1. Hardware sítí

# Kabeláž

Koaxiální kabel – nejstarší druh kabelu; základem je měděný vodič, který je obalen plastovou izolací, tato izolace je opletena stíněním. Vše je pak vloženo do vnějšího izolačně – mechanického obalu z plastu. Existují dva druhy koaxiálního kabelu – liší se elektrickými a mechanickými vlastnostmi. Typické je použití sběrnicové topologie.

Rychlost přenášených dat je až 10 Mb/s.

**1. Tlustý koaxiální kabel:**

- nejstarší druh kabelu, dnes je velmi málo používán

- 10 mm tlustý, žluté barvy

- dobré elektrické vlastnosti

- používal se pro páteřní vedení (spojení jednotlivých sítí)

Nevýhody: tloušťka kabelu (potíže při montáži), způsob připojení kabelu ke stanici

**2. Tenký koaxiální kabel:**

- standard kabeláží lokálních sítí (dnes se s ním setkáme u starších sítí)

- 5 mm tloušťka, červená nebo šedá barva

- snadněji se instaluje, ale má horší vlastnosti než tlustý koax. => kratší síťové segmenty

Kroucená dvojlinka – je odvozena od telefonního kabelu, dnes je nejrozšířenější v síti LAN. El. signál je náchylný na rušení. Ochrana spočívá v kroucení. Oba vodiče, jimiž se signál přenáší, se pravidelně střídají (vzájemné kroucení)=> ruší se možnosti vlivu jednoho vodiče na druhý. Typická pro hvězdicovou topologii.

Nejčastěji se používá kategorie 5, která obsahuje 4 páry vodičů (100 Mb/s).

**1. Nestíněná kroucená dvojlinka (UTP):**

- jednotlivé páry jsou vloženy do vnější plast. izolace – nejpoužívanější v LAN

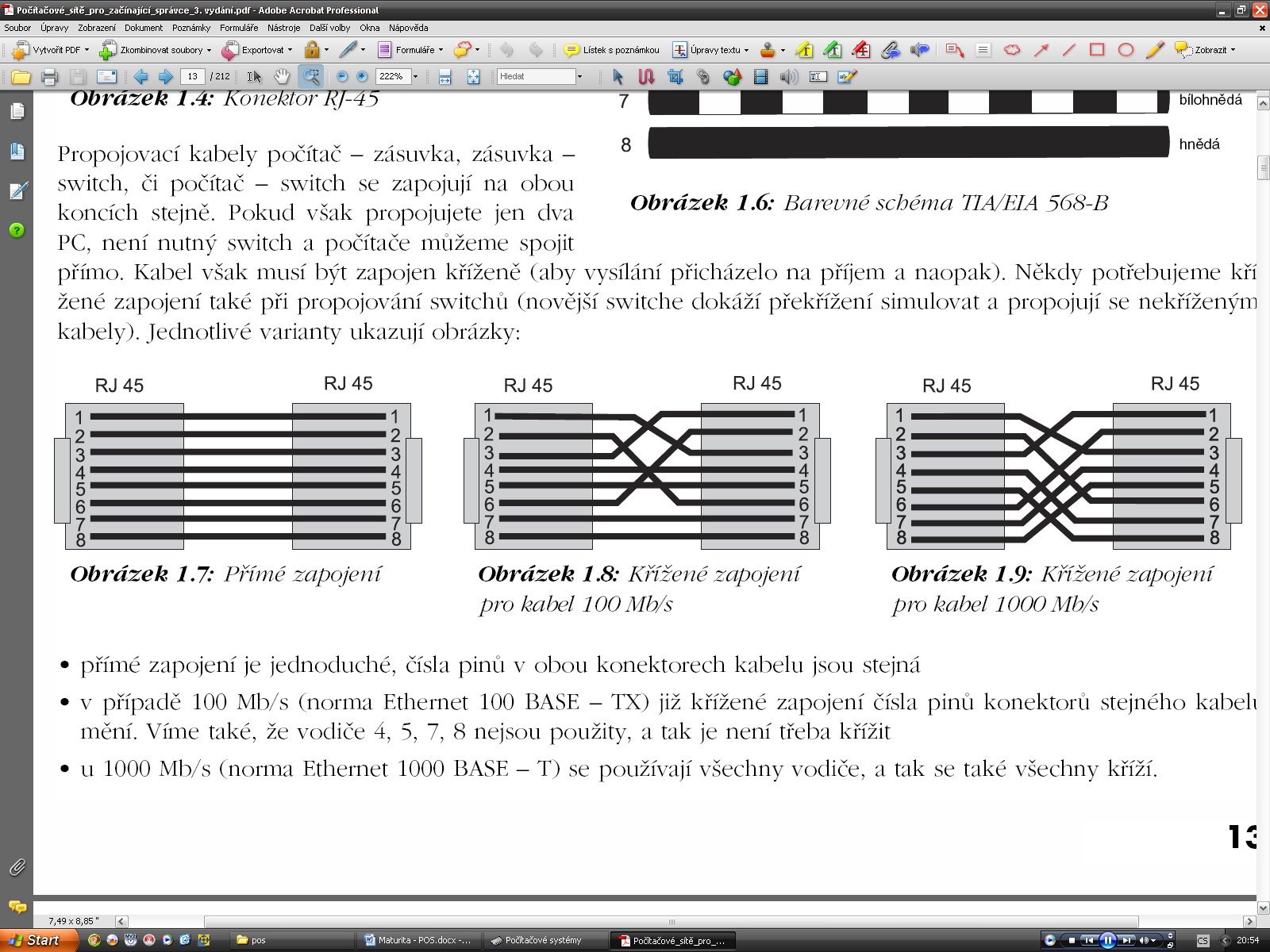
**2. Stíněná kroucená dvojlinka:**

- má kovové opletení => zvyšuje ochranu proti rušení

- dražší než nestíněný kabel a používá se jen tam, kde k vnějšímu rušení

dochází

Tabulka zapojení kroucené dvojlinky – Počítačové sítě – str. 6

**Kabel kategorie 5e**

* hlavní použití je v sítích gigabitového ethernetu
* maximální teoretická rychlost 1 000 Mbps

### Optický kabel

– data jsou přenášena světelnými impulsy v průsvitných vláknech

Základní prvek kabelu – optická vlákna (minimálně 2 – tam a zpět)

Konstrukční vrstvy zvyšuje pevnost kabelu (plastový vnější kryt)

**1. Mnohovidové:**

- paprsek se odráží od pláště vlákna

- u tohoto kabelu záleží na indexu lomu – rozložení na více světelných paprsků

(tzv. vidů), na konec kabelu dojde paprsek v několika částech – dorazí s

určitým časovým odstupem

- přenášený údaj je zkreslen

- horší optické vlastnosti

- levnější a lépe se s ním pracuje, použití převážně v sítích LAN

**2. Jednovidové:**

- index lomu mezi jádrem a pláštěm optického vlákna je velmi malý

- kabelem prochází pouze 1 paprsek bez lomů a ohybů

- vyšší přenosová kapacita, dokáže přenést signál na delší vzdálenost

Koncovky – kulatý konektor ST

- hranatý konektor SC

Rychlost u optických kabelů je 10/100/1000 Mb/s.

# 

# Topologie sítí

Sběrnicová topologie – (bus topology) – používá se průběžné vedení od stanice ke stanici. Stanice se připojují pomocí odbočovacích prvků (např. T- konektorů). Použití s koaxiálním kabelem.

Výhody:

- kabel vede od stanice ke stanici

- malá spotřeba kabelů – nízké pořizovací náklady

- nízká cena kabeláže

Nevýhody:

- je velký počet spojů v kabelu => potíže a poruchy

- principielní nespolehlivost

- obtížné hledání místa poruchy

- porucha 1 kabelu vyřadí celou síť

Hvězdicová topologie – (star topology) – každá stanice je připojena vlastním kabelem. Kabely jsou poté připojeny do rozbočovače (hub, koncentrátor), který tvoří jakýsi střed sítě. Používá se kroucená dvojlinka.

Výhody:

- spolehlivost a rychlost

- nízká náchylnost k chybám

- porucha 1 kabelu vyřadí pouze 1 stanici na rozdíl od sběrnicové

topologie, která vyřadí všechny počítače

- jednoduché hledání poruchy

Nevýhody:

- vyšší spotřeba kabelů

- nutnost použít rozbočovač

Nejpoužívanější v sítích LAN.

Kruhová topologie – (ring topology) – spojení stanic vytváří souvislý kruh => použití metody postupného předávání zpráv (token - pešek)

Výhoda:

- pravidelné předávání zpráv v kruhu (token)

Nevýhoda:

- přerušení vodiče znamená poruchu celé sítě. To se řeší zdvojením kabelu.

# Přístupové metody

-pravidla, jimiž se řídí přístup síťových stanic ke kabelu.

-jak zabezpečit, aby do sítě vysílala v jednom okamžiku pouze jedna stanice

CSMA – CD (metoda náhodného přístupu)- je neprioritní metoda s náhodným přístupem, určená pro sběrnicovou topologii. Vychází ze situace, kdy jednotlivé uzly soupeří o získání přenosového kanálu. Uzel, který chce zahájit vysílání, naslouchá provozu na přenosovém kanále a zahájí vysílání pouze tehdy, když neuslyší na kanále přenos. Při tomto přístupu ovšem může zjistit klid na lince několik uzlů najednou a zahájit vysílání ve stejný okamžik. Dochází ke kolizi, kterou je třeba řešit buď přímo na úrovni CSMA (tedy linková vrstva) nebo pomocí vyšších vrstev OSI.

Výhody:

- jednoduchost

- rychlost

- nízká cena komponent

Nevýhoda:

- se stoupajícím počtem stanic se zvyšuje pravděpodobnost kolizí – lze

eliminovat pomocí přepínačů (switch) a mostů – zabraňují propouštění

paketů do části sítě, kam nejsou určeny

- přidělování vysílacího času je náhodné, a tak nelze dopředu vědět, kdy

bude zpráva doručena

Tato metoda se používá u Ethernetu a u sítí LAN.

### Token ring:

Sítí koluje speciální paket (token). Vysílat může jen ta stanice, která token vlastní. Právo vysílat má v 1 okamžiku pouze 1 stanice. Token si stanice postupně předávají.

- chybí společný uzel

- PC jsou spojena do kruhu – kruhová topologie

- je citlivý vůči výpadku každé stanice, nemusí to být porucha, ale stačí,

když je 1 PC vypnut a síť je neprůchodná, proto se token ring zapojuje

pomocí koncentrátorů (oproti Hubu je spojovací kabel dvojitý – 1 linka

vede do koncentrátoru a druhá zpět do PC). Pokud 1 kabel vypadne z PC,

koncentrátor jej automaticky přemostí

- přenosová rychlost 4 nebo 16 Mbit/s.

Výhody:

- odolnost proti zahlcení i při vysokém zatížení sítě

- pravidelné přidělování vysílání všem stanicím

Nevýhody:

- složitost

- nižší rychlost

### Token bus:

Stejné jako u Token ring, ale není nutná kruhová topologie.

- každá stanice obdrží logickou adresu, token pak putuje cyklicky od adresy k adrese

# Protokoly

Protokol definuje komunikační pravidla, jimiž se řídí výměna dat v síti. Pro správnost funkce je nutno, aby všechny stanice v síti používaly stejný protokol.

### NetBEUI:

- starý protokol

- vyvinula ho firma IBM, kdy na sítě nebyly kladeny požadavky jako dnes

- nepodporuje směrování

- výhodný jen pro malé sítě Peer to Peer

### IPX/SPX:

- vyvinula ho firma Novell

- ve specifikaci je obsaženo mnoho protokolů se speciálními úkoly

IPX:

- pracuje na úrovni síťové vrstvy ISO/OSI

- zajišťuje přenos paketů vyšších protokolů a přenos dat mezi stanicemi,

ale nekontroluje správnost dat

SPX:

- je vyšším (nadřízeným) protokolem IPX

- pracuje na úrovni transportní vrstvy ISO/OSI

- kontroluje správnost přenosu dat, při zjištění chyby vyžaduje opakování

přenosu

Adresace v sítích IPX/SPX:

- každý kabelový segment sítě má své vlastní **číslo externí sítě IPX**

- **číslo uzlu** též udávané jako MAC adresa (adresa síťové karty)

- **číslo interní sítě**

### TCP/IP:

- nejrozšířenější skupina protokolů

- používá se v internetu, v sítích Novellu a Microsoftu

TCP:

- vytváří spolehlivou službu nad protokolem IP

- vytváří spojení mezi vysílacím a přijímacím PC

- segmentuje data a potvrzuje příjem dat

- spojení navazuje prostřednictvím adres a portů umístěných na každém PC

IP:

- pracuje v síťové vrstvě modelu ISO/OSI

- jeho úkolem je vysílání datagramů na základě adres v nich obsažených

- protokol nespojový

- příjem paketů neověřuje

Adresace v sítích TCP/IP:

- každá stanice musí mít originální číslo => aby z čísla bylo zřejmě umístění

stanice v síťovém segmentu

- každá stanice má svoji IP adresu – čtveřice třímístných desetinných čísel

jednotlivá čísla jsou oddělena tečkou. Maximální hodnota je 255

Třída A) 0-127 – pro rozsáhlé sítě

Třída B) 128 – 191 – pro středně velké sítě

Třída C) 192 – 223 – menší sítě

Maska podsítě:

- podsíť – počítače jsou přímo spojeny (na 2. vrstvě)

- maska podsítě určuje hranici mezi adresou podsítě a adresou počítače v ní

- obsahuje 1 v bitech adresy sítě a podsítě, 0 jinde

- např. 147.230.26.98 s maskou 255.255.255.0 – počítač s adresou 98 v

podsíti 147.230.26.98

- pokud cílová adresa leží ve stejné podsíti, posílá se datagram přímo

adresátovi

### DHCP:

- automatické přidělování IP adresy (při každém

připojení máme jinou IP adresu)

### DNS:

- čísla se převádějí na znaky (každá WWW stránka má svoji IP adresu, a

abychom si nemuseli pamatovat IP adresu, tak tato funkce ji převádí – např.

[www.seznam.cz](http://www.seznam.cz) – 194.228.32.18)

# Aktivní prvky

### Zesilovač, opakovač (repeater):

Nejjednodušší aktivní prvek. Pouze zesiluje procházející signál. Používá se

u kabelů tak dlouhých, na jehož konci by nebyl dostatečně silný signál.

Nejčastěji se používá u koaxiálních sítí.

### Převodník:

Je podobný zesilovači. Zesiluje signál a převádí jej z ještě z jednoho typu

kabelu na jiný typ.

### Rozbočovač,koncentrátor (hub):

- nezbytný prvek v sítích s hvězdicovou topologií

- základní funkce je rozbočování signálu neboli větvení sítě

- větví síť + umí zesilovat a převádět signál

- často má v sobě integrované další aktivní prvky (hlavně funkce mostu)

### Most (bridge):

- první inteligentní prvek, zajímá se o přenášená data

Plní 2 funkce:

1. filtrace paketů – most si přečte cílovou adresu paketu a paket propustí

pouze do té části sítě, v němž je obsazen cíl paketu

Filtrování snižuje zatížení sítě, protože pakety neputují

tam, kam nemají.

2. propojení 2 sítí různých segmentů – pracuje v linkové vrstvě ISO/OSI

### Přepínač (switch):

Velmi používaný aktivní prvek. Podobný mostu, ale filtraci paketů

provádí mezi jednotlivými zdířkami. Komunikace může probíhat mezi

více páry síťových karet (zdířek switche) současně.

### Směrovač (router):

Nejinteligentnější aktivní prvek. Pracuje na úrovni síť. vrstvy ISO/OSI.

Shromažďuje informace o připojených sítích a pak vybírá nejvýhodnější

cestu pro posílaný paket. Má zabudovanou filtraci paketu + inteligentní

směrování. Setkáváme se s ním při připojování sítě k internetu.

### Brána (gateway):

- pracuje v aplikační vrstvě ISO/OSI

- slouží k připojování sítí LAN na cizím prostředí

Shrnutí:

Zesilovač – zesiluje signály (fyzická vrstva)

Převodník – převádí signály mezi různými typy kabelů (fyzická vrstva)

Rozbočovač – rozvádí signály do všech větví sítě (fyzická vrstva)

Most – filtruje pakety (linková vrstva)

Směrovač – směruje pakety (síťová vrstva)

Brána – propojuje 2 rozdílné sítě (aplikační vrstva)

# ISO/OSI

- obsahuje 7 spolupracujících vrstev

- rozděluje síťovou práci na vrstvy

- vyšší vrstva převezme úkol od podřízené vrstvy, zpracuje jej a předá vrstvě

nadřízené

### Aplikační vrstva:

- je určitou aplikací zpřístupňující uživatelům síťové služby

- nabízí a zjišťuje přístup k souborům (na jiných PC), vzdálený přístup k

tiskárnám, správu sítě, elektronické zprávy, …

- uživatel má k ní přímý přístup

- k vytvořené zprávě je připojena hlavička aplikační vrstvy => struktura

identifikující vysílající a cílový PC

### Prezenční vrstva:

- má na starost konverzi dat, přenášená data mohou totiž být v různých

sítích různě kódována => vrstva zajišťuje sjednocení formy vzájemně

přenášených údajů

- komprimuje a případně šifruje

### Relační vrstva:

- navazuje a po skončení přenosu ukončuje spojení

- může provádět ověřování uživatelů a zabezpečení přístupů k zařízení

- rozhoduje se, jakým způsobem bude spojení realizováno:

1. poloduplexně – PC se střídají v příjmu a vysílání

2. duplexně – PC zároveň přijímají a vysílají

### Transportní vrstva:

- nezabývá se vlastním přenosem dat

- data jsou rozdělena do menších částí (paketů), zde jsou vytvářeny

kontrolní součty, které umožňují následnou kontrolu správnosti přenosu

### Síťová vrstva:

- je zodpovědná za spojení a směrování mezi 2 PC nebo celými sítěmi,

mezi nimiž neexistuje přímé spojení

- zajišťuje volbu trasy při spojení

### Linková vrstva:

- uskutečňuje přenos údajů po fyzickém médiu, pracuje s fyzickými

adresami síťových karet

- odesílá a přijímá rámce

- kontroluje cílové adresy každého přijatého rámce a určuje, zda bude

rámec odevzdán vyšší vrstvě

- dohlíží na vlastní přenos paketů

- v případě chybného přenosu musí vrstva zabezpečit jeho opětovné

vyslání

### Fyzická vrstva:

- zajišťuje zakódování rámců do podoby elektrických signálů a jejich

přenos po síťových kabelech

- skutečná fyzická komunikace probíhá vždy vertikálně, tj. mezi

jednotlivými vrstvami, pak přes fyzickou vrstvu k sousední stanici

2. Síť peer to peer (P2P)

# Koncepce práv a uživatelů

### Guest

- účet pro příležitostné uživatele systému

- jejich práva by měla být nastavena na minimum

- defaultně je účet zřízen, ale zároveň zakázán => administrátor může

účet povolit nebo zakázat

doplnit ještě běžné účty – user, administrator….

### Profily

- každý účet má svůj uživatelský profil, který se vytvoří při prvním

přihlášení

- jsou v nich uloženy data a nastavení konkrétního uživatele

- informace najdeme ve složce Documents and Settings

- složky jsou nepřístupné pro ostatní uživatele počítače (kromě správce)

- základní složky profilu: Dokumenty, Nabídka Start, Oblíbené položky a

plocha

### Skupiny

- do skupin se pro snadnou práci administrátora přiřazují uživatelé

- snadné přidělení určitých vlastností více uživatelům najednou

- administrátor může přiřazovat uživatele do připravených skupin

Rozsahy skupin:

- síťové objekty jsou zařazeny do domén

- v jedné velké síti může být několik domén

Místní doménová skupina

Globální skupina

Univerzální skupina

Předdefinované skupiny:

univerzální skupiny – používají se ve vícedoménových strukturách

velkých sítí

systémové skupiny – nejsou v nich umístěni konkrétní uživatelé, ale

zapisují různé uživatele podle toho, jak k počítači

přistupují

### Sdílení

**Místní sdílení** - určuje, kam budou moci přistupovat uživatelé místní, kteří se střídají u pc - do systému se přihlásí na svůj účet, podmínkou místního sdílení je existence uživatelského účtu

**Síťové sdílení** – platí pro ty, kteří do Windows přistoupí z vnějšku (ze sítě)

**Zjednodušené sdílení** – umožňuje sdílet složky se všemi uživateli v pracovní skupině nebo v síti a nastavit složky v uživatelském profilu jako soukromé. V případě povolení tohotosdílení nelze konkrétním uživatelům ani skupinám zabránit v přístupu ke sdíleným složkám.

**Složené sdílení** – používá se, pokud chceme nastavit oprávnění pro konkrétní uživatele a skupiny

# Oprávnění

- zpřístupňování sdílených složek uživatelům v síti

- složka > Vlastnosti > Sdílení > Zatrhnout Sdílet tuto složku

(lze definovat, kolik uživatelů může najednou se složkou pracovat)

Vlastnictví – při vytvoření souboru nebo složky uživatelem, se tento uživatel

automaticky stane vlastníkem tohoto souboru nebo složky

- vlastnictví může převzít od původního vlastníka pouze administrátor

pomocí okna Vlastnosti > Zabezpečení > Upřesnit > Vlastník

Dědění oprávnění – oprávnění složky i její soubory lze dědit => dědění

Dědění můžeme potlačit:

- dědění složce přímo zakážeme (zaškrtávacím

políčkem v kartě Zabezpečení)

- nebo jí přidělíme jiná oprávnění, než má složka

nadřazená

Zděděná oprávnění můžeme zrušit zaškrtnutím políčka ve sloupečku

odepřít.

3. Možnosti vzdáleného přístupu k PC:

Guest – účet, který se vytvoří automaticky při instalaci windows a zároveň se při ní

zablokuje, tohoto účtu může použít každý, kdo nemá vlastní účet v

systému; uživatel má povolen přístup do složky Sdílené dokumenty

Přihlašovací jméno – standardní postup, jak chránit Windows, nutné zadání

uživatelského jména a hesla, v PC nesmí být žádné prázdné

heslo u účtu, do kterého se hlásíme

Shodná jména na všech PC – na všech PC nastavíme stejná jména, čímž si umožníme

vzdálený přístup k PC.

Vzdálená plocha – umožňuje systému Windows XP Professional přístup k relaci systému Windows spuštěné na vašem počítači z jiného počítače. Použitím funkce vzdálená plocha se tedy můžete například připojit k pracovnímu počítači z domova, a získat tak přístup ke všem aplikacím, souborům a síťovým prostředkům, jako byste pracovali přímo s daným počítačem.

- cesta – Tento počítač => vlastnosti => vzdálený přístup => vzdálená plocha

=> povolit

- pracuje na portu 3389

- je nutné připojení k internetu

- na PC nesmí být účet bez hesla a mohou k němu přistupovat pouze někteří

uživatelé (administrátoři a ti, kterým jsme to povolili)

Vzdálená pomoc - lze umožnit známému uživateli, aby se připojil k vašemu počítači přes Internet, konverzoval s vámi a sledoval obrazovku vašeho počítače. S vaším svolením může tento uživatel pomocí své klávesnice nebo myši s vámi spolupracovat na vyřešení problému.

Koncepce sítě:

V síti typu peer to peer (také nazývané [pracovní skupina](ms-its:C:\WINDOWS\Help\network.chm::/hnw_overview.htmHELP=glossary.hlp%20TOPIC=gls_workgroup)) spolu počítače komunikují přímo a ke správě síťových prostředků nevyžadují [server](ms-its:C:\WINDOWS\Help\network.chm::/hnw_overview.htmHELP=glossary.hlp%20TOPIC=gls_server_only). Síť typu peer to peer je vhodná, jestliže je v téže obecné oblasti méně než deset počítačů. Počítače v pracovní skupině jsou považovány za rovnocenné, protože jsou na stejné úrovni a sdílejí mezi sebou prostředky (peer to peer). To, která data v počítači budou sdílena v síti, určují jednotliví uživatelé. Sdílení společných prostředků umožňuje uživatelům tisknout na jedné tiskárně, mít přístup k informacím ve sdílených složkách a pracovat na jednom souboru, aniž by jej bylo třeba přenášet na médium.

K instalaci tohoto druhu sítě je potřeba:

- zapojit kabely

- zapojit síťové karty a nainstalovat jejich ovladače

- nainstalovat klienta sítě, nastavit síťové protokoly a vytvořit pracovní

skupiny

- nastavit sdílení složek a adresářů – přiřadit případná přístupová práva

Klient:

- software, který nám zprostředkuje připojování k jiným počítačům a umožní

využívat jejich služby

- ve Windows je pro připojení k síti peer to peer určen „Klient sítě Microsoft“.

4. Zabezpečení PC, Firewall

- podstatou firewallu je omezování služeb, kterým docílíme vyšší bezpečnost sítě

- software nebo hardware (PC s běžícím softwarem, router,…), jímž je oddělena

lokální síť od internetu

- je to jakási zeď mezi hostitelským počítačem a Internetem

- „díry“ ve Firewallu mohou být definovány číslem portu (staticky), nebo programem

(dynamicky)

- účel firewallu je chránit lokální síť před přístupem z internetu

- základem Firewallu je **NAT**

Firewall je založen na:

- NAT

- otevírání portů TCP/IP

- filtrování paketů TCP/IP

Číslo portu – v tomto případě definujeme číslo portu = služby, která bude otevřená

Typy portů

Programem – mnoho programů si otevírá porty samo

- firewall u ostatních programů povolí otevření portu pouze na základě

důvěryhodného programu

Příklady několika známých portů a jejich služeb:

52 220 – windows messenger

220 – IMAP 3 – pro stahování pošty z internetu do PC

110 – POP3 – stahování pošty

25 – SMTP – pro odesílání pošty

20-21 – FTP – pro stahování dat

23 – Telnet – promítání obrazovky na vzdálenou obrazovku

3389 – Vzdálená plocha

53 – DNS

80 – http

443 – https – zabezpečené http – šifrováním

123 – NTP – synchronizace času

# NAT (Network Address Translator)

- do LAN nepustí pakety, které přichází z Internetu (pouze pokud to

nepovolíme otevřením některého z portů)

- ale umožní navázat spojení z LAN do Internetu

- pokud je nalezen odpovídající záznam, je paket vpuštěn do sítě a jeho

cílová adresa je změněna na adresu PC v lokální síti, který paket odeslal

- komunikaci s Internetem musí začít vždy klientský počítač

- navázat spojení z internetu do sítě později není možné

# 3 prvky zabezpečení počítače

1 – Update systému

2 – Antivirový systém

3 – Firewall

4 – Vyhledávač spywaru

5 – Zakázaný účet Guest

5. Doména Windows Server 2003

Doména – je logické seskupení síťových počítačů, které sdílejí centrální databázi síťových údajů (uživatelské účty, informace o zabezpečení)

- po přihlášení k doméně máme k dispozici všechny zdroje serveru

Active Directory – databáze síťových objektů, používají se nejčastěji tyto objekty:

- uživatel (informace o přihlašovacím jménu a heslu)

- skupina (obsahuje uživatele nebo jiné skupiny)

- tiskárna (tiskárna použitelná v síti)

- počítač (reprezentuje počítač v síti, všechny potřebné informace)

- sdílená složka (informuje o sdílené složce, která je zapsaná v

registru konkrétního počítače)

logická struktura – organizuje všechny prvky databáze podle pravidel, která se

snaží kopírovat správní strukturu organizace.

- základní prvek je objekt – vlastnosti síťových prostředků

- kontejner – jsou tam uloženy buď kontejnery, nebo objekty

- organizační jednotka – nižší stupeň kontejneru

- doména – v ní může být uloženo několik organizačních jednotek

fyzická struktura – údaje o objektech 1 domény jsou uloženy na PC s Windows

server 2003

Uživatelské účty

Místní uživatelské účty – zprostředkovávají připojení uživatelů k místnímu PC,

kde je účet vytvořen

Doménové uživatelské účty – uživatel se přihlásí do domény, čímž získá

přístup k síťovým prostředkům

Skupiny

místní skupiny počítače – platí pouze pro 1 počítač (Guest, Users, Power

Users, Backup operators, Administrators)

místní skupiny domény – pro přidělování oprávnění ke sdíleným

prostředkům jakéhokoliv počítače v doméně

(Guest, Users, Account operators, Server

operators, Print operators, Backup operators,

Administrators)

6. Práce v doméně Windows Serveru 2003

Oprávnění používají Windows 2000 ke zpřístupňování sdílených složek. Sdílená složka je ta, která se nabízí ostatním

uživatelům sítě. Zpřístupňujeme především složky na serveru, protože ten bývá hardwarově nejlepším PC v síti a navíc

ho nevypínáme – sdílená složka je vždy k dispozici. V dalším výkladu budeme předpokládat, že sdílíme složky

souborového systému NTFS, který se používá u serverů (je běžný i u Windows 2000 Professional).

Přiřazení oprávnění složce

Na složku, kterou chceme v síti sdílet, klepneme pravým tlačítkem myši a z menu vybereme Vlastnosti > Sdílení > nastavíme vlastnosti pro použití

vlastnosti pro použití složky uživatelem ze sítě:

>Sdílet tuto složku **–** zde je možno nastavit komentář a počet uživatelů, kteří mohou ke sdílené složce připojit současně

Na této kartě se nachází Oprávnění, kterépovoluje práci uživatelům, kteří jsou připojeni do sítě. K dispozici máme tyto volby:

Oprávnění NTFS (v kartě Vlastnosti > Zabezpečení) mají přednost před oprávněním složek!

Druhy oprávnění

Procházet složku / spouštět soubory

Zobrazovat obsah složky / číst data

Číst atributy

Číst rozšířené atributy

Vytvářet soubory / zapisovat data

Vytvářet složky / připojovat data

Zapisovat atributy

Zapisovat rozšířené atributy

Odstraňovat podsložky a soubory

Odstraňovat

Číst oprávnění

Měnit oprávnění

Přebírat vlastnictví

Dědění oprávnění – oprávnění složky i její soubory lze dědit => dědění

Dědění můžeme potlačit:

- dědění složce přímo zakážeme (zaškrtávacím

políčkem v kartě Zabezpečení)

- nebo jí přidělíme jiná oprávnění, než má složka

nadřazená

Zděděná oprávnění můžeme zrušit zaškrtnutím políčka ve sloupečku

odepřít.

Vypnutí serveru

- pomocí Start > Vypnout

- před vypnutím serveru je nutné zkontrolovat, zda někdo nepracuje se serverem. To

zjistíme pomocí položky Ovládací panely > Správa počítače. Na kartě by měly být

relace a otevřené soubory prázdné

- správce by měl na vypnutí serveru předem upozornit každého uživatele počítače v

síti

Připojení PC do domény

- pomocí Tento počítač > Vlastnosti > Název počítače > Identifikace v síti

- k připojení do domény vybereme „tento počítač je součástí podnikové sítě…“ >

„společnost používá síť s doménou“ > zde je nutno vyplnit údaje (Uživatelské

jméno, heslo a doménu) > Dokončit > restart PC

- po restartu je počítač přiřazen do domény

Mapování

- jestliže často užíváme složky z jiného počítače v síti, můžeme si je namapovat

- složce, kterou chceme sdílet, přiřadíme logické jméno disku (např.: F: )

- Tento počítač – připojit síťovou jednotku > vybereme jednotku a popřípadě

složku na disku, zde lze navolit také, zda chceme mít složku namapovanou i při

příštím přihlášení – pomocí zaškrtnutí políčka „znovu připojit při přihlášení“

Příkazy NET

- příkazy pro práci se sítí

- nejsou omezeny pouze na server, ale fungují i na XP a Windows 2000

- najdeme je v nápovědě

Net Accounts – práce se jmény a hesly

Net Use – připojuje a odpojuje PC od sdílených prostředků (pro mapování)

Net Send – posílání zpráv v síti

8. Síť Novell

**Přístupová práva a atributy k adresářům a souborům v síti Novell Netware**

Přístupová práva k adresářům a souborům slouží k zamezení nežádoucího přístupu k datům.

Vlastní systém přístupových práv je složen z:

1. Effective Rights (efektivní práva) – skutečná práva, kterými je schopen uživatel disponovat
2. Trustee – definice práv konkrétnímu adresáři nebo souboru
3. Inherited rights filters (IRF)– filtry děděných práv – jestliže nejsou práva nastavena konkrétnímu adresáři nebo souboru pomocí Trustee, dědí se práva na tento adresář nebo soubor z nadřazené složky
4. Atributy – jsou nastaveny u každého adresáře nebo souboru; u každého souboru nebo adresáře je možné atributy měnit a tím ovlivňovat jejich vlastnosti přesněji

**Druhy práv**

Supervisor – S – Jsou umožněna všechna práva k adresářům a souborům

Read – R – Umožňuje otevírat, číst a spouštět

Write – W – Umožňuje otevírat, zapisovat a měnit obsah adresáře

Create – C – Umožňuje v adresáři vytvořit nové adresáře a soubory

Erase – E – Zruší všechny podadresáře a soubory

Modify – M – Umožní měnit atributy, přejmenovat adresář i soubory v něm obsažené a

adresáře. !Neumožňuje měnit obsah adresáře nebo souborů v něm!

File Scan – F – Dovolí vidět adresář a soubory v něm.

Access Control – A – Umožňuje přidělovat Trustee (kromě Supervisora)

Kombinace přístupových práv se v novellu zařazuje do hranatých závorek.

Např.: [RWCEMFA]

**Trustee**

Novell umožňuje přidělovat práva nejen uživatelům ale i skupinám uživatelů, což usnadňuje práci administrátora. To znamená, že právo, které přiřadíme skupině, se přenese na všechny uživatele v této skupině. Objekt, který má přidělená práva přímo, je Trustee tohoto adresáře.

**Inherited Rights Filters – dědění práv**

Dědění práv z nadřazeného adresáře nemusí být automatické – je možno ho upravit. Při dědění práv na konkrétní adresář se mění atributy (ne atributy, ale přístupová práva) souborů v tomto adresáři – tyto soubory mají stejná práva, jako samotný adresář.

**Effective Rights – efektivní práva**

Práva k souborům a adresářům jsou definována dvěma způsoby(pomocí Trustee a IRF).Proto byla zavedena práva efektivní, která spojují Trustee a IRF na práva skutečná. Postup, kterým určujeme efektivní práva, nazýváme logický součin. Př.: Pokud má adresář přidělena trustee [RMFA] a IRF [SRWCEMFA], potom budou výsledná práva pouze ta, která se vyskytují v obou částech. Tedy [RMFA].

Ještě upřesnit konstrukci práv – nejlépe přes vývojový diagram)

**Atributy**

Umožňují nastavit další vlastnosti adresářů a souborů. Mají přednost před efektivními právy. Atributy u souboru či adresáře může měnit pouze administrátor či uživatel s právem M.

Nejčastěji používané atributy a jejich význam:

Archive needed – A – informuje, že soubor byl od poslední archivace změněn

Can’t Compress – Cc – soubor se nezkomprimuje, protože úspora místa by byla malá

Compressed – Co – soubor je komprimovaný

Delete Inhibit – Di – zabraňuje výmaz adresáře nebo souboru

Hidden – H – neviditelný adresář nebo soubor, nelze ho smazat ani zkopírovat

Purge Immediate – P – pokud soubor nebo adresář logicky smažeme, je smazaný i

fyzicky

Read Only – Ro – soubor je pouze pro čtení, nelze ho zrušit nebo změnit. Současně

se nastavují i atributy Ri a Di.

Read / Write – Rw – soubor lze modifikovat či mazat.

Rename Inhibit - Ri – zabraňuje přejmenování adresáře či souboru.

Práva a atributy se nejčastěji mění pomocí Netware Administratoru nebo pomocí klienta sítě Netware od firmy Novell.

11. Základní koncepce Linuxu

- uživatel není závislý na vývoji SW firmy

- není nutné čekat na opravy chyb

- na vývoji se podílí mnoho vývojářů (jsou schopni odhalit mnoho chyb)

- uživatel si sám přizpůsobuje software (systém)

S těmito cíli vznikl projekt GNU:

- založeno na Unixu (překlad na X86)

- bez licenčních omezení – zahrnuto do licence GPL

GPL (GNU Public Licence):

- SW je volně šiřitelný – nikdo to nesmí porušit

- SW může kdokoli šířit (i prodávat), ale vždy musí být k dispozici zdrojový kód

- licence se vztahuje i na prodaný produkt

- programátor není zodpovědný za chyby SW

Autorem je Linus Torwalds (1991) verze 1.

verze 2.2 už obsahovala pouze 5% jeho kódu

**Distribuce:**

- linux je pouze operační systém (přiděluje paměť, obsluhuje HW, uživatele)

- k běžné práci jsou potřeba další aplikace (programy, grafické rozhraní,…)

Linux – jádro systému

GNU Linux – celý systém

Binární distribuce – jsou předkompilované – lze je nainstalovat inst. Programem

Nejznámější distribuce: Debian Linux GNU

RedHat GNU Linux

SuSe GNU Linux – distribuuje Novell (provozuje pod

ním servery)

Zdrojové distribuce – nutno zkompilovat a převést do bin. tvaru (lze je zkompilovat

přesně pro určený HW) – doporučeno pro servery

Live distribuce – nic se neinstaluje (Knopix, Danix, Adios, Manix,…)

**Souborový systém:**

- organizuje soubory na disku

- linux zná všechny běžné souborové systémy

Souborové systémy Linuxu: Ext2 (FS2)

Ext3 (FS3) – doporučovaný

REISER (FS)

Disky a diskové oddíly:

- monolitické jádro linuxu obsahuje všechny ovladače pro všechny známé typy disků

(IDE, SCSI, SATA)

- na 1 disku může být více zařízení (ta mohou mít svá jména)

/dev/hdx (jedná se o disky IDE)

/dev/sdx (jedná se o disky SCSI)

x – má každý z oddílů – jméno disku a jeho oddíl

**Uživatelé linuxu**

- v linuxu musí být každý soubor nebo složka ve vlastnictví nějakého uživatele

- přístup k souboru záleží na právech uživatelů nebo skupin

3 kategorie uživatelů:

- Administrátor (ROOT)

- běžný uživatel

- některé služby

- každý uživatel má vlastnosti – 1. přihlašovací jméno

2. heslo

3. UID – uživatelské ID (unikátní, má ho každý)

4. GID – ID skupiny, kam uživatel patří

5. popis uživatele

6. domovský adresář, zpravidla /home/jméno

7. interpret příkazu (shell) – příkazové rozhraní

(BASH)

Veškeré konfigurace jsou uložené v textových souborech:

/etc/passwd – hesla zde nejsou uložena

/etc/shadow – zde jsou hesla šifrována metodou, která i totožná hesla

zapíše jinak

**Konfigurační soubory v linuxu související s uživateli**

etc/passwd

Příklad.:

Linux : x :100:100: linux : /home/linux :bin/bash

přihl. jméno:odkaz na heslo:UID:GID:popis uživatele:domovský adresář:příkaz. shell

etc/shadow

etc/group