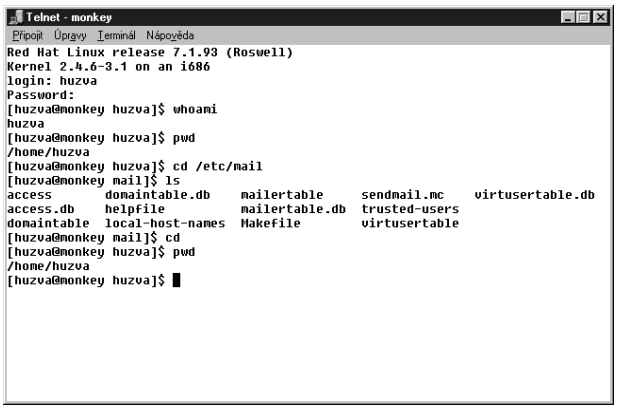
Terminálový přístup

Jinou možností, jak pracovat s Linuxem, je přihlásit se k systému pomocí počítačové sítě. V tom případě máme opět několik možností. Základním způsobem je přihlášení pomocí terminálové emulace, kdy získáme podobný přístup jako u textové konzole (tj. je spuštěn shell a uživatel může pracovat v textovém režimu).

Pro terminálový přístup lze použít například program `telnet.exe`, který je přímo součástí MS Windows. Jeho nevýhodou však je, že spojení se serverem lze odposlouchávat a zjistit tak i přihlašovací jméno a heslo. Proto se v poslední době pro terminálové spojení se vzdáleným počítačem používá šifrovaného spojení pomocí protokolu SSH.

K dispozici jsou jak komerční, tak i volně šiřitelní klienti. Jejich stručný přehled najdete v následující tabulce.

Zvláštní problém je s kódováním znaků, které v českém jazyce používáme. Ve světě Windows se pro náš jazyk používá kódová stránka CP-1250, která se v některých písmenech liší od mezinárodního standardu ISO-8859-2, který používají systémy Unix. Proto jsou v prostředí Windows vidět v terminálu české znaky špatně. Systémové řešení předpokládá, že terminál bude schopen převádět napsané znaky před odesláním do vzdáleného systému do kódování ISO a přijaté znaky před zobrazením naopak do kódování Windows. Toto elegantní řešení podporují jen některé terminálové programy, a proto jejich výběru věnujte dostatečnou pozornost.



Obrázek 6.3: *Ukázka přihlášení pomocí programu telnet.exe z Windows k Linuxu*

Tabulka 6.1: Klienti pro šifrované spojení se serverem

Název	SecureCRT	PuTTY	F-Secure SSH	SSHDOS
Popis	Komerční klient, k dispozici je i implementace serveru pro Windows	Volně šiřitelný klient, umožňuje i překlad kódování ISO na kódování používaná v MS Windows	Komerční klient, k dispozici je i implementace serveru pro Windows	Volně šiřitelný klient pro paketový driver
Adresa	http://www.vandyke.com/	http://www.chiark.greenend.org.uk/~sgtatham/putty/	http://www.f-secure.com/	http://sshdos.sourceforge.net

Práce v grafickém režimu

Pokud chceme pracovat s Linuxem v grafickém prostředí, lze si ho na konzoli (tj. přímo na počítači, kde Linux běží) po přihlášení spustit ručně (obvykle příkazem `startx`) nebo Linux nastavit tak, aby bylo grafické prostředí spuštěno ihned po startu systému (obvykle změnou implicitního runlevelu, např. pomocí nástoje `linuxconf` nebo ruční úpravou souboru `/etc/inittab`).

Do grafického uživatelského prostředí lze vstoupit i ze vzdáleného počítače. Ke komunikaci se používá tak zvaný X protokol (podle názvu grafického prostředí X Window System, které se v prostředí Unixů používá). Programy pak běží na vzdáleném počítači a k nám je přenášen jen jejich grafický výstup (obdobným způsobem funguje Terminálový server v prostředí Windows 2000). Uživatel může sedět u počítače s jiným Unixem nebo pracovat v prostředí MS Windows, které je rozšířeno o možnost spolupráce se vzdáleným systémem X Window System pomocí speciálního programu (např. X-Win32, viz *http://www.starnet.com*).

Pro vzdálenou práci v grafickém prostředí lze využít také VNC (Virtual Network Computing, *http://www.uk.research.att.com/vnc/*). Jeho výhodou je, že se od něj lze v jakémkoliv okamžiku odpojit a po opětovném připojení (i z jiného místa) je pracovní plocha stále ve stejném stavu. Připojovat se lze z různých operačních systémů i prostředí, dokonce i pomocí prohlížeče WWW. Pokud budete chtít VNC používat, je potřeba na serveru (tj. v Linuxu na cílovém počítači) spustit serverovou část VNC (démona), která poběží stále a bude udržovat vzhled pracovní plochy. Po připojení klienta je pracovní plocha po síti přenášena k uživateli a vstup klávesnice a myši je přenášen zpět k aplikacím na serveru.

Oprávnění k souborům a adresářům

Základní model přístupových práv pracuje v Unixech i v Linuxu na velmi jednoduchém principu. Každý soubor, i adresář, patří nějakému uživateli a skupině. Přístupová práva jsou definována pro každý soubor i adresář zvlášť pro vlastníka, skupinu a pro všechny ostatní. Při vyhodnocování přístupových práv se uvažují vždy jen ta nejkonkrétnější přístupová práva. To znamená, že pokud k souboru přistupuje jeho majitel, systém vezme v úvahu jen jeho přístupová práva, kdežto práva skupinová a práva pro ostatní se neuplatní (tj. ani v případě, že uživatel je členem skupiny, které soubor či adresář patří). Podobně pro členy skupiny jsou významná jen práva skupinová. Práva pro ostatní jsou vyhodnocována jen pro uživatele, kteří nejsou ani vlastníci příslušného souboru či adresáře, ani nepatří do skupiny, které soubor nebo adresář patří. Jedinou výjimkou je uživatel root, který je administrátorem systému. Na tohoto uživatele se žádná práva nevyhodnocují (může úplně vše). Jednoduše lze také říci, že systém nikdy nevytváří průnik nebo sjednocení přístupových práv.

Samotná práva jsou vždy tři (tři pro vlastníka, tři pro skupinu a tři pro ostatní). Jedná se o právo čtení (Read), zápisu (Write) a spuštění (eXecute). Význam jednotlivých práv je uveden v následující tabulce.

Tabulka 6.2: Význam jednotlivých práv

Právo	Soubor	Adresář
R (Read)	Ze souboru je povoleno číst	Zadáním příkazu ls je vidět obsah adresáře (tj. seznam souborů a adresářů)
W (Write)	Do souboru je možno zapisovat (tj. měnit jeho obsah)	V adresáři lze zakládat a mazat soubory i adresáře
X (eXecute)	Soubor je možno spustit (tj. je to program nebo skript)	Do adresáře lze vstoupit (pro přístup k souboru či adresáři je nutné mít právo x i ve všech nadřízených adresářích)

Nastavení přístupových práv

Přístupová práva se nejjednodušeji nastavují pomocí interaktivního nástroje. V textovém režimu můžete použít program `mc` (Midnight Commander, obdoba Norton Commandera nebo Manažera 602), kde lze práva nastavit pomocí menu přístupného pomocí klávesy F9. V grafickém prostředí lze (podobně jako v prostředí Windows NT nebo 2000) využít kontextové menu, které je ve správci souborů přístupné klepnutím pravým tlačítkem myši na požadovaný soubor nebo adresář.

Na příkazovém řádku lze použít příkaz `chmod`. Práva se vyjadřují buď trojmístným oktalovým číslem, nebo jednopísmennými zkratkami. Trojmístné oktalové číslo zastupuje na svých pozicích práva pro vlastníka, skupinu a ostatní. Hodnota čísla na pozici je vždy součtem vah příslušných práv (read 4, write 2, execute 1), takže přístupová práva rwxr-xr --- můžeme vyjádřit číslem 754 (rwx je 4+2+1, r-x je 4+1 a r -- je 4). V případě zápisu podle zkratek se používá písmene *u* pro vlastníka, *g* pro skupinu, *o* pro ostatní a znak *a* pro všechny tři zároveň. Práva můžeme nastavit znakem =, přidat znakem + a odebrat znakem – (např. příkaz `chmod a+x soubor` přidá vlastníkovi, skupině i ostatním právo soubor spustit). Následující tabulka porovnává všechny zmíněné způsoby:

Tabulka 6.3: Příklady vyjádření přístupových práv

Práva	Číselné vyjádření	Znakový zápis	Význam
`rwxr-xr-x`	*755*	u=rxw,g=rx,o=x	Obvyklé nastavení práv u spustitelných souborů (měnit může jen vlastník, spouštět mohou všichni) nebo u všeobecně dostupných adresářů.
`rw-rw-r–`	664	u=rw,g=rw,o=r	Obvyklé nastavení obyčejných souborů (texty a podobně).
`rwx——`	600	u=rwx,g=,o=	Obvyklé pro domácí adresář, kam může jen jeho vlastník.

Alternativní metody řízení přístupových práv

V Linuxu lze přiřazovat práva i pomocí tzv. access listů (ACL), kdy lze přiřazovat práva jemnějším způsobem, než to umožňuje výše popsaný standardní způsob (pro každý soubor a adresář lze vytvořit seznam uživatelů a skupin, které mají přesně specifikovaná přístupová práva). Protože je však tato vlastnost nadstandardní (tj. není zahrnuta ve standardním jádře Linuxu), doporučujeme, abyste se informovali u tvůrce distribuce, kterou používáte.

Síťování v Linuxu

Linux byl od počátku na Internetu, a proto jsou počítačové sítě jeho domácím prostředím. Výborně se hodí jako WWW server, router, poštovní server, FTP server, DNS server, SQL server, firewall a mohli bychom pokračovat ještě dlouho. Jeho přirozeným protokolem, pomocí kterého dokáže komunikovat se svými sousedy, je TCP/IP. Tento protokol dnes vstupuje i do lokálních sítí a stává se tak univerzálním komunikačním nástrojem.

Síťová rozhraní

Máme-li v počítači s Linuxem síťovou kartu, pak o ní mluvíme jako o síťovém rozhraní. Síťové rozhraní nemusí být jen fyzické zařízení, ale může být i virtuální. Mezi virtuální počítáme například tzv. loopback, o kterém bude ještě řeč, nebo aliasy (přezdívky), které umožňují přiřadit jednomu síťovému rozhraní více různých IP adres.

Síťová rozhraní jsou v Linuxu pojmenována zkratkou, za kterou následuje číslo. Číslo značí pořadí, v jakém bylo rozhraní v systému detekováno, takže pokud máme v systému několik ethernetových síťových karet, budou označeny postupně názvy *eth0*, *eth1*, *eth2* atd. Přítomnost síťových zařízení se dá nejjednodušeji zjistit výpisem souboru `/proc/net/dev` (příkazem `cat /proc/net/dev`). V tomto souboru nám jádro systému oznamuje, která síťová zařízení zná. Trvale přítomno je zde zařízení pro loopback, které se označuje zkratkou *lo*. Loopback je povinné zařízení pro všechny implementace protokolu TCP/IP a přiděluje se mu (obvykle automaticky) adresa 127.0.0.1 a maska 255.0.0.0.

V případě, že v počítači máte síťovou kartu, a přesto ji v seznamu síťových zařízení nevidíte, znamená to, že jádro Linuxu kartu nerozpoznalo. Obvykle je to způsobeno tím, že jádra jsou v distribucích kompilována co nejmenší a všechny ovladače jsou k dispozici jako moduly, které zavádíme za běhu systému jen v případě potřeby. Moduly nalezneme v adresáři `/lib/modules`, kde jsou systematicky rozčleněny do adresářů podle verze používaného jádra a podle jejich typu. Každý modul slouží k ovládání jednoho nebo několika podobných zařízení. Seznam zařízení podporovaných Linuxem by byl velmi dlouhý a mění se podle verze použitého jádra. Proto v tabulce najdete jen seznam nečastěji používaných modulů pro běžné síťové karty. Kompletní seznam naleznete v dokumentaci své distribuce.

Tabulka 6.4: Nejčastěji používané moduly pro síťové karty

Jméno modulu	Parametry	Podporované síťové karty
ne	io, irq	NE2000 a kompatibilní (ISA)
3c59x		3Com900, 905, 595, …
ne2k-pci		NE2000 a kompatibilní (PCI)
8139too		RealTek RTL8129, RealTek RTL8139, SMC1211TX, …

Některé moduly potřebují při zavádění do paměti doplňující informace o zařízení, které v počítači máte. Týká se to zejména zařízení umístěných na sběrnici ISA, protože je nelze bezpečným způsobem automaticky detekovat. Protikladem jsou zařízení používající sběrnici PCI, kde lze všechny podstatné informace snadno zjistit, a tak si je moduly mohou snadno přečíst. Informace o zařízeních na PCI sběrnici si můžete pro orientaci snadno vypsat příkazem `lspci`.

Při ručním zavádění modulů do paměti (hodí se zejména pro testování) se používá příkaz `modprobe`, pro výpis zavedených modulů slouží příkaz `lsmod` a pro odstranění modulu z paměti pak příkaz `rmmod` (pokud je zařízení používáno, nelze modul odstranit, zařízení je potřeba nejprve deaktivovat příkazem `ifconfig eth0 down`).

Jako příklad si uveďme zavedení modulu pro klasickou ethernetovou síťovou kartu ISA (NE2000 kompatibilní). Předpokládejme, že je nastavena na přerušení 10 a port 300. Modul, který dokáže ovládat všechny NE2000 kompatibilní karty, se jmenuje *ne*. Tomuto modulu stačí předat číslo portu, přerušení si zjistí sám, takže jeho zavedení do paměti by mohlo vypadat třeba takto:

```
modprobe ne io=0x300
```

Správnou detekci síťové karty ověříme vypsáním souboru `/proc/net/dev`, případně pomocí příkazu `dmesg`, který vypíše poslední hlášení jádra Linuxu na obrazovku. V Linuxu není potřeba zavádět moduly ručně, jádro si je umí zavést automaticky. Je však potřeba určit vazbu mezi jménem zařízení a modulem, který slouží k jeho ovládání. V případě, že bychom chtěli mít výše uvedenou síťovou kartu v počítači jako zařízení *eth0*, bylo by potřeba doplnit do souboru `/etc/modules.conf` následující řádky (od tohoto okamžiku bude při pokusu o nastavení rozhraní *eth0* automaticky zaveden modul *ne* s parametrem tak, jak je uvedeno výše):

```
alias eth0 ne
options ne io=0x300
```

Konfigurace sítě

Síťová rozhraní, která mají komunikovat protokolem TCP/IP, musíme správně nakonfigurovat. Nejprve však potřebujeme vědět několik důležitých údajů (IP adresu, masku sítě, bránu a adresu DNS serveru). Všechny nám sdělí administrátor vaší sítě, protože je nelze volit libovolně. Je také možné, že jsou tyto informace předávány stanicím automaticky pomocí protokolu DHCP, a v tom případě si je Linux při startu zjistí sám. Spustíme si konfigurační nástroj, který je dodáván s naší distribucí (v distibuci Red Hat je to `linuxconf`), najdeme sekci o síťových rozhraních, a zaškrtneme volbu automatické konfigurace nebo pečlivě vyplníme vše ručně.

V následujícím textu předpokládáme, že odpovídající nastavení systému chceme provést ručně, zkontrolovat ho nebo najít chybu. Celý naznačený postup je možné vynechat, pokud jsou příslušné informace vyplněny v přehledném konfiguračním nástroji distribuce, protože systém po startu provede všechna příslušná nastavení podle zadaných údajů sám.

Síťová rozhraní lze nastavit příkazem `ifconfig`. Zkusíme-li tento příkaz použít samotný bez doplňujících parametrů, vypíše přehled již nastavených síťových rozhraní a jejich parametry. Pomocí příkazu `route` (resp. `route -n`, pokud není DNS zcela funkční nebo pokud chceme místo jmen počítačů vidět přímo IP adresy) lze zobrazit aktuální směrovací tabulku. Vše lze měnit za provozu systému bez nutnosti jeho restartu.

Předpokládejme, že máme v počítači síťovou kartu, která má mít adresu 10.0.0.7 s maskou 255.255.255.0 a brána má adresu 10.0.0.1. Nastavení sítě lze pak provést příkazy:

```
ifconfig lo 127.0.0.1 netmask 255.0.0.0 broadcast 127.255.255.255
ifconfig eth0 10.0.0.7 netmask 255.255.255.0 broadcast 10.0.0.255
route add default gw 10.0.0.1
```

Všimněte si prvního řádku, kde se nastavuje speciální rozhraní *lo* (loopback), které je povinnou součástí implementace TCP/IP protokolu. Toto rozhraní ukazuje vždy na náš vlastní počítač. Loopback je smyčka, a pokusíme-li se s touto adresou spojit, připojíme se vždy ke stejnému systému, na kterém pracujeme.

Deaktivace síťového rozhraní se provádí příkazem `ifconfig eth0 down` (resp. `ifconfig lo down`). Současně s deaktivací rozhraní jsou odstraněny i příslušné záznamy ze směrovací tabulky. Konvence a syntaxe zápisu jednotlivých příkazů je prakticky stejná jako na jiných Unixech, takže kromě dokumentace k Linuxu lze doporučit i studium jakékoliv další příbuzné literatury.

Abychom při práci mohli místo IP adres používat jména počítačů, je potřeba nastavit DNS. Pro jeho správnou funkci je potřeba ověřit, zda máme správně nastaveny údaje v několika souborech. Základním souborem pro převod jmen na IP adresy je soubor `/etc/hosts`, ve kterém můžeme vyjmenovat IP adresy a k nim přiřadit libovolná jména. Linux je obvykle nastaven tak, že tento soubor má při převodu jmen na IP adresu přednost. Lze zde tedy předdefinovat převod jmen na konkrétní IP adresy, ovšem musíme dát pozor, aby správce nezměnil IP adresu zde uvedeného počítače. V takovém případě by se náš počítač pokoušel připojit na již neexistující IP adresu. Proto je v souboru `/etc/hosts` obvykle jen velmi málo údajů. Jeho větší využití může nastat v případě, že nechceme provozovat v uzavřené síti DNS servery, ovšem v takovém případě budeme muset do tohoto souboru vyjmenovat všechna používaná jména počítačů, přiřadit k nim IP adresy a nakopírovat takový soubor do všech počítačů v síti (Windows tento soubor používají také, nachází se obvykle v C:\WINDOWS\HOSTS).

Do souboru `/etc/hosts` se vkládají vždy alespoň dva záznamy. Jde o adresu zařízení loopback a o vlastní IP adresu počítače. Soubor by mohl vypadat třeba takto:

```
127.0.0.1       localhost
10.0.0.7        monkey.mojedomena.cz monkey
```

V prvním sloupci je uvedena IP adresa, následuje plné jméno počítače včetně domény a dále jsou uvedena zkrácená jména počítače, která jsou oddělena mezerami. Nenajde-li se IP adresa v tomto souboru, snaží se systém provést převod jména na IP adresu dalším dostupným způsobem, což je obvykle dotaz na DNS server.

IP adresu DNS serveru je potřeba uvést v souboru `/etc/resolv.conf`. V tomto souboru je na začátku řádku klíčové slovo, mezera a pak příslušná hodnota. Nejčastěji jsou používány záznamy *nameserver*, *domain* a *search*. Klíčové slovo *nameserver* definuje IP adresu DNS serveru. Pokud chceme uvést více DNS serverů, je potřeba zadat více záznamů po jednom na každý řádek. Další záznam je *domain*, který určuje doménu, ve které se počítač nachází. Posledním záznamem je *search*, který umožňuje předdefinovat seznam domén, ve kterém se bude příslušné jméno počítače hledat. Pokud zadané jméno počítače nelze převést na IP adresu, jsou k němu postupně přidávány zá-

znamy z direktivy *search* (lze nadefinovat až 16 domén oddělených navzájem mezerami). Pokud tato volba chybí, je použita jen doména určená klíčovým slovem *domain*. Soubor `/etc/resolv.conf` by mohl vypadat třeba takto:

```
domain mojedomena.cz
search mojedomena.cz jinadomena.cz
nameserver 10.0.0.1
```

V příkladu je nadefinován jediný DNS server s IP adresou 10.0.0.1, doména počítače je *mojedomena.cz*. Pokud uživatel zadá jméno počítače, které nepůjde přímo převést (tj. zadá jméno bez domény), přidá se k němu nejprve *mojedomena.cz,* a pokud se opět převod nepovede, zkusí se ještě přidat doména *jinadomena.cz*. Když se převod nepovede ani zde, bude ohlášena chyba. Je-li seznam příliš dlouhý, může převod nebo oznámení chyby trvat velmi dlouho, a proto obvykle obsahuje nejvýše dvě domény.

Posledním souborem je `/etc/nsswitch.conf`, který na řádku začínajícím klíčovým slovem *hosts:* definuje pořadí, ve kterém se bude převod odehrávat. Standardní záznam (soubor obsahuje mnoho dalších direktiv) je obvykle:

```
hosts:  files dns
```

Tento záznam předepisuje, že převod se provede nejprve podle souboru `/etc/hosts` a v případě, že tento pokus selže (jméno nebude v souboru uvedeno), provede se dotaz na DNS server (podle údajů v souboru `/etc/resolv.conf`).

Ověřování funkčnosti síťové komunikace

Pokud chceme ověřit, že Linux komunikuje se svým síťovým okolím, je potřeba nejprve vizuálně zkontrolovat připojení do počítačové sítě. Kromě připojeného kabelu bychom měli vidět na síťové kartě nebo na zařízení, do kterého je počítač připojen, svítit signalizační diody (obvykle zelené barvy na znamení, že spojení je funkční). Dále ověříme správné nastavení IP adres pomocí příkazu `ifconfig` a správnost záznamů ve směrovací tabulce pomocí příkazu `route` (resp. `route -n`, nepotřebujeme-li převod IP adres na jména počítačů).

Dalším krokem je první pokus o vyslání IP datagramu z počítače ven a čekání, zda přijde odpověď. K tomu slouží příkaz `ping`, který vysílá k zadanému počítači žádosti o odpověď (tj. něco na způsob otázky: „Žiješ?“ a následné odpovědi „Ano, žiju.“). Kromě prostého zobrazování došlých odpovědí příkaz `ping` zobrazuje i dobu odezvy a na závěr i statistické údaje (počet ztracených odpovědí, minimální, maximální a průměrná doba odezvy). Pinkání na sousední počítač je nejprostší způsob ověření funkčnosti síťového subsystému a spojení s okolními počítači. Příklad použití příkazu `ping` je uveden níže (všimněte si, že místo jména počítače je použita IP adresa našeho přímého souseda, tj. počítače ve stejné síti; provádění příkazu bylo přerušeno pomocí kombinace kláves CTRL+c):

```
$ ping -n 10.0.0.8
PING 10.0.0.8 (10.0.0.8) from 10.0.0.7 : 56(84) bytes of data.
64 bytes from 10.0.0.8 (10.0.0.8): icmp_seq=0 ttl=255 time=284 usec
64 bytes from 10.0.0.8 (10.0.0.8): icmp_seq=1 ttl=255 time=269 usec
64 bytes from 10.0.0.8 (10.0.0.8): icmp_seq=2 ttl=255 time=283 usec
64 bytes from 10.0.0.8 (10.0.0.8): icmp_seq=3 ttl=255 time=293 usec
```

```
—- 10.0.0.8 ping statistics —-
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.269/0.282/0.293/0.014 ms
```

Stejně jako u příkazu `route` lze použít přepínač `-n`, který zakáže převod IP adres na jména počítačů. Někdy se používá ještě parametr `-s 1440`, který zajistí vyslání delších datagramů, než je obvyklé. Tak můžeme lépe otestovat kvalitu své sítě a schopnost přenášet i delší zprávy (např. při použití bezdrátového spojení).

Dalším užitečným nástrojem je příkaz `traceroute`, který zobrazuje všechny směrovače (routery) na cestě k cílovému počítači. Proto se mu jako parametr obvykle zadává nějaký vzdálenější počítač, abychom mohli zjistit, kam až naše spojení se světem funguje (resp. kudy jednotlivé datagramy cestují). V následujícím příkladu je vidět cesta k počítači s IP adresou 10.0.1.1, který leží v sousední síti za směrovačem s IP adresou 10.0.0.1 (tj. za bránou, přes kterou směrujeme provoz):

```
$ traceroute -n 10.0.1.1
traceroute to 10.0.1.1 (10.0.1.1), 30 hops max, 38 byte packets
 1  10.0.0.1  0.227 ms  0.154 ms  0.153 ms
 2  10.0.1.1  1.945 ms  2.066 ms  2.115 ms
```

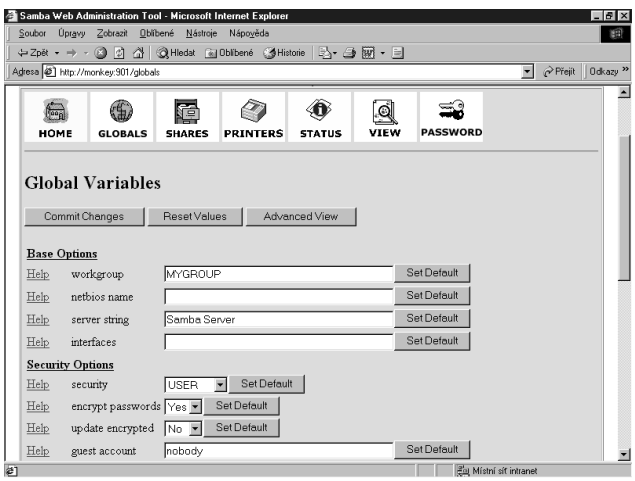
Sdílení souborů v sítích Windows – Samba

V prostředí Unixových systémů se soubory sdílí pomocí NFS (Network FileSystem). Tento způsob však není obvyklý pro klasické počítače PC, na kterých převládá operační systém MS Windows. Mezi těmito počítači se používá tzv. Sdílení v sítích Microsoft, které používá SMB protokol. Z této zkratky vychází název Samba, což je název projektu, který umožňuje sdílet soubory umístěné na Linuxovém serveru takovým způsobem, jako by na něm běžel systém MS Windows. Emulace sdílení není úplná, ale všechny nejběžnější funkce jsou dnes již podporovány (přihlašování do domény, log-on skripty, přidělování práv na sdílené adresáře a soubory, tisk do síťové tiskárny atd.).

Samba je součástí každé větší distribuce a jedná se o velmi propracovaný projekt. Jeho vývoj je velmi živý a každou chvíli jsou do něj doplňovány další možnosti a novinky. Stránky projektu naleznete na adrese *http://www.samba.org/*. Na této adrese najdete odkazy na dokumentaci i na příbuzné projekty. Pro čtenáře bude asi nejlepší odkaz na knihu **Robert Eckstein: Samba Linux jako server v sítích s Windows**, kterou vydal Computer Press.

Konfigurace Samby

Nastavení Samby je uloženo v souboru `/etc/samba/smb.conf`. Protože jeho ruční upravování je poměrně nepohodlné, je k dispozici i nástroj Swat, který umožňuje Sambu nastavovat pomocí prohlížeče WWW. Ukázku WWW stránky při konfiguraci Samby si můžete prohlédnout v následujícím obrázku.



Obrázek 6.4: *Ovládání Samby pomocí WWW rozhraní (Swat)*

Zprovoznění programu Swat

Program Swat je potřeba před použitím nastavit tak, aby přijímal síťová spojení. Standardně je spouštěn síťovým superserverem *inetd*, resp. *xinetd*. Všechny následující kroky se budou vztahovat k distribuci Red Hat verze 7.1. U jiných distribucí bude posloupnost kroků prakticky stejná, rozdíly budou způsobeny jen jejich vzájemnými odlišnostmi v umístění konfiguračních souborů nebo použitými komponentami.

1. Povolíme službu *swat* a *xinetd*, nejsnadněji pomocí nástroje `ntsysv`, tj. spustíme démona *xinetd* a v jeho nastavení povolíme službu *swat* (při příchodu spojení na port 901 démon *xinetd* předá řízení programu *swat*).
2. V případě, že budeme chtít komunikovat s programem Swat z jiného počítače, zakomentujeme v souboru `/etc/xinetd.d/swat` řádek, na kterém se vyskytuje klíčové slovo *only_from* (tj. na začátek tohoto řádku napíšeme znak křížek – #). Tento způsob přístupu je poměrně nebezpečný, protože po síti se bude pohybovat nezašifrované heslo, které si může prakticky kdokoliv odposlechnout. Lepší je přistupovat k nástroji Swat ze stejného počítače, na kterém je sám umístěn, heslo pak odposlechnout nelze.
3. Přikážeme démonovi *xinetd* znovu načíst konfigurační soubor: `/etc/init.d/xinetd reload`.
4. Spustíme si prohlížeč, do kterého napíšeme jméno počítače s programem Swat a do adresy doplníme za dvojtečku číslo portu 901, tj. například: *http://monkey:901*.
5. Autorizujeme se do programu Swat jako administrátor systému (tj. uživatel root).

Základní nastavení Samby

Samba komunikuje s klientskými stanicemi pomocí protokolu TCP/IP, takže základním předpokladem je, aby nám TCP/IP v lokální síti fungovalo. Dále s musíme rozhodnout, zda se má Samba chovat spíše jako stanice s Windows 95 (resp. Windows 98 nebo Windows ME) nebo spíše jako stanice s Windows NT (resp. Windows 2000 nebo Windows XP).

Pokud chceme Sambu používat, jako kdyby to byla stanice s MS Windows 9x, kdy je přístup k jednotlivým nabízeným prostředkům (sdílené disky nebo tiskárny) rozlišován pouze na základě hesla, nastavíme Sambu do režimu *security=share*.

V případě, že chceme na Linuxu založit stejné účty, jaké budou sloužit pro přihlašování ke stanicím s MS Windows, pak je k dispozici režim *security=user*. Práva na sdílené soubory pak budou přímo vyplývat z práv, která má k daným souborům uživatel v Linuxu. V tomto režimu lze Sambu provozovat i jako PDC (Primary Domain Controller), kdy se uživatelé přihlašují do domény a jejich přihlašovací jména a hesla se ověřují proti serveru, na kterém je Samba spuštěna. Při přihlašování do domény lze používat přihlašovací skripty, profily a na server lze také ukládat uživatelská nastavení (stejně jako při přihlašování do domény vedené na serveru s Windows NT).

Pokud máme účty uživatelů v síti již zavedeny (např. na jiném Windows NT serveru nebo na jiné Sambě), pak použijeme režim *security=server*. V tomto případě bude Samba provádět autorizaci přístupu proti serveru, který uvedeme v položce *password server*.

Pokud máte uživatelské účty již vedeny v NT doméně, pak je k dispozici volba *security=domain*, kdy Samba provádí autorizaci přístupu proti uživatelům vedeným v doméně (provozované na jiném počítači).

Hesla při používání Samby

Teprve od verze MS Windows 95 OSR 2 a MS Windows NT 4.0 SP 3 jsou při přenosu po síti hesla šifrována. Pokud ve svojí lokální síti používáte stanice se staršími verzemi Windows, doporučujeme jejich upgrade. Pokud upgrade není možný, je nutné Sambu přesvědčit, že má používat nešifrovaná hesla pro komunikaci se všemi klienty (stejně jako kdyby server byla např. stanice s MS Windows 2000). K tomu slouží volba *encrypt passwords*, kterou nastavte na

„*no*“. Najdete ji v globální sekci konfigurace Samby (při tomto nastavení musí být i uživatelské stanice nastaveny pro používání nešifrovaných hesel).

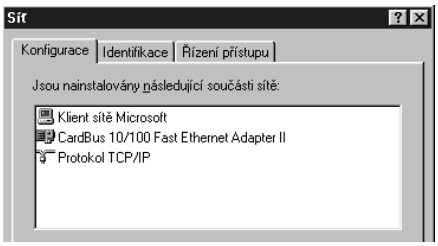
V případě, že chcete používat šifrovaná hesla (je to bezpečnější), je potřeba nastavit v Sambě cestu k souboru s hesly (volba *smb passwd file*). Hesla pro přihlašování se pak v Linuxu nastavují pomocí příkazu smbpasswd. Při prvním použití je potřeba uživatele do tohoto souboru přidat, k čemuž slouží parametr –a. Má-li uživatel René Hužva v Linuxu účet huzva, nastavíme mu pro přihlašování do Samby heslo pomocí příkazu:

```
smbpasswd -a huzva
```

Heslo je potřeba zadat dvakrát, podruhé pro kontrolu. Od této chvíle se může René přihlašovat k Sambě pomocí přihlašovacího jména huzva a výše zadaného hesla. Heslo do Linuxu je uloženo na jiném místě, a proto mohou být hesla různá. Není to však příliš praktické, a tak jsou obvykle hesla nastavena stejně. Je-li v konfiguraci Samby zapnuta volba *unix password sync* a uživatel si heslo změní (buď v Linuxu příkazem `smbpasswd` nebo ze stanice s MS Windows), jsou obě hesla automaticky nastavena stejně.

Konfigurace klienta

Chceme-li se ze stanice s MS Windows připojovat k Sambě, aktivujeme na ní Klienta sítě Microsoft. Je také potřeba přidat protokol TCP/IP, protože Samba pomocí něho se stanicí komunikuje. U protokolu TCP/IP nastavíme IP adresu, bránu a případně také adresu DNS serveru. Standardní konfiguraci sítě v MS Windows 9x ukazuje následující obrázek, ve kterém můžete vidět kromě zmíněného klienta a protokolu ještě ovladač síťové karty.



Obrázek 6.5: *Konfigurace Windows 9x pro připojení k Sambě*

Linux jako klient sítě Microsoft

Linux si dokáže připojit vzdálené disky, které jsou sdíleny pomocí SMB protokolu. Mohou to být sdílené adresáře na stanicích s Windows, ale i na jiných Linuxech se spuštěnou Sambou (ovšem v tomto případě by bylo lepší využít nativní sdílení pomocí NFS nebo jiných protokolů, které jsou Unixům bližší).

Pro připojení sdíleného adresáře používáme příkaz `mount`. Doplňující údaje potřebné pro připojení se zadávají jako parametry. Nejčastěji používané volby jsou shrnuty v tabulce:

Tabulka 6.5: Volby pro připojení sdílených disků k Linuxu

Volba	Význam
username=	Uživatelské jméno, pod kterým se bude provádět autentizace
password=	Heslo připojovaného uživatele
ip=	IP adresa počítače, ke kterému se připojujeme (pokud ji nelze zjistit ze jména počítače)
ro	Připojit jen pro čtení (read-only)
rw	Připojit pro zápis (read-write)
guest	Připojit bez dotazu na heslo (jako anonymní uživatel, host)

Pokud bychom si chtěli připojit disk z počítače Monkey, který je sdílen pod názvem CD-ROM a heslem tramvaj do adresáře `/mnt/cd-rom-monkey`, pak bychom použili příkaz:

```
mount -t smbfs -o password=tramvaj //monkey/cd-rom /mnt/cd-rom-monkey
```

Pro výpis nabízených sílených prostředků můžeme použít příkaz `smbclient -L monkey`. Pokud je nutné uvést jméno uživatele (např. při dotazu na stanici s Windows NT), použijeme navíc parametr –U jméno. Podobným způsobem lze parametrem –I adresa uvést IP adresu, např. tedy:

```
smbclient -U huzva -I 10.0.0.8 -L monkey
```

Podobně jako v prostředí MS Windows lze i v grafických prostředích používaných při práci v Linuxu procházet okolní počítače a připojovat sdílené disky pomocí myši. Všechny zde uvedené příklady slouží jako vzorové příklady, které budou fungovat vždy.

Sdílení souborů v sítích Novell NetWare

Linux se může v síti tvářit i jako server Novell NetWare pomocí programu Mars_NWE (MArtin Stover NetWare Emulator). Bohužel kvalita je velmi nízká, posledních několik let se již tento program nevyvíjí a obsahuje několik nepříjemných nedostatků, takže ho nelze doporučit. Samba dosahuje mnohem vyšších kvalit a navíc se velmi dynamicky rozvíjí, proto nebudeme tuto možnost dále podrobněji rozebírat.

Potřebujeme-li si v Linuxu připojit sdílené disky ze serveru Novell NetWare, je to možné jak pomocí protokolu IPX, tak pomocí protokolu TCP/IP (záleží na tom, jak je nakonfigurován NetWare server). V případě, že je serverem podporován výhradně protokol IPX, je nutné tento protokol nastavit i na síťovém rozhraní Linuxu. Nastavení je možné ponechat na automatické detekci rámce, která však může selhat v prostředí se spuštěnými stanicemi Windows, nebo lze všechny hodnoty ručně zadat do konfiguračního programu pro nastavení sítě v Linuxu. Typ rámce a číslo sítě se musí shodovat s nastavením na NetWare serveru.

Aktivace automatické detekce rámce a čísla sítě se provádí příkazem:

```
ipx_configure –auto_interface=on –auto_primary=on
```

Zjištěné hodnoty můžeme zjistit buď přímo výpisem souboru `/proc/net/ipx_interface`, nebo na výstupu programu `ifconfig`. Automatická detekce může trvat několik desítek vteřin a její možný výsledek je vidět v následujícím příkladu, kde byl na síťovém rozhraní *eth0* nastaven rámec 802.3 pro síť 13 a rámec Ethernet II pro síť číslo 12 (na jednom segmentu může být IPX přepravován v různých rámcích, avšak vždy s různými a nenulovými čísly sítí).

```
monkey:~> cat /proc/net/ipx_interface
Network     Node_Address    Primary   Device      Frame_Type
00000012    00A024D6F9F9    Yes       eth0        EtherII
00000013    00A024D6F9F9    No        eth0        802.3
```

Stejné hodnoty, jaké jsou uvedeny výše, lze nastavit příkazy:

```
ipx_interface add -p eth0 etherii 12
ipx_interface add    eth0 802.3   13
```

Funkčnost ověříme například výpisem dostupných NetWare serverů pomocí příkazu `slist`:

```
monkey:~> slist
Known NetWare File Servers      Network    Node Address
-------------------------------------------------------
PRUM                              0003333    000000000001
```

Připojování sdílených disků ze serveru Novell NetWare se provádí pomocí příkazu `ncpmount` (odpojení pak příkazem `ncpumount`). Pomocí parametru –S určujeme jméno serveru, ke kterému se připojujeme, parametrem –U pak uživatelské jméno a jako poslední je uveden adresář, do kterého se mají sílené disky připojit:

```
ncpmount -U huzva -S projekce /mnt/projekce
```

Firewall a další pokročilé možnosti Linuxu

Linux má přímo v jádře zabudovaný velmi kvalitní datagramový firewall, který je schopen podle různých kritérií propouštět, odmítat nebo zahazovat jednotlivé datagramy, které po síti přicházejí. To z něj činí velmi robusní systém, který lze použít pro ochranu počítačových sítí, které jsou jeho prostřednictvím připojeny k Internetu. V posledních jádrech je i základní podpora pro stavový firewall, který dokáže rozhodovat o zpracování datagramu i podle toho, co přišlo dříve (tj. pravidla se mění podle vývoje situace).

Linux dokáže zajistit i NAT (Network Address Translation). Lze použít statické přepisování hlaviček datagramů (1:1, tzv. portforwardig) nebo i dynamické (1:N, N:M), kdy je možné pomocí několika veřejných IP adres zprostředkovat připojení mnoha počítačů k Internetu bez toho, abychom potřebovali pro každý z nich zvláštní IP adresu (tzv. masquerade).

Konfigurace firewallu vyžaduje podrobnější znalosti protokolu TCP/IP a mechanismů zpracování IP datagramů v jádře Linuxu. Proto ho zde jen zmíníme, přestože existují i příjemné a jednoduché grafické nástroje, které konfiguraci jednoduchých firewallů přibližují i amatérům. Stále totiž platí, že opravdu bezpečný firewall, který má chránit větší množství počítačů, by měl nastavovat profesionál.

Pomocí NAT lze vybudovat tzv. „transparentní proxy“. Proxy cache umožňuje ukládat průchozí data na pevný disk a při opakovaném požadavku klienta (např. prohlížeče WWW) poskytne tato uložená data místo toho, aby byla opakovaně přenášena ze vzdáleného počítače. Proxy tak šetří přenosovou kapacitu linek, kterými je síť připojena k Internetu. Její nevýhodou je, že proxy cache musí být v prohlížeči správně nastavena. Existují sice možnosti automatické konfigurace, ale ani tak se na ně nelze spolehnout. Transparentní proxy tyto nedostatky odstraňuje tak, že se postaví prohlížeči do cesty k Internetu a pomocí manipulace s datagramy bude do ní přesměrován veškerý odchozí provoz (tj. v našem případě veškerá komunikace prohlížečů s WWW servery) bez toho, aby o tom prohlížeč věděl. Zajistíme tak, že veškerá komunikace s WWW servery (na standardním portu 80) bude procházet skrz transparentní proxy. Nevýhodou tohoto přístupu je, že je potřeba vytvořit seznam WWW adres, pro které se proxy používat nebude. Důvodem je například vazba placených služeb na pevnou adresu nebo nevhodně napsaná obsluha dynamických WWW stránek (resp. skriptů, které je generují).

Nastavení transparentní proxy vyžaduje úpravu síťové konfigurace firewallu (firewall je poměrně vhodné místo pro její umístění) a podporu příslušného programu zajišťujícího samotnou proxy. Nastavení je celkem jednoduché, ale je závislé na použitých prostředcích. Proto odkazujeme na dokumentaci, kde naleznete podrobnější informace (např. proxy cache Squid má problematiku ve své dokumentaci podrobně popsánu).

Mezi další pokročilé možnosti lze počítat i QoS (Quality of Service), čímž souhrnně označujeme vše, co umožňuje ovlivňovat předávání datagramů mezi jednotlivým počítači. QoS umožňuje, aby některé datagramy „předbíhaly“ nebo naopak byly zdrženy. Cílem je poskytnou některým službám nebo uživatelům nadstandardní služby, např. rychlejší přenos dat nebo zaručit minimální datovou propustnost sdílené linky a zároveň neplýtvat její kapacitou (tj. „půjčovat“ dočasně nevyužitou část kapacity těm, kteří ji zrovna potřebují).

Dokumentace

K Linuxu existuje velké množství dokumentace, která je na Internetu volně k dispozici. Největším projektem je LDP (Linux Documentation Project, *http://linuxdoc.org/*). Jeho nejrozsáhlejší částí jsou tzv. HOWTO čili dokumenty, které kromě popisu problémů a technologií obsahují i návody, jak je řešit. V rámci LDP jsou k dispozici i knihy (Network Administrators Guide, Securing and Optimizing Linux, atd.).

Dalším tradičním zdrojem informací jsou manuálové stránky, které jsou k dispozici přímo v běžícím systému. Pokud budeme chtít například nápovědu pro příkaz `cp`, stačí na příkazové řádce napsat:

```
man cp
```

Prohlížení manuálové stránky se ukončuje stiskem klávesy *q* (quit), k posunu textu dopředu a dozadu slouží klávesy mezerník a klávesa *b* (back). K pohybu lze použít i šipky, další nápovědu získáme stiskem klávesy *h* (help). Některé manuálové stránky jsou přeloženy i do češtiny a jsou obvykle standardní součástí všech větších distribucí.

Protože jsou manuálové stránky již dnes považovány za zastaralý systém pro prezentování dokumentace, je k dispozici nový systém Info, ve kterém lze provázat text pomocí hypertextových odkazů (tj. systém odkazů, který známe z WWW stránek). Pro prohlížení dokumentace ve formátu Info lze použít příkaz `info`, který má však poměrně nestandardní ovládání. Místo něho proto někteří uživatelé dávají přednost programu `pinfo`. Jak manuálové stránky, tak dokumentaci Info lze snadno prohlížet v integrovaných prohlížečích nápovědy, které jsou k dispozici v různých grafických prostředích.

Každý program má navíc doplňující informace umístěné pod svým jménem v adresáři `/usr/share/doc`, tj. například Samba ji má v adresáři `/usr/share/doc/samba-2.0.10` (číslo vyjadřuje verzi programu).

Kromě těchto nejrozsáhlejších zdrojů nápovědy je potřeba ještě zmínit diskusní skupiny NetNews (v českém jazyce *cz.comp.linux*) a elektronické konference (*linux@linux.cz*, viz *http://www.linux.cz*). Mnoho informací lze získat na běžných internetových stránkách, jejichž přehled je uveden v následující tabulce.

Tabulka 6.6: Přehled stránek informujících o Linuxu

Adresa	popis
http://www.linux.org	mezinárodní vstupní brána do světa Linuxu
http://www.linux.cz	české stránky o Linuxu
http://www.penguin.cz	server hostující několik různých projektů
http://www.ll.cz	seznam odkazů na různé stránky o Linuxu (Linux Links)

Rejstřík