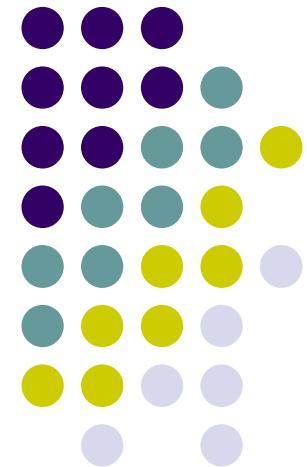


Principy a možnosti počítačových sítí

Školení ICT koordinátorů
29.11.2008





Představení se

- Ing. Ondřej Kasan
- programátor-analytik, vývoj informačních systémů na zakázku, B2B, v komerční sféře
- 1-denní úvazek – externí administrátor počítačové sítě Gymnázium Voděradská
- Od r. 1996 (během studií na FEL ČVUT, od r. 2002 při zaměstnání)

Principy a možnosti počítačových sítí



- Původní námět bloku, připravené prezentace a dokumenty v Moodle
- Co bude však přínosnější, jak naplnit vyhrazený čas?
- Odklon od čistě technického a odborného zaměření ke zprostředkování vlastních zkušeností, nápadů, poznatků (technické věci ale nemineme, budeme se jim věnovat)
- Zprostředkování mých vlastních zkušeností a poznatků, v několika kapitolách



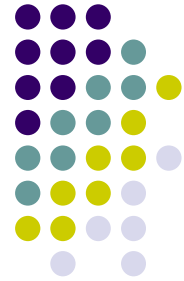
„Vybrané partie z problematiky počítačových sítí“

Vybrané partie z problematiky počítačových sítí



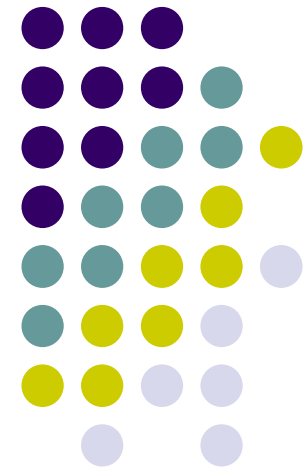
1. [Úvod k počítačovým sítím](#)
2. [Principy a realizace sítí](#)
3. [ISO OSI, TCP/IP](#)
4. [Servery, doménové prostředí, profily](#)
5. [Sdílené prostředky na síti](#)
6. [Vzdálený přístup k ICT prostředkům](#)
7. [Auditace, inventarizace](#)
8. [Zálohování](#)
9. [Připojení k internetu, server, e-mail, groupware](#)
10. [Antivirová a antispam řešení](#)
11. [Bezpečnostní záplaty, aktualizace systému](#)
12. [Software](#)
13. [Hardware](#)

Vybrané partie z problematiky počítačových sítí



1. [Úvod k počítačovým sítím](#)
2. [Principy a realizace sítí](#)
3. [ISO OSI, TCP/IP](#)
4. [Servery, doménové prostředí, profily](#)
5. [Sdílené prostředky na síti](#)
6. [Vzdálený přístup k ICT prostředkům](#)
7. [Auditace, inventarizace](#)
8. [Zálohování](#)
9. [Připojení k internetu, server, e-mail, groupware](#)
10. [Antivirová a antispam řešení](#)
11. [Bezpečnostní záplaty, aktualizace systému](#)
12. [Software](#)
13. [Hardware](#)

1. Úvod k počítačovým sítím





Smysl a důvody sítě

- přístup k jedněm datům, jedněm aplikacím
- sjednocení, jednotnost prostředí
- paralelizace práce
- možnost obsluhy dat odkudkoli, nezávisle na stanici
- zastupitelnost prvků v síti
- efektivní využití prvků v síti (sdílení)
(sem patří i připojení k internetu)



Počítačová síť

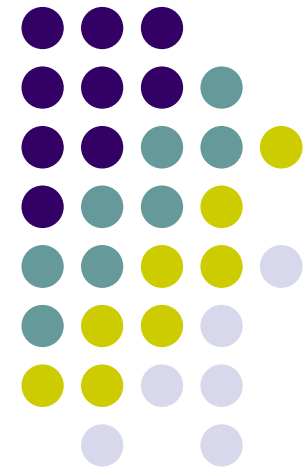
- Je to hardware nebo software?
- Obojí najednou!
- Vztahuje se k tomu ISO OSI architektura, ta role hw a sw rozděljuje

Účely, role a potřeby sítě



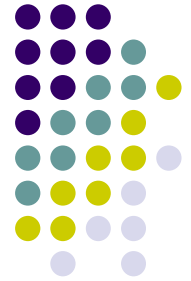
- Pro potřeby vedení, administrativa, řízení, evidence, zpracování (sem patří i agenda školní jídelny, agenda přijímaček, výstupů pro úřady)
- Příprava kantorů na výuku, vzdělávání, sdílení mezi kantory, podpora výuky
- Vlastní výuka, práce studentů

2. Principy a realizace síti



Rozdělení

- Podle přenosového média
- Podle topologie
- Podle způsobu přenosu





Podle přenosového média

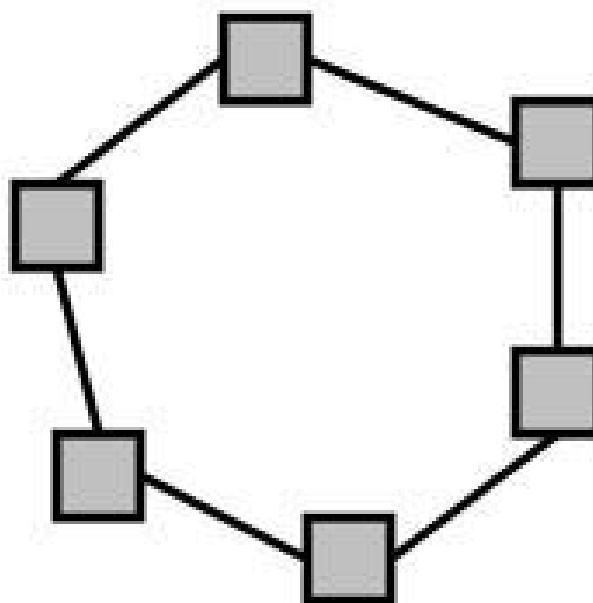
- Klasické, drátové – wired network – LAN jsou založené většinou na TP kabelech (Twisted Pair – kroucená dvojlinka) a Ethernetu – IEEE 802.3. Přístupové linky pro napojení do WAN využívají telefonní měděné ddráty (ISDN, ADSL) nebo koaxiální kabely kabelové televize.
- Bezdrátové – wireless network - přenos přes antény v mikrovlnném pásmu 2.4 nebo 5 MHz – IEEE 802.11, využívají se jako alternativa telefonní linky pro „poslední míli“.
- Optické kabely – fiber optics - signál není rušen elektromagnetickým zářením – IEEE 802.8. Využívají se zejména pro páteřní spoje Internetu.



Podle topologie

A) Kruh

- nemá centrální uzel, používalo se u sítě TokenRing

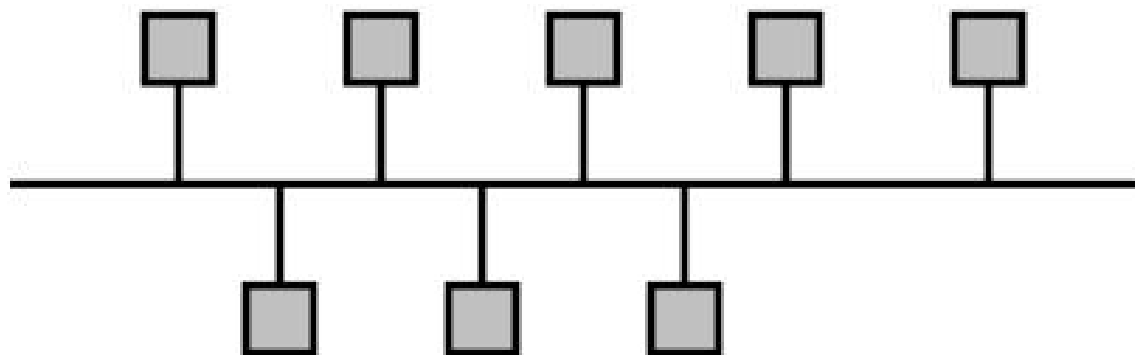




Podle topologie

B) Sběrnice

- sítě založené na koaxiálním kabelu (dnes již nepoužívané) nebo optickém kabelu

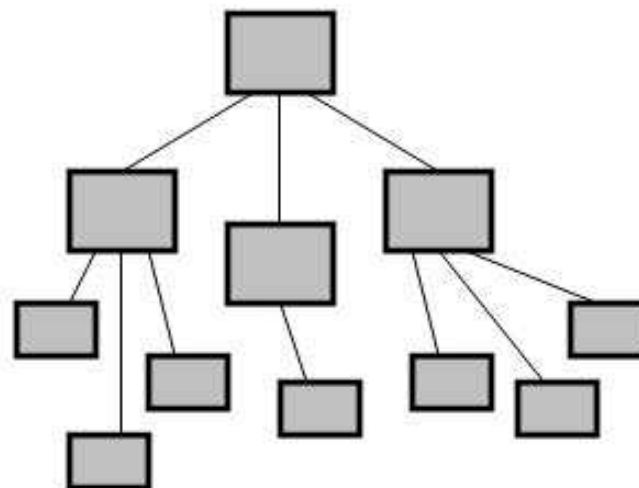
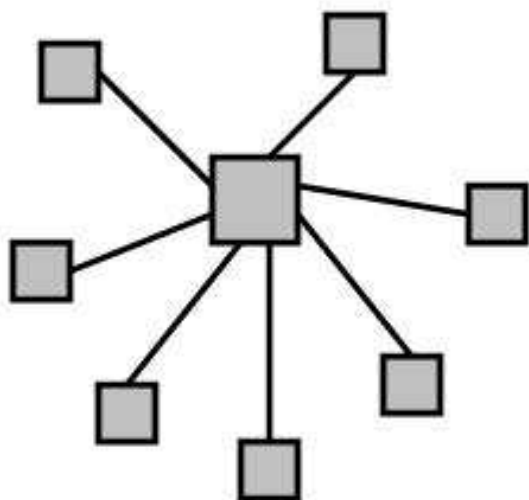




Podle topologie

C) Hvězda, popř. strom

- nejobvyklejší uspořádání Ethernet sítí - s centrálním rozbočovačem





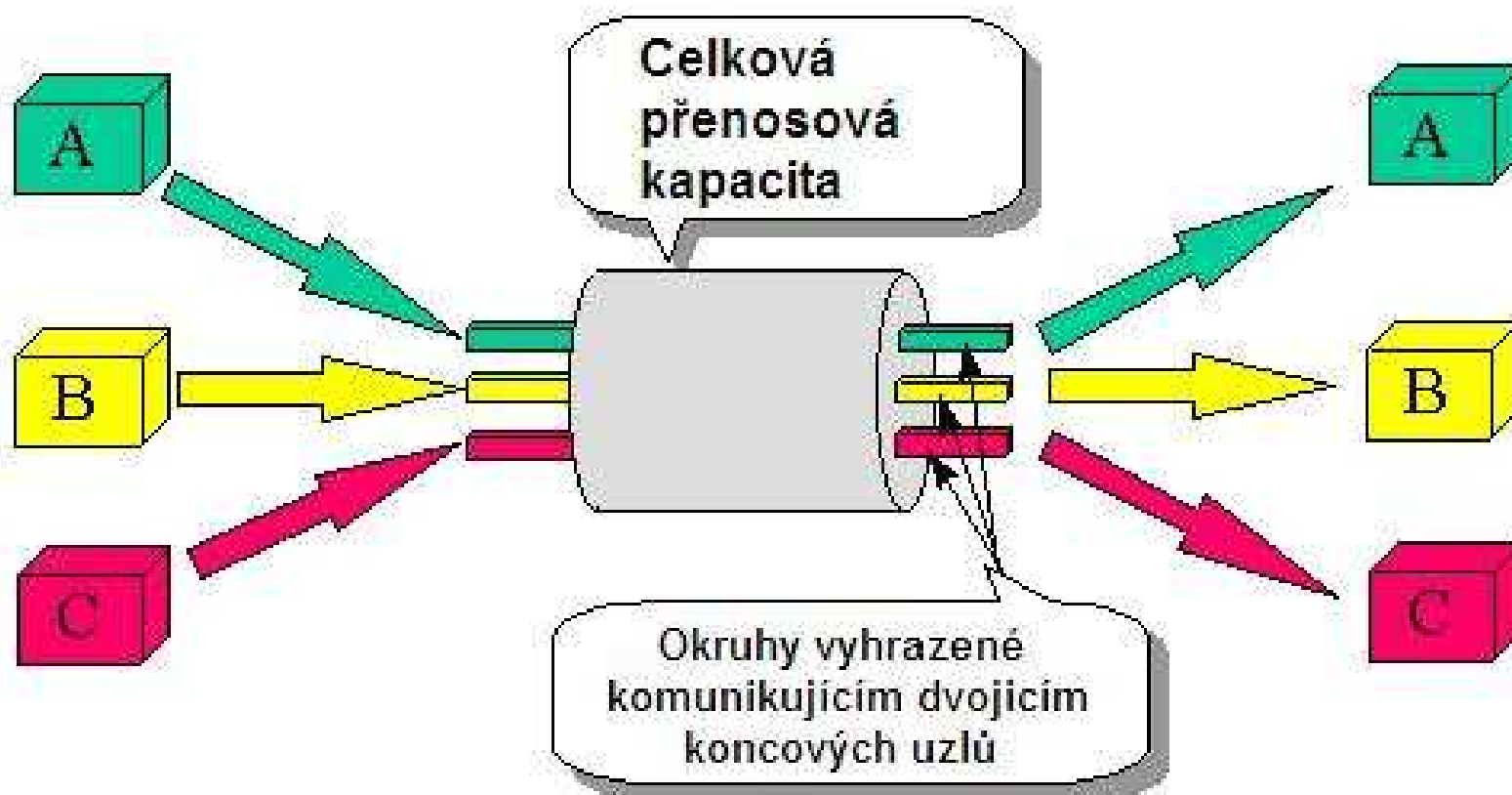
Podle způsobu přenosu

A) Přepojování okruhů – circuit switching – vzniklo ve světě telekomunikací

- vytvoření vyhrazeného kanálu propojením v ústřednách (jako při telefonování)
- přenáší se proud dat pouze jednoho uživatele
- platí se telekomunikační firmě i když kanál právě není využíván
- tzv. pevné (vyhrazené) linky, vytáčené spojení, ISDN
- přenosová kapacita je pevně dána.
- síť je řízena přepojovacími ústřednami - „chytrá síť, hloupé uzly“
- vhodná k přenosu multimédií – zvuk, obraz



Přepojování okruhů



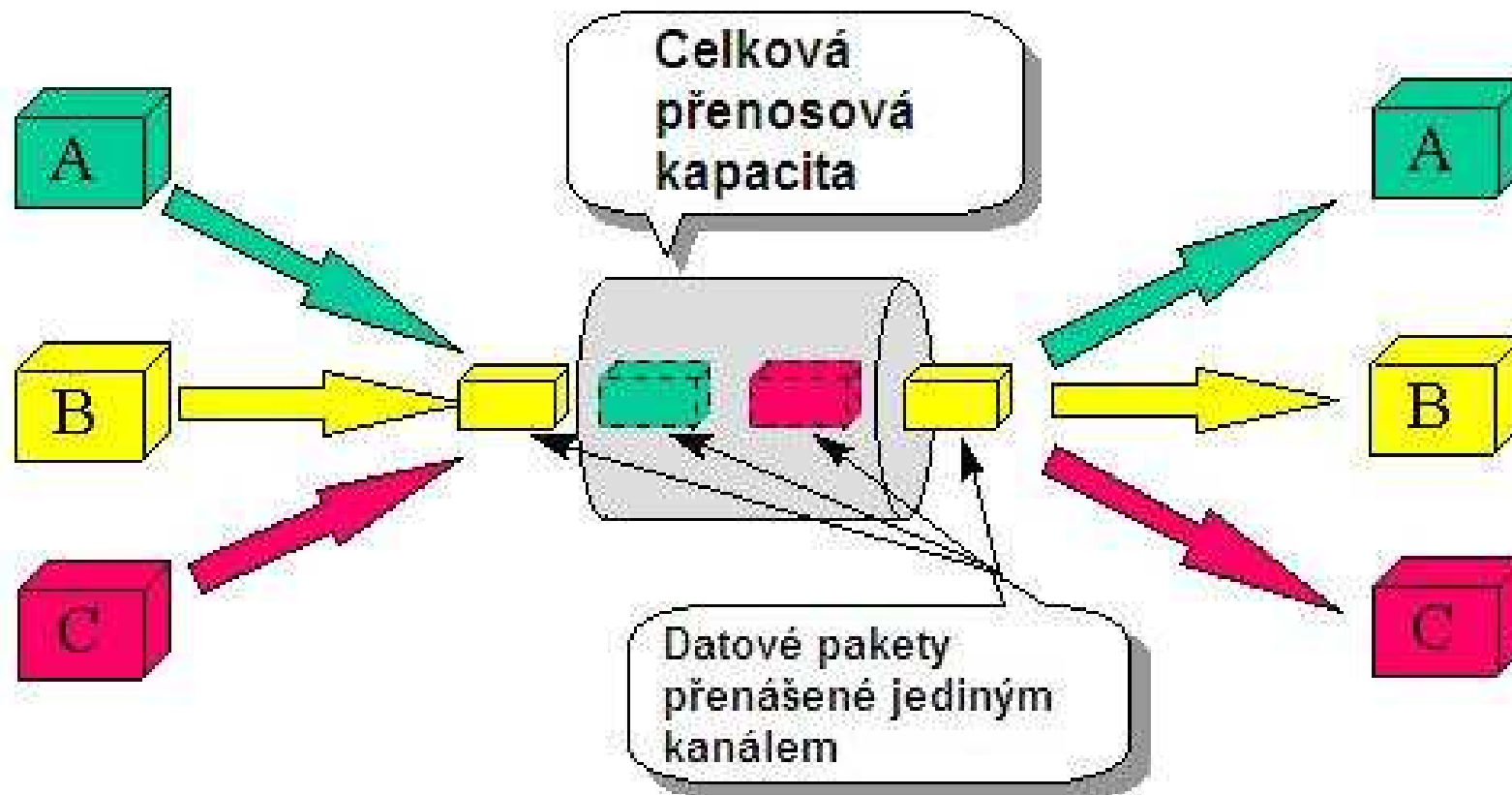


Podle způsobu přenosu

B) Přepojování paketů – packet switching – vzniklo ve světě datových sítí

- sdílení kanálu s dalšími uživateli
- přenáší se kousky dat (pakety, rámce) od různých uživatelů a na konci cesty se skládají
- platí se jen za přenesená data
- ADSL, WI-FI, GPRS, EDGE, UMTS
- síť je řízena koncovými uzly - „hloupá síť, chytré uzly“
- vhodná k přenosu dat – soubory, HTML stránky, e-mail

Přepojování paketů



Ethernet



Ethernet* 10BASE-5 a 10BASE-2

- koaxiální kabel, sběrníková topologie, již minulost
- dosah 185m

Ethernet 10BASE-T – IEEE 802.3i

- nejrozšířenější typ ethernetu
- topologie „hvězda“ s centrálním rozbočovačem (hub)
- přenosová rychlost 10Mbit/s
- realizováno na kroucené dvoulince – UTP – kabel kategorie 3 nebo 5 – použity 2 páry ze 4
- dosah 100m

Ethernet



Ethernet 100BASE-TX – **FastEthernet** – IEEE 802.3u,
y

- 100Mbit/s
- UTP Cat5, 2 nebo 4 páry, ale také na optickém kabelu (100BASE-TX) nebo na telefonních rozvodech (100BASE-T4)

Ethernet 1000BASE-T – **GigabitEthernet** – IEEE
802.3z, ab

- realizováno hlavně na optice, ale také na UTP Cat5, 4 páry



Ethernet

- pozor na rychlost, není to:
 $10 / 8 = 1,25 \text{ MB/s!}$
 $100 / 8 = 12,5 \text{ MB/s!}$
 $1000 / 8 = 125 \text{ MB/s!}$
- princip Ethernet média – kolizní sdílené médium, praktická efektivita kolem 25%, často ale o něco více (díky full duplex)

Gigabit ethernet



- dříve pouze optika, dnes i metalika
- použití kvalitnějších kabelů UTP, normováno jako UTP6
- lze však provozovat i na UTP5, UTP5e, kabely jsou kvalitní (jen není podle normy)
- trochu marketingový podvod, gigabit není 10x rychlejší oproti 100 Mbit



Gigabit ethernet

- důvod – velký tok dat - data nestačí proběhnout přes PCI sběrnici, ani být zpracována (síťové karty jsou však už integrovány přímo na chipset základní desky, přes PCI Express apod.)
- přesto vzhledem ke klesajícím cenám za to stojí
- minimálně pro páteřní části sítě – spojování segmentů a pro servery



Aktivní prvky

- switche (ne huby) – přepínání paketů na linkové vrstvě
- dražší-kvalitnější switche mají smysl, jsou propustnější, manageovatelné (prioritizace, VLAN)
- lépe víceportové, než kaskády switchů
- případné kaskády realizovat gigabit ethernetem (páteřní části sítě)

Potřebujeme jednu novou zástrčku LAN a museli bychom tahat nový kabel?



- řešení možné, není jen podle normy (ale komu to vadí?)
- základní ethernet UTP s RJ45 má 8 vodičů
- využívají se na data pouze 4 (ostatní pro power over ethernet apod.)
- použijeme „rozdvojku“ – rozbočuje jednu zásuvku na dvě
- nutno ji zapojit na straně zásuvky i racku

Problém oddělení studentské sítě od sítě vedení



- potřeba je jasná
- nutno však zachovat sdílení prostředků
- oddělení prostřednictvím routování (router nebo na úrovni propojovacího serveru)
- možno i prostřednictvím VLAN
- není to však někdy paranoia? sniffing?
- případné úniky dat jsou stejně vždy dány chybami mezi židlí a klávesnicí



Bezdrátové sítě (Wifi)

- drát je vždycky drát
- nižší přenosové rychlosti, rušení, zahlcenost nelicencovaného pásma, neprostupnost zdí, menší spolehlivost, pomalejší odezva
- nebezpečí odposlechů (přesahy mimo budovu)



Bezdrátové sítě (Wifi)

- používat spíše jen pro studentskou část sítě, routovat (oddělení sítě)
- používat spíše jako dokrývač pro části, místnosti, malý dosah
- nebo tam, kde nelze tahat dráty
- nebo využití z „opačné strany“ – připojení k internetu

Jak to probíhalo u nás? 1/3



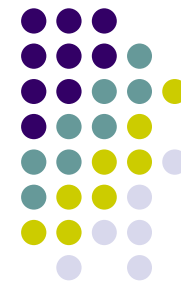
- polovina 90. let
- koaxiální rozvody, BNC, terminátory, na dosah učebna + server
- velmi často zlobilo – výpadek terminátoru, ohnutí kabelu = výpadek celé sítě, hledání místa chyby
- izolované segmenty sítě (učebny, vedení školy, samostatné servery)
- dokonce izolované počítače po škole
- síťový OS – Novell 3.12, 4.11

Jak to probíhalo u nás? 2/3



- postupná náhrada za modernější rozvody UTP
- ad hoc rozšiřování, bez plánů a koncepce do budoucna
- spojování dosavadních částí sítí, sjednocování, společné prostředky
- síťový OS - dobíhající Novell, začínající Windows 2000 Server

Jak to probíhalo u nás? 3/3



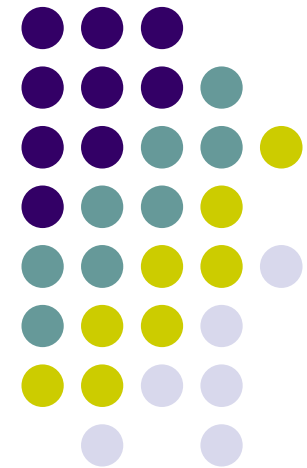
- poslední 3 roky
- nová koncepce síťových rozvodů po škole, po celé budově (realizace ve 2 etapách)
- zavedení přípojek všude, kde lze hypoteticky v budoucnu připojovat
- dostatečné dimenzování
- orientace na drát, bezdrát nemáme



Jak to probíhalo u nás? 3/3

- do všech učeben, pracoven, kabinetů atd.
- serióznější provedení (rozvodné skříně, snížení počtu kaskád aktivních prvků, definování páteřní sítě mezi rozvodnými skříněmi)
- komplexní jednotné doménové prostředí (serverová farma Windows Server 2003, 2000) – viz dále

3. ISO OSI a TCP/IP





Konceptuální modely

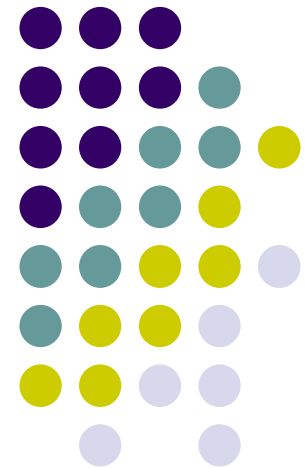


TCP/IP



- IP = unifikovaná adresa PC v síti pro komunikaci, napříč světem (zpravidla 1 síťová karta = 1 IP adresa)
- TCP = slouží pro paketování (kousíčkování) dat zasílaných mezi PC, servery, internetem, lokální sítí
- Potvrzovaná služba (na rozdíl od UDP)
- Příklad IP adresy: 192.168.1.52
- Maska = „příslušnost k lokální síti“
např. 255.255.255.0
- Co nepatří do „lokální sítě“, směřuje se přes bránu (gateway) – ta rozhodne, kam s daty
- V současnosti IPv4, v budoucnu IPv6

4. Servery, doménové prostředí, profily





Servery ve škole

- Mít jeden server na všechno?
 - Nebo více serverů – rozložení zátěže?
Rozložení úloh? Zálohování dostupnosti?
- kombinace obojího, záleží na zpracovávaném rozsahu

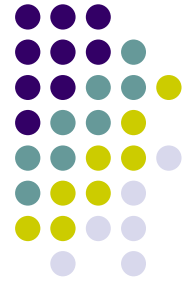
Servery ve škole

- v našem případě



1. **hlavní datový a programový server, primární řadič domény**
2. **sekundární datový a programový server, SQL server, pro potřeby vedení školy**
3. terminálový server (vzdálené připojení)
4. **internetový server (s e-mailem, www a dalšími službami)**
5. zálohovací server
6. server pro OCS Inventory

Jednotné prostředí autentifikace a řízení práv



- **doména** – Active Directory (od Windows 2000 Server výše)
- jedno jméno a heslo pro uživatele pro celou síť
- jednotná správa domény a objektů v něm
- možnost třídit do organizačních jednotek, přidělovat vlastnosti skupinám
- stanice jako součást domény – platí pro ně stejný systém práv i na lokální prostředky (=homogenní prostředí)



Doménový řadič

- může být jeden, může jich být více (pro jednu doménu)
- rozložení zátěže
- pokud jeden řadič vypadne, autentifikaci na síti zajistí další řadič
- mezi řadiči probíhá synchronizace
- příliš mnoho řadičů škodí



DNS server

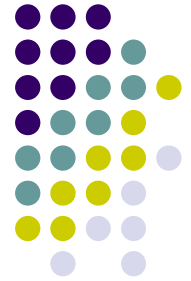
- DNS = překlad jmenných názvů na IP adresy (www.seznam.cz → 77.75.72.3)
- s doménovým řadičem nutno zprovoznit
- vhodné mít i sekundární, na jiném serveru
- může i trochu urychlit internet – požadavky při brouzdání uživateli ukládá do vyrovnávací paměti



Z výhod domény

- asociace uživatelů AD s účty v daném systému
- jsou aplikace, které využívají autentifikaci v AD (Kerio Mailserver, 602 LanSuite Groupware 5 atd.)
- změny hesla proběhnou najednou všude

Skupinové politiky (Group Policies)



- efektivní distribuce pravidel na síti a na stanicích
- nemusíme obcházet stanice a všude nastavovat, stačí nastavit ve skupinových politikách nastavit parametry, v čase probublají po síti)
- s Windows Server 2003 R2 lze centrálně instalovat uživatelům i síťové tiskárny
- lze prostřednictvím jich i instalovat aplikace po síti, automatizovaně (MSI balíčky)



MSI balíčky

- často je má k dispozici výrobce programu
- můžeme si je vyrábět i sami
(bohužel trochu náročnější disciplína
+ dobré nástroje jsou komerční - drahé)
- některé MSI balíčky nefungují ☹
(někdy problém jazykových verzí)



Cestovní profily

- klasické profily ve Windows 2000/XP/Vista známe, používáme, každý uživatel (login) má svůj profil
- v síťovém prostředí význam profilu mírně roste
- nastavením vlastností uživatele můžeme lokální profil převést na cestovní



Cestovní profily

- cestovní profily se udržují ve dvou kopiích – na stanici a na serveru
- při přihlašování a odhlašování probíhá synchronizace obou kopií
- díky serverové kopii si můžeme sednout k jinému počítači a po přihlášení vidíme své prostředí, svoje ikony, plochu, dokumenty atd.



Cestovní profily

- užitečné zvlášt' v učebně, studenti si sedají pokaždé jinam, stejně tak učitelé si předsedávají po kabinetech po škole
- můžeme na serveru upravovat serverovou kopii (nahrávat ikony atd.)
- lze nastavit v GP mazání lokálních kopií
 - zvýšení bezpečnosti
 - zpomalení přihlašování příště

Cestovní profily - nevýhoda



- nevýhoda – zvýšené nároky na síťový provoz při synchronizaci
- profil může mít od jednotek MB po stovky MB či dokonce GB (přihlášení a odhlášení může trvat i desítky minut)

Cestovní profily

– řešení nevýhod



- ponechávat lokální kopie cestovních profilů (příště se nenačítá celý, jen rozdíly)

+ rychlost

- menší bezpečnost (relativně) (data profilu jsou „roztroušena“ po stanicích na síti)

Cestovní profily

– řešení nevýhod



- vybrané složky (Plocha, Dokumenty, Data aplikací), které mají datovou náročnost, přesměrovat v nastavení skupinových politik do domovských složek uživatele
- + vlastní cestovní profil je malý
- +/- vše je okamžitě ukládáno na síť
- + vyšší bezpečnost (nic z určených stanic nezůstává na lokálních discích)



Mandatorní profily

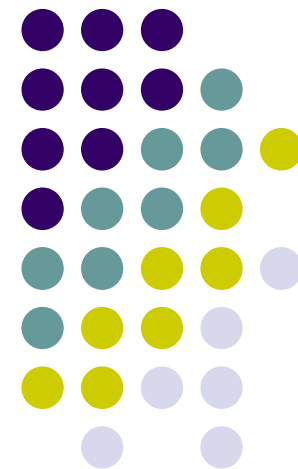
- cesta, jak zajistit uživatelům, že si udrží čistou plochu, prostředí
- USER.DAT → USER.MAN
- Po přihlášení se vnutí vždy podoba předdefinovaného mandatorního profilu (= vytvoříme si vhodný výchozí stav pro práci, neřešíme odchylky)



Mandatorní profily

- Při odhlášení se aktuální podoba profilu a změny v něm zahodí
- Mandatorní profil nemá vliv na přesměrované složky! (výhoda)
- Vhodné pro použití pro studenty (jinak by to bylo neudržitelné, při stovkách účtů)

5. Sdílené prostředky na síti



Sdílené prostředky na síti



- rozložení zátěže, efektivní využití prostředků
- prostředky ke sdílení:
 - soubory (dokumenty, data atd.)
 - aplikace (klient-server architektura)
 - internet a navazující služby
 - tiskárny
 - skenery
 - faxy
 - ...



Sdílené tiskárny

- nejjednodušší řešení – nasdílení lokální tiskárny připojené k počítači
 - + nejlevnější, nejrychlejší způsob zprovoznění
 - nutno mít spuštěný hostitelský počítač
 - trošku horší nastavování práv
 - částečně i zátěž pro daný počítač

Sdílené tiskárny



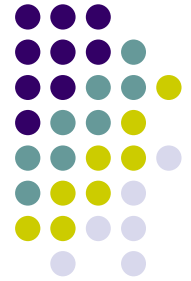
- lepší řešení – plnohodnotné síťové tiskárny, se síťovou zásuvkou, IP adresou + nezávislost na spuštění hostujících počítačů
 - mírně vyšší pořizovací náklady (HP JetDirect), dnes už minimální
 - nutno se do toho víc ponořit, námaha se ale vrátí



Sít'ové tiskárny

- dvě řešení připojení sít'ových tiskáren
 - a) konfigurace stanic pro přímý tisk na tiskárnu (TCP/IP)
 - + rychlejší, není potřeba zprostředkovatelský server
 - nemožnost managementu, řízení práv, hůře se překonfigurovává

Sít'ové tiskárny



- b) konfigurace stanic pro tisk přes server (který zprostředkovává vlastní tisk)
+ řízení práv, překonfigurovatelnost, jednotný management, sledování tisků
- může být nepatrně pomalejší (tisková úloha po síti „cestuje dvakrát“)

Sít'ové tiskárny



- nejlépe tiskárny jedné značky (společný management, např. HP JetAdmin)
- obecný poznatek – lidé neradi chodí od počítače někam jinam 😊
- je potřeba je to naučit, zvyknout si



Sít'ové tiskárny

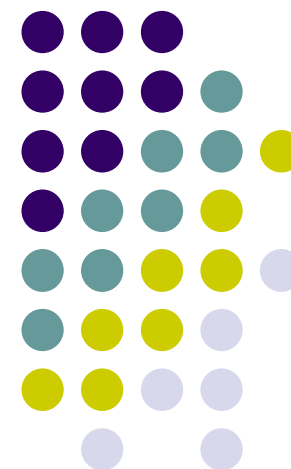
- robustní sít'ové tiskárny umí i více
- více formátů papírů, rychlejší, umí oboustranný tisk, sešívat výtisky, nižší náklady na tisk, fungují jako kopírka, skener atd., umí i autentifikaci proti doménovým účtům, zaheslování úloh, ukládání do paměti pro pozdější tisk

Sít'ové skenery



- zpravidla součástí multifunkčních sít'ových tiskáren
- práce jako s kopírkou – naskenovaný výtisk možno:
 - a) odeslat na mail (svůj, cizí)
 - b) automaticky uložit do definované sít'ové složky
 - c) odfaxovat (dnes už asi nemá valný význam)

6. Vzdálený přístup k ICT prostředkům



Vzdálený přístup k ICT prostředkům



- Jeden z požadavků ICT plánu
- Jak ho vnímat?
- zpřístupnění datových a programových prostředků navenek geograficky prostorám školy – mít data všude ve světě, na základě přístupu k internetu (= „data anywhere“)

Vzdálený přístup k ICT prostředkům



- Co všechno zpřístupnit? Komu?
Administrativa, kantoři, studenti?
- Zpřístupňujeme síťové disky, data, programy
- Ještě něco dalšího?

Způsoby realizace – vzdálený přístup



1. **www rozhraní** – musí umět nativně aplikace (webmail, web Bakaláři, groupware) – nejpohodlnější (na druhé straně stačí prohlížeč), svým způsobem ale nejzranitelnější (phishing apod.)
2. **WebDAV** – zpřístupnění složek ze sítě směrem do internetu, přes www prohlížeč, čtení, zápis
autorizace lokálními účty, vhodné https

Způsoby realizace

– vzdálený přístup

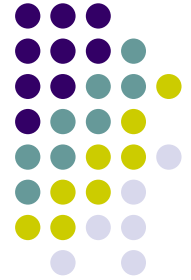


- 3. VPN připojení-klient**
= připojení do školní lokální sítě přes internet tak, jako bychom seděli přímo na ní
– přes internet se stáváme její součástí
– vhodné např. pro notebooky, které máme připojené do domény
- 4. Terminálové řešení** (u sebe mimo školu provozujeme a ovládáme obrazovku na dálku)



VPN klient

- výhoda možnosti lepšího šifrování, zabezpečení
- na nižší systémové úrovni (TCP/IP protokol – transportní vrstva)
- realizace:
 - a) hardware - Cisco firewall apod.
 - b) software - Kerio WinRoute, služba Směrování přímo ve Windows Server 2003), Linux



Terminálové připojení

- vše se odehrává na hostujícím stroji, k uživateli a od uživatele se po internetu přenáší pouze:
 - a) vstup (myš, klávesnice)
 - b) výstup (obrazovka, ale i tisk, zvuk atd.)



Terminálové připojení - realizace

1. VNC a podobné (RealVNC a odrůdy TightVNC, UltraVNC, ...)

zdarma, jednoduché na instalaci, pouze jedno připojení – jedno PC

- v základu není šifrováno
- + vhodné pouze pro administraci

Terminálové připojení - realizace



2. Windows Server 2003

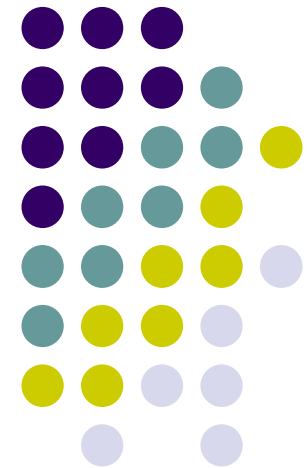
- samotná terminálová služba nic nestojí, stačí jen nainstalovat, dokupují se jednotlivé licence per user/per device (cca 1000 Kč na uživatele)
- výhodou je optimalizace (MS ví, jak volat přímo volání oken, na rozdíl od VNC)
- alespoň základní šifrování
- paralelní provoz více sessions (sezení) na jednom serveru – současně třeba 10-20 lidí, podle předpokládané zátěže odhadovat hw (říká se, že jeden uživatel = min. 128 MB RAM, u Windows Server 2003)
- nutno dostatečný upload internetu!

Terminálové připojení - realizace



- Citrix Metaframe atd.
 - profesionální řešení, lepší optimalizace přenosové trasy, prostředků, lepší iluze „přímého sezení u stroje“
 - výrazně dražší

7. Auditace, inventarizace





Auditace, inventarizace

- auditovat a inventarizovat lze hardware a software
- lze ručně – proč ne?
- s rostoucím rozsahem počtu počítačů roste náročnost ručního auditu (udržet rozsah i aktuálnost dat auditace)
- Lépe nějak automatizovat – existují různé nástroje, smysluplné jsou zpravidla drahé
- Serverová část + klientská část (zjišťuje a dodává informace pro server)



Auditace - hardware

- např. produkt OCS Inventory
 - + zdarma, vcelku funkční, jednoduché na nasazení na klientské části (stačí přidat příkaz do login skriptu), konfigurovatelnost, reporty
 - pouze hardware, náročnější na instalaci na serverové části (instaluje si vlastní www a db server, plus další komponenty, může snadno kolidovat s jinými aplikacemi na serveru) plus další komponenty
 - řešení u nás – vyhrazený samostatný starý server (s Windows 2000 Professional)



Auditace - software

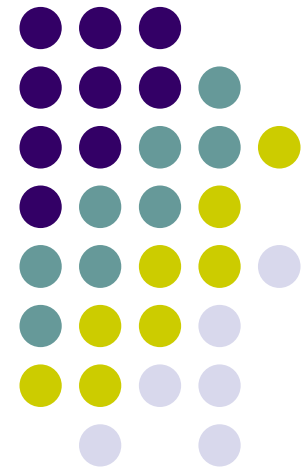
- např. AuditPro
 - kontrola instalovaného software – sesbírání, informace pro porovnání se skutečně zakoupeným stavem (proti fakturacím nebo licenčním smlouvám)
 - hlídání software nelegálně instalovaného na počítačích kantory, studenty



Auditace - software

- jsou dva způsoby, na základě kterého se zjistí, jaký sw je instalován na stanicích:
 - a) prohlédne registry a „Přidat/odebrat programy“ (někdy stačí, většinou nedostatečné)
 - b) proskenovává disk a zjišťuje spustitelné soubory, porovnává s databází (obdoba antivirů) – reportování na náš auditovací server
- komerční produkty, kvalitní jsou velmi drahé, licencování podle počtu stanic v síti, navíc nutno roční udržovací poplatky (za aktualizace programových bází)

8. Zálohování





Zálohování

- Význam záloh si uvědomíme až v okamžiku ztráty dat nebo dostupnosti služeb
- Co chceme zálohovat?
- Dvě otázky:
 - a) Jak předcházet haváriím?
 - b) Jak obnovit stav před havárií?



Zálohování

a) Jak předcházet haváriím?

→ redundantní systémy (např. diskové RAID), redundantní zdroje v serverech (vypadne-li jeden, nahradí druhý), redundantní servery (řešení přes DFS – Distributed File System)

Zálohování



b) Jak obnovit stav před havárií?

→ více záloh, i v čase, duplicitní zálohy, do více cílů (vypadne jedna, máme druhou)

Typy záloh



- a) Možnost obnovit nejaktuálnější zachovaný stav před havárií:
- zpravidla stačí „jedna záloha“
 - méně náročné na velikost zálohovacího zařízení
 - při uživatelských chybách riziko, že zálohujeme chyby, není historie

Typy záloh

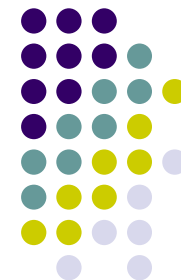


- b) Možnost získat starší data, z historie, např. zjistíme, že nás zajímají data ve stavu před x týdny, měsíci, roky
 - velmi náročné na objem zálohovacího zařízení
 - jsme schopni dohledat starší stavy

Zálohování – stínové kopie



- Od Windows Server 2003
- Možnost zapnout nad síťovou jednotkou
- V definovaný čas vytváří snímky dat – souborů a složek (např. v 7:00 a 12:00)
- Jsme schopni snadno uživatelsky k časům snímků dohledat stavy dokumentů a složek
- Funguje velmi systémově úsporně!



Jaké médium zvolit?

- disketa 😊
- optická média CD, DVD, BlueRay?
Moc malé 😞
- páskové zařízení?
Moc neohrabané, někdy i malé, navíc nepraktická výměna pásek (kdo to bude dělat? loadery drahé, pořád jen pásy – daná spolehlivost a nespolehlivost, špatná přístupová doba při obnovování – sekvenční přístup)



Jaké médium zvolit?

- pevné disky
 - zdá se, že nejpraktičtější, i cenově
 - výborný poměr cena/paměťová jednotka
 - rychlost ukládání, rychlost vybavení dat (přístupová doba)
 - možnost spojování do polí
 - lze připojit v podstatě k jakémukoli PC, serveru (interní, externí disky)
 - díky kapacitám disků je možné na jednom zařízení mít více záloh (držet historii), bez nutnosti vyměňovat médium



Plánování záloh

a) **Manuální**

Ize využívat i optická média (vypalování), při různých okamžicích (uzávěrky, před upgradem) – tedy to, co si pohlídáme

b) **Automatické**

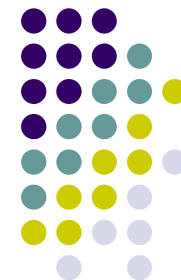
naplánovat úlohy k zálohování, nejčastěji na noční hodiny nebo víkend (představuje celkem zátěž pro zálohy), zálohovat denně (data) formou synchronizace, jednou týdně pak komplexnější zálohy

Zálohy

– nápad na zajímavé řešení



- externí HDD disk, s připojením na LAN – 0.5 a více TB
- samostatné vedení, umístění v jiné části budovy (např. rack)
- spojení se zálohovacím serverem, samostatnou linkou, na vyhrazenou druhou síťovou kartu v serveru (oddělení dat pro odposlech, plus zvýšení výkonnosti přenosu dat – „duplex“)
- výhoda – vyšší odolnost proti krádežím nebo požárům (v budově obě události jistě neproběhnou najednou a ve stejném rozsahu)



Jak často zálohovat?

- nejčastěji jak to jde
- problém – velké množství dat (v dnešní době až stovky GB)
- každá záloha představuje zátěž (pro síť, zálohovaný server - přenosy)



Jak často zálohovat?

- jak minimalizovat? → zálohovat jen rozdíly (buď rozdíly nebo udržovat zrcadlovou kopii)
 - velmi vhodný produkt - 2BrightSparks SyncBackup SE (zdarma) - na synchronizaci
 - na plné zálohy např. Cobian (zdarma)
- většinou kopírujeme soubory, dostačující
- u aplikačních serverů (SQL atd.) nutno využívat jejich proprietárních zálohovacích nástrojů, zálohovat teprve až výsledně vzniklý soubor



Strategie zálohování

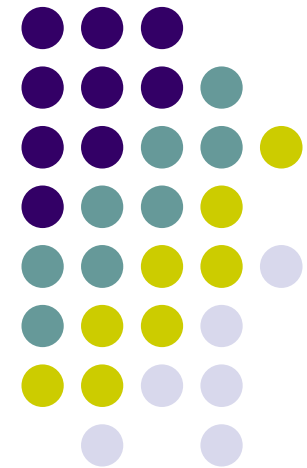
- nutit uživatele ukládat data na síť
- zálohovat především data na síti
- zálohovat na různé cílové jednotky (redundance záloh) – ne každá záloha se musí povést, být funkční
- u vybraných aplikací (např. školní jídelna - nelze provozovat ze sítě) vytvořit zálohovací prostředí na dané stanici, naučit uživatele spouštět příslušnou dávku (zálohující na síť) --- částečné přenesení odpovědnosti na uživatele



Strategie zálohování

- kontrolovat provedené zálohy
- pozor! Vytvořená záloha sama o sobě není zárukou obnovy! Je potřeba občas vyzkoušet obnovu nanečisto (týká se aplikačních serverů, SQL serverů – tam, kde nevidíme na funkčnost v podobě pouhých souborů)

9. Připojení k internetu, server, e-mail, groupware





Připojení k internetu

- každý stroj v síti svůj internet – neefektivní, drahé
- připojení k internetu se vždy sdílí, má to i další výhody (ochrana firewallem)
- vyhrazené zařízení, zprostředkující internet
- pro malé sítě stačí router (krabička), pro větší sítě celý server s routovací funkcí



Internetový server

- **routing** - překlad adres (NAT, zjednodušeně PAT)
- **proxy server** – vyrovnávací paměť na stránky, filtr obsahu, autentifikace/ověření přístupu – zrychlení přes cache mělo význam spíš dříve, dnes je to někdy komplikace (když špatně proxy server předkládá stránky uživatelům)
- **e-mailové služby** – SMTP, POP3, webmail
- **www server** – pro vlastní aplikace

Vlastní internetové připojení



- Jak rychlé potřebujeme?
- Jakou symetrii download/upload?
- Jakou potřebujeme garanci dostupnosti?
- Stačí domácí typ připojení?
ADSL/kabelovka?



Rychlost připojení

- zpravidla připojení bývá asymetrické (ADSL, kabel)
– vysoký download, nízký upload
- nízký upload silně ovlivňuje download, rychlost odezev (i v případě full duplexu)
- čím upload blíže downloadu, tím průchodnější linka
- vyšší upload potřebujeme, pokud provozujeme vlastní poštovní server (SMTP), www server apod.
- vyšší upload potřebujeme, pokud používáme vzdálený přístup k ICT prostředkům
- vyšší upload je drahý, některé technologie mají strop (ADSL/kabel)



Garance dostupnosti

- levná domácí připojení podle smlouvy garantují řešení problému např. až do druhého dne
- může to být pozdě, zvláště pokud provozujeme vlastní aplikace navenek
- drahá komerční řešení – doba reakce např. do 30 minut (proaktivní přístup provozovatele)



Elektronická pošta

- Mít vlastní doménu (např. @gymvod.cz)
- Většinou ji už stejně máme (jinak cca 300 Kč ročně)
- Možnost správy účtů vůči doméně (pokud to mailserver umí)
- Kdo všechno?
Vedení? Kantoři? Studenti?

Groupware



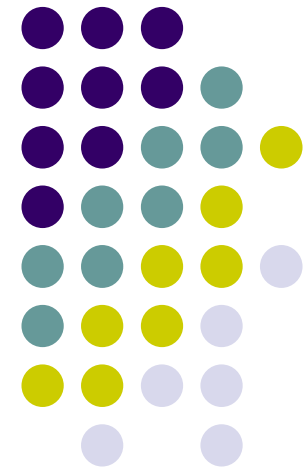
- slouží ke sdílení dokumentů, kontaktů, kalendáře, plánů akcí mezi uživateli, ve www prostředí
- příklady groupware – Microsoft SharePoint Portal Server / Services, 602 LanSuite 5 Groupware
- systém práv, ověřování

Groupware



- často propojeno přímo s e-mailovým serverem (602)
- SharePoint – jde dál, umožňuje programovat procesní zpracování činnosti, dokumentů, umožňuje verzování dat
- SharePoint Portal Services zdarma, plná verze placená
- Je to všechno zapotřebí? Nevystačíme si postaru?

10. Antivirová a antispam řešení



Antivirová a antispam řešení



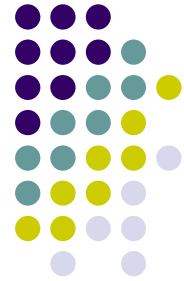
- volit kombinaci různých produktů nebo ucelená řešení?
- Různé druhy produktů – některé pouze antiviry, některé kombinují navíc i antispam, antiphishing, antispyware
- Jaký produkt vhodný?

Antivirová a antispam řešení



- AVG, dnes ve verzi 8 – jeho původní cenová výhoda pro školství se stírá
- Eset NOD32, Norton Antivirus atd.
- Licencování zpravidla na počet stanic v síti
- Vhodnější produkty, které umožňují dokupovat licence po jedné, nikoli pásmově

Antivirová a antispam řešení



- důležitá je údržba, časté aktualizace
- vhodné řešení zvolit takový produkt, který umožňuje lokální síťovou správu, management, vhodné i pro vzdálenou instalaci na stanice
- možnost nastavit stanice tak, aby si aktualizace bází stahovaly z tohoto management serveru a nikoli přímo z internetu (úspora internetových přenosů – za stanice stáhne od výrobce z internetu aktualizace a ty pak nabízí ke stažení v lokální síti)

Antivirová a antispam řešení



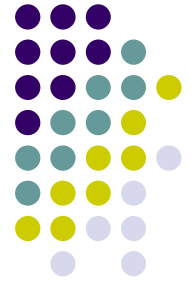
- Výhoda síťového managementu – možnost zpětné vazby ze stanic, víme, kde se co děje, lze reportovat, sbírá se na jednom místě
- Problém – zpravidla nestačí produkt koupit, ale nutno platit ročně udržovací poplatky za aktualizace produktu a virových bází (řádově až desetitisíce ročně, nutno s nimi počítat v rozpočtu školy)

Antivirová a antispam řešení



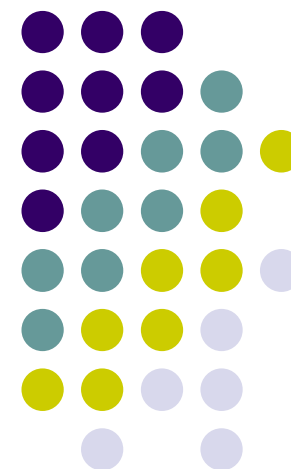
- Rostoucí komplexnost antivirových programů (zahrnují v sobě antispam, antispyware, kontrola odkazů a obsahu na www, různé typy rezidentních štítů)
 - zvyšující se zátěž na počítače, výrazné zbrzdění (i o polovinu), dobře funguje jen na nejnovějších strojích (i „čtyřjádra mají co dělat“)

Antivirová a antispam řešení



- Pozor na nepřekombinování a násobení antivirových ochran (na stanici + na serveru + internet serveru)
- důležitá optimalizace a nalezení kompromisu účinnosti a rychlosti
- vypínat nepotřebné části řešení

11. Bezpečnostní záplaty, aktualizace systému



Bezpečnostní záplaty, aktualizace systému



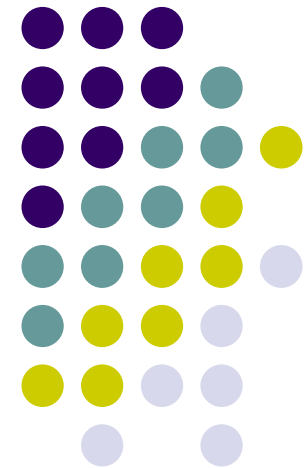
- ponechat nastavení Windows 2000/XP pro stahování oprav, aktualizací
- případně vynutit skupinovými politikami, lze měnit hromadně pro celou síť i chování, např. možnost odkladu instalace, restartu stanic uživatelům

Bezpečnostní záplaty, aktualizace systému



- zvážit možnost instalace Windows Server Update Services – stanice aktualizace nestahují přímo každá zvlášť z internetu, ale WSUS stahuje za ně a tyto stanice pak už stahují, jsou řízeny z WSUS
- úspora internetových přenosů
- optimalizace a řízení “vlastních aktualizací“

12. Software



Software



- Komerční či nekomerční?
- Preferovat jedno nebo druhé?
- Nejlépe kombinovat obojí

Software



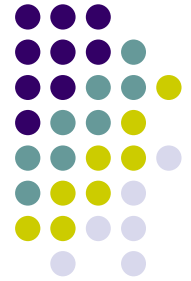
- a) **komerční produkty** – s těmi se budou studenti a učitelé setkávat dál v životě nejčastěji (typicky MS Office)
- b) **produkty zdarma** – možnost ukázat alternativy, jiné funkce, výhody, porovnání (OpenOffice), možnost i touto cestou alternativy protlačit

Komerční + nekomerční software



- možnost instalovat souběžně
- tam, kde to nejde, tak zvážit možnost demonstrací pomocí např. virtuálních počítačů (MS Virtual PC 2007 - zdarma)

Komerční + nekomerční software



- Otázka komerční nebo nekomerční znovu?
- Pokud vybrat jedno nebo druhé, které zvolit?
- Nejlépe to nejpohodlnější!

Komerční + nekomerční software



- Ve školství se zpravidla často najdou peníze na pořízení věcí než na mzdy 😊
- Šetřete si svoji práci!
- Typická ukázka – provozovat servery na Linuxu nebo Windows Server?
- Jaké jsou lidské náklady na administraci?



Komerční software

- Sledovat které produkty existují v EDU verzi
- Nebát se i jednat s výrobcí
(zvláště pokud by výsledná částka vyšla nesmyslně vysoko)



Komerční software

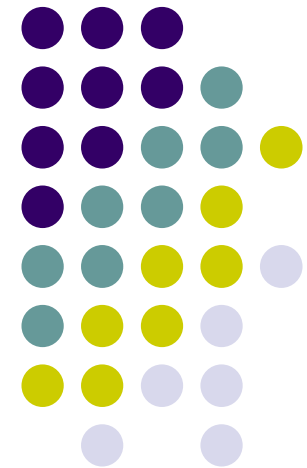
- U komerčního software se zaměřit na produkty s plošnou licencí (nezávisí na počtu instalací, licence platí na školu a často i na doma pro kantory nebo studenty)
- Příkladem jsou české produkty např. Zoner Callisto, Zoner Photo Studio, Altap Salamander



Komerční software

- Jsou produkty, které jsou v jednotlivých licencích poměrně drahé (i v EDU cenách)
- Nicméně se dodávají např. ve variantách pro učebnu, např. 15+1 licence (15 studentských, 1 kantorská) – za velmi výhodnou cenu, která odpovídá cca 2x samostatným běžným licencím.
- Příklad: Macromedia Studio, Paint Shop Pro atd.

13. Hardware





Hardware

- Jak drahý je náš čas?
- Kolik ho máme volného?
- Kolik nám ho škola zaplatí?
- Budeme si stavět počítače?
- Necháme si je stavět?
- Budeme kupovat hotové značkové?



Hardware

- Co je dnes nejdražší?
- Práce! A náhradní díly a jakýkoli servis okolo
- Je vhodné tuto část víceméně outsorcovat, pokud nejsme fandové



Hardware

- Mít jednoho dodavatele hw, na dlouhodobou spolupráci
- Budou mít sami zájem, úspora z rozsahu, osobnější přístup
- Nemusíme navíc řešit „od koho jsme tento počítač koupili“
- Obracení se na jeden servis, zajištění dopravy, minimalizace starosti



Hardware - záruky

- Je potřeba se zaměřit na záruku
- Čím delší, tím lepší – velké úspory.
Typická je 3-letá záruka
- U serverů zvažovat dokupování zvláštních prodloužených záruk (např. u HP jsou to Carepaqy, někdy jsou i v ceně serveru, NBD varianta umožňuje reagovat servisu do druhého pracovního dne přímo na místě)
NBD = Next Business Day OnSite
NBR = Next Business Day Response