

Naša veľká/malá sieť

Prológ k seriálu

Pojmy ako LAN, WAN, ISDN, ATM, Ethernet, FastEthernet sa dnes stávajú čoraz bežnejšími. Táto oblasť už nie je výsostnou doménou počítačových mágov a miliónových investícií. Samozrejme, sú oblasti, v ktorých sú potrebné špičkové znalosti a veľké skúsenosti expertov a, pravdaže, aj tie peniaze je treba. No veľká časť malých spoločností si nemôže dovoliť platiť drahé analýzy a implementovať špičkové systémy špičkových výrobcov. A načo aj, keď ich podnik má iba 5-10 počítačov, rozložených v 4 kanceláriách, a v podstate potrebujú iba zdieľať tlačiarne, prístup do internetu, nejaký ten e-mail a podobne. Tento seriál by mal práve dať návod, ako si takúto sieť urobiť, nakonfigurovať a rozumne používať. Nie, nelakajte sa! Nikto od vás nežiada, aby ste ešte dnes kúpili vítačku a montérky. Paralelne s návodmi, ako sieť budovať, tu budeme uvádzať aj tipy a rady pre tých, ktorí si ju radšej nechajú vybudovať.

Všetky informácie spomínané v tomto seriáli budú formulované hlavne s dôrazom na použiteľnosť, a teda tu nečakajte traktáty o funkcii jednotlivých bitov v poli Options v hlavičke IP paketu a podobne. Preto sa zameriame iba na najbežnejšie používané produkty a technológie, ako sú štruktúrované kabeľáže, Ethernet a Fast Ethernet, rozbočovače (huby) a prepínače, sieťové operačné systémy a ich konfigurácia a pod. Samozrejme, všetky informácie budú dopĺňané on-the-fly, t. j. „za jazdy“, tak, aby sme vám čo najviac vyhovelí. Tým sa iba snažíme naznačiť, že ak budete mať akúkoľvek otázku v oblasti týkajúcej sa tohto seriálu (a vlastne akúkoľvek otázku dotýkajúcu sa počítačových sietí), stačí, ak pošlete e-mail na adresu siete@pcrevue.com a my sa

1. budeme snažiť zodpovedať ju
2. ak bude zaujímavá, pokúsime sa ju obšírnejšie vysvetliť v samostatnom článku.

Pred začatím budovania siete, či už veľkej, alebo malej, je potrebné predovšetkým čo najpresnejšie odpovedať na pár otázok:

1. Aké sú moje problémy?
2. Vyrieši ich počítačová sieť?
3. Aká je situácia v mieste, kde by mala byť inštalovaná počítačová sieť?
4. Aká by mala byť nová sieť?
5. Som schopný zvládnuť návrh/realizáciu tejto siete sám?

Odpovedať na predchádzajúce otázky je potrebné, pretože veľa problémov v podniku nesúvisí s potrebou vybudovať počítačovú sieť. Manažéri podnikov a aj samotní používatelia počítačov si často myslia, že sieť automaticky vyrieši problém vnútrofiriemnej komunikácie, ktorý je asi najčastejší (pokiaľ nepočítame ekonomické problémy). Rovnako často si používatelia predstavujú, že sieť automaticky zvýši ich produktivitu, rozšíri ich možnosti. V tomto momente je dobré uvedomiť si, že sieť je iba nástroj na dosiahnutie týchto predstáv. A každý nástroj potrebuje majstra, ktorý ho ovláda. Nie, nechceme vás strašiť, ale všetky predchádzajúce problémy sú najmä organizačného charakteru a sieť ich nevyrieši. Preto nie je dobré robiť si prehnané ilúzie o tom, čo všetko sa zmení po inštalácii siete. Váš pohľad by mal byť realistický.

Na realizáciu počítačovej siete veľmi vplyvujú aj podmienky, do akých má byť inštalovaná. Je vhodné prv, ako sa

rozhodnete sieť budovať, komplexne zmapovať požiadavky používateľov, konfigurácie počítačov, používané programové vybavenie, rozmiestnenie tlačiarň, rozmiestnenie a rozmery miestností, lokalizovať predpokladané zdroje problémov (napr. transformátory, elektromotory, rozvody elektrického prúdu, agresívne prostredia). Dôkladná analýza situácie vám dá odpoveď na ďalšiu otázku: Aká by mala byť nová sieť?

Konfigurácia a požiadavky počítačov napovedia, či je rozumné umiestniť v sieti server alebo stačí iba zaviesť zdieľanie zdrojov jednotlivých počítačov, aký výkon sa očakáva od počítačovej siete (náročný ekonomiko-informačný systém vyžaduje vyšší výkon ako bežné kancelárske aplikácie). Podobne je to aj s programovým vybavením, teda so softvérom. Častá je otázka: „Máme N počítačov. Ako budú zatažovať sieť?“ Táto otázka vo všeobecnosti nie je správne položená. Skôr by mala znieť: „Máme N počítačov, na ktorých používame tieto aplikácie. Ako budú zatažovať sieť?“ Rozdiel v záťaži a „zátazi“ sa vám pokúsime vysvetliť na príklade: bežný dokument vyprodukovaný v niektorom z kancelárskych balíkov (MS Office, Lotus SmartSuite ...) je v rozsahu niekoľko sto kilobajtov, ktorých prenos po sieti trvá niekoľko desiatin sekundy. Naproti tomu si vezmeme účtovnícku aplikáciu, ktorá potrebuje na vyprodukovanie zostavy v rozsahu niekoľko sto kilobajtov analyzovať dáta s veľkosťou niekoľko megabajtov.

Takže samotné požiadavky na výkon siete závisia nie tak od počtu staníc, ako od aplikácií, ktoré sa na nich používajú.

Pri rozhodovaní sa o tom, aká by mala byť nová sieť, je vždy najlepšie spojiť sa s niekým, kto už v oblasti počítačových sietí má skúsenosti. Najlepšie je ak si informácie potvrdíte z viacerých zdrojov. Zdroje informácií, ako sú informačné listy jednotlivých firiem skúste v prvom kroku použiť iba ako referenčné, t. j. dajte si ich kompletne vysvetliť. Problémom takýchto informácií býva, že všetky vlastnosti daného produktu alebo systému sa najčastejšie opisujú v superlatívoch a veľmi ťažko sa hľadá alebo vytvára nejaké porovnávacia tabuľka. Základným vodidlom pri budovaní vašej siete by však malo byť to, že ju budete najmenej na 3-4 roky, a teda nesnažte sa riešiť iba akútnu situáciu, ale myslíte aj na budúcnosť. Rovnako by ste nemali zabúdať na normy a štandardy. Je síce pravda, že väčšina produktov spĺňa aspoň minimálne požiadavky noriem, ale treba si na to dať pozor, lebo nekompatibilita zariadení by vám mohla spôsobovať problémy pri rozširovaní siete.

Návrh siete je v podstate až posledným krokom pred realizáciou siete. Pri malých sieťach sa môže otázka „Som schopný zvládnuť návrh/realizáciu tejto siete sám?“ zdať trápna a určite si väčšina z vás pomyslí, že návrh siete nie je nijaký problém. Čuduj sa svete, ale máte pravdu. Prvotný návrh naozaj nie je ťažký, veď papier znesie všetko. Najťažšie býva rozhodnutie o použití typu centrálného prvku siete. Toto je však pohľad iba na tú najzákladnejšiu časť siete, t. j. kabeľáž a aktívne prvky. A pravdepodobne pre takéto podcenenie kabeľáží asi 80 % výpadkov siete spôsobuje práve chyby v nich (o chybách v kábloch a chybách pri ich inštalácii si povieme v budúcom čísle) Náročnejšou časťou návrhu

sú už spomínané aktívne prvky siete. Pri nich sa treba rozhodnúť, aké služby má sieť poskytovať, a tým smerom následne orientovať aj návrh aktívnych prvkov. Či už použijete jednoduché rozbočovače, výkonné prepínače, alebo sa vo vašom riešení vyskytnú smerovače, je to vždy iba otázka služieb siete. Najzložitejšia časť návrhu siete je, samozrejme, návrh služieb siete, t. j. čo potrebujeme na to, aby sieť poskytovala také služby, aké od nej požadujeme. Na túto časť návrhu sa často zabúda. Je to také isté, ako keby ste si chceli kúpiť auto a nezaujímal by vás jeho spotreba. A zabúdanie stojí peniaze... A tak sa stáva, že po samotnej inštalácii siete sa príde na to, že tamtie dva počítače a tento server vlastne potrebujú komunikovať vyššou rýchlosťou a namiesto jedného fastethernetového portu potrebujeme tri a keby sme neboli kúpili ten prepínač, ale kúpili by sme iný, tak výsledné náklady mohli byť o 10 000 Sk nižšie, že v tamtej kancelárii potrebujeme už od budúceho mesiaca o dve zásuvky viac, lebo nastúpia noví zamestnanci a ten nový smerovač s drahým modemom sme tiež nemuseli kupovať, pretože teraz by sa hodilo pripojenie cez ISDN... Takéto a podobné chyby sú veľmi časté. Možno to nebude práve váš prípad, ale čo ak predsa?

Samotná realizácia je v prípade, že ste si pripravili vhodné podklady, jednoduchá. Predpokladá však, že ste odborníkom alebo máte k dispozícii odborníka na viac oblastí. Rovnako aj v tejto fáze treba dať pozor na to, z čoho chcete sieť urobiť. Na trhu sa našťastie vyskytuje veľké množstvo kvalitných kabeľážnych systémov, inštaláčného materiálu, komunikačných zariadení, prípadne iných častí počítačovej siete v niekoľkých kategóriách, delených podľa kvality, ceny, prípadne podľa iných vlastností. Naťahanie káblov, ich popripájanie a inštalácia zariadení ešte nič neznamená, lebo ďalším krokom je konfigurácia zariadení a počítačov. Pokiaľ však budete postupovať podľa nášho návodu (v budúcich číslach budú aj návody, ako „rozchodiť“ sieť a jej služby na rôznych platformách – Windows 9x/NT, Novell Netware, Linux), mali by ste to zvládnuť.

Ak bude realizácia poslednou časťou budovania vašej siete, tak ste geniálny dizajnér sietí a vynikajúci projektový manažér a pravdepodobne by ste sa mali zamestnať v niektorej z renomovaných firiem... Bohužiaľ, takmer vždy po prvotnej konfigurácii prichádza takmer nekončn fáza testovania, doladovania a rozširovania siete. Ako sme naznačili, v tejto fáze zotrváte asi naveky. Veľmi sa vám bude hodiť váš pôvodný návrh a celková dokumentácia siete. Sú to síce „papierovačky“, ktoré na začiatok určite robiť nebudete, ale časom im „prídete na chuť“.

Tak čo, ešte stále ste rozhodnutí, že si to urobíte sami? Ak áno, v nasledujúcich častiach tohto seriálu dostanete presné a najmä praktické informácie a postupy, ako čo urobiť a ako sa vyvarovať základných chýb. Bohužiaľ, nie je v našich silách „odfiltrovať“ všetky chyby, pretože ich vytvára sám život, a ako iste veľmi dobre viete, život sa správa tak, ako sa mu práve zachce...

Alebo ste rozhodnutí, že si sieť radšej necháte vybudovať? V každej časti budú uvádzané aj rady pre tých, ktorí budú komunikovať s dodávateľom...

Veľké problémy s malými sieťami

alebo Sprievodca budovaním malými sieťami

2. časť – Základy siete = kabeláž

Základný princíp znie: „Ak dve zariadenia (počítače) majú spolu komunikovať, musí medzi nimi existovať spojenie.“ A v našom prípade je ním metalický kábel (metalický kábel = kábel s kovovým jadrom, najčastejšie medeným).

V tejto časti sa teda budeme venovať tomu čo majú všetky počítačové siete spoločné, t. j. kabeláži. Niežby boli všetky počítačové siete postavené rovnako, ale drvivá väčšina z nich využíva tú istú technológiu. Určite ste už počuli o štruktúrovanej kabeláži alebo aspoň o koaxiálnej kabeláži. Aj keď sa dnes už koaxiálna kabeláž takmer vôbec neinstaluje, pretože nie je univerzálna, pokúsime vysvetliť oba základné systémy.

A. Koaxiálna kabeláž

Nebudeme sa venovať všetkým typom koaxiálnych kabeláží, ale sústredíme sa na jeden, a to na ethernetovú koaxiálnu kabeláž. Všimnite si slovo ethernetová. Znamená, že táto kabeláž bola/je/bude navrhnutá tak, aby na nej mohla fungovať prenosová technológia ETHERNET. Čo to je Ethernet a ako funguje, to sa dozviete v budúcich častiach. Zatiaľ vám musí stačiť iba to, že je to technológia, ktorú používa drvivá väčšina existujúcich počítačových sietí...

Návrh koaxiálnej kabeláže pre ethernet

Pokiaľ plánujete vybudovať novú sieť, zabudnite na koaxiálnu kabeláž, resp. uvažujte o nej iba ak musíte prepojiť maximálne 3-4 počítače alebo sa plánujete zo súčasných priestorov v najbližšom čase presťahovať. Túto časť ocenia hlavne tí, ktorí z nejakých dôvodov musia rozširovať/meniť už existujúcu kabeláž.

Základnými časťami sú:

- kábel,
- rôzne typy konektorov (I konektor, T konektor, BNC konektor na ukončenie kábla a zakončovací terminátor),
- sieťová karta (stretnete sa aj s pojmom NIC = Network Interface Card) – tá musí mať konektor pre koaxiálnu kabeláž. Vzhľadom na to, že sa koaxiálna kabeláž takmer vždy nahradí štruktúrovanou kabelážou, dajte prednosť radšej tzv. combo kartám. Tie majú konektory aj pre koaxiálnu, aj pre štruktúrovanú kabeláž.

Používané typy káblov sú:

- tenký koax** (*thinnet*) – rozpoznáte ho podľa toho, že je sivý a na vonkajšom obale kábla má označenie IEEE 802.3. Jeho lacnejšou alternatívou býva kábel RG58, ktorý je čierny a na rozdiel od tenkého koaxu má iba jednu vrstvu tienenia. Odporúčaný je sivý tenký koax, ktorý je síce drahší, ale vyhnete sa problémom s možným rušením,
- hrubý koax** (*yellow ethernet*) – ako napovedá anglický názov, jeho vonkajší plášť je žltý (yellow = žltý) a používal sa na preklopenie väčších vzdialeností. Jeho použitiu sa nebudeme venovať.

Konektory majú pri koaxiálnej kabeláži presne určenú funkciu: BNC konektorom sa ukončuje koaxiálny kábel, I konektor (nazývaný aj barrel) sa používa na napájanie koaxiálnych káblov, T konektor sa používa na pripájanie zariadení (počítačov, opakovačov ...) do počítačovej siete a zakončovací terminátor sa používa na ukončenie segmentu siete.

Spôsob inštalácie a použitie jednotlivých konektorov je pre koaxiálnu kabeláž kritický, t. j. nesprávne použitie

alebo nepoužitie správneho konektora môže viesť k nefunkčnosti celého segmentu siete. Veľmi častou chybou býva napríklad pripojenie počítača na sieť bez T konektora, priamo pomocou BNC konektora, prípadne sa stáva, že segment nebýva zakončený zakončovacím terminátorom (je to vlastne BNC konektor so zabudovaným 50-ohmovým rezistorom).

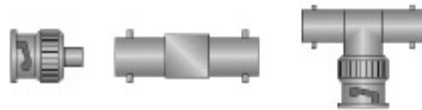


Obr. 1 Štruktúra koaxiálneho kábla (zľava: vonkajší obal z PVC, kovový oplet, hliníková fólia, izolačná vrstva plastu/dielektrikum, medený vodič)

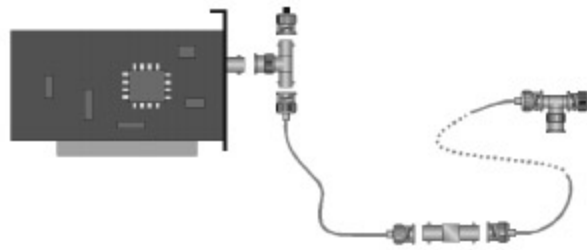
Inštalácia

Inštalácia počítačovej siete založená na koaxiálnom kábli je jednoduchá a pri dodržaní niektorých odporúčaní a zásad a trochu šikovnosti ju zvládne každý.

Ako už viete (alebo aspoň tušíte), koaxiálna kabeláž, pokiaľ spája viac ako dva počítače, sa skladá z viacerých



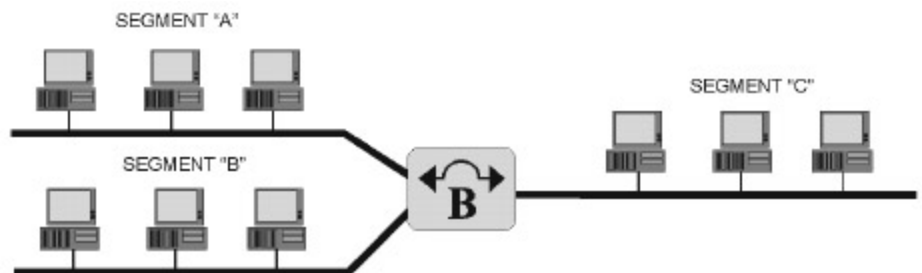
Obr. 2 Typy konektorov (zľava: BNC konektor, I-konektor, T-konektor, zakončovací terminátor)



Obr. 3 Použitie jednotlivých konektorov v koaxiálnej

kabeláži (pozor: segment musí byť na oboch koncoch ukončený zakončovacím terminátorom, ktorý je pripojený na I alebo T-konektor.)

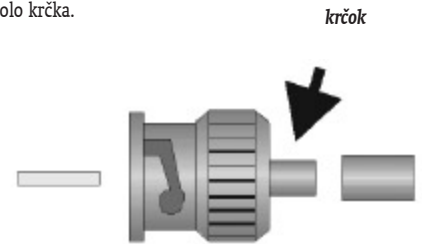
kusov koaxiálneho kábla ukončeného BNC konektormi a pospájaného T a I konektormi. Kritickým momentom inštalácie je práve ukončovanie koaxiálnych káblov BNC konektorom. Je to asi jediná možnosť, ako urobiť chybu. Pri inštalácii sa používajú dva nástroje: špeciálne odblan-



Obr. 5 Prepojenie segmentov pomocou sieťového mosta

kovacie kliešte a lisovacie kliešte. Odblankovacie kliešte sa používajú na odstraňovanie plášťa, kovového opletu, hliníkovej fólie a izolácie. Samozrejme, dá sa to urobiť aj nožikom, ale je to zdlhávavé a nepresné. Odblankovacie kliešte túto operáciu pomocou svojich troch nožov zvládnu naraz. Druhým krokom je inštalácia BNC konektora na takto pripravený kábel. BNC konektor sa dodáva v rozloženom stave.

Najprv sa medený vodič koaxiálneho kábla zasunie do kolíka a pomocou lisovacích klieští sa pevne spoja. Potom sa na kábel nasunie vývodka. V ďalšom kroku sa kolík cez krčok zasunie do tela BNC konektora a hliníková fólia spolu s kovovým opletom sa obmotajú okolo krčka.



Obr. 4 Rozložený BNC konektor (zľava: pozlátený kolík, telo konektoru, vývodka)

Následne sa na krčok nasunie vývodka a pomocou lisovacích klieští sa s ním pevne spojí. To je všetko. Najčastejšími chybami sú skratovanie konektora, t. j. niektoré z vlákien opletu sa spojí s vodičom, alebo zlé uchytienie vývodky, ktoré následne spôsobuje to, že sa kábel z konektora neustále vyťahuje. Konektor po inštalácii radšej vždy skontrolujte ohm metrom. Keď pripojíte jeden kontakt na kolík a druhý na vonkajšiu kovovú časť konektora, nesmiete namerať spojenie, resp. musíte namerať nekonečný odpor.

Ani inštalácia káblov nie je zložitá. Stačí ich iba pozapájať a na konce segmentov dať zakončovacie terminátory. Je však pár vecí, na ktoré si je treba dať pozor:

- Impedancia kábla musí byť 50 ohmov.
- Odpor terminátora musí byť 50 ohmov (tu je povolená odchýlka tuším +/-10%) Ak terminátory chýbajú alebo majú väčší/menší odpor ako 50 ohmov,

na konci kábla vzniká impedančná anomália, od ktorej sa potom signál odráža a ruší práve vysielaný signál.

- Aby sa kábel nelámalo, ohyby koaxiálneho kábla by nemali mať príliš malý polomer.
- Dĺžka segmentu by nemala presiahnuť 185 m. Je pravda, že väčšinou to funguje aj na viac ako 185 m, ale to je už bez záruky. Prídlhé segmenty signál utlmujú, takže sa nedostane ku vzdialeným staniciam a následne vznikajú poruchy v komunikácii. Dôležité je podotknúť, že 185 m je limit pre segment vrátane pripojovacích

kábel, lebo hlavne pri systémoch TWC alebo EAD, čo sú systémy s tzv. bezpečnostným kontaktom, sa často stáva, že bez pripojovacích káblov má segment povedzme 170 m, ale už pri použití 10 trojmetrových káblov sa z pôvodných 170 stáva 230 m. (Poznámka: Pri týchto systémoch sa používajú duplexné – dvojité – káble, a teda 3 m dlhý pripojovací kábel vlastne znamená predĺženie segmentu o 6 m.)

5. Nepripájajte medzi T konektor a sieťovú kartu ďalší kábel. Takýto „ypsilon“ vám síce môže fungovať, ale opäť je to bez záruky.

6. Treba dodržať topológiu siete.

Topológia ethernetovej siete založenej na koaxiálnom kábli je v rámci jedného segmentu vždy zbernicová, t. j. segment sa niekde začína a niekde končí. Neexistuje nijaká rozvojka alebo kruh. Jednotlivé segmenty však po prepojení môžu vytvárať aj hierarchickú alebo hviezdnicovú topológiu. Na prepojenie segmentov sa používajú opakovače (repeatery), mosty (bridge), prepínače (switch) alebo smerovače (routery). Najčastejšie však prvé dve uvedené zariadenia.

Odstraňovanie problémov v koaxových sieťach

Základným nástrojom pri odstraňovaní problémov je vždy ohm meter. Dokážete ním zistiť základné problémy, ako sú skrat, prerušenie, chýbajúci terminátor a nesprávny terminátor. Efektívnejším, ale finančne náročnejším spôsobom, ako zisťovať poruchy v koaxovej kabeľži, je zakúpenie si špeciálneho meracieho prístroja. Takéto prístroje dokážu presne lokalizovať každú zo spomínaných porúch (pri skrate, prerušení, impedančnej anomálii aj určitú vzdialenosť od poruchy), zisťovať šum, záťaž siete, percento kolízií atď. Takýmito prístrojmi sú napríklad výrobky firiem Datacom (www.ies.sk/datacom), Fluke (www.fluke.com) a Microtest (www.microtest.com). Pretože ide o produkty, ktorých ceny sa začínajú od 25-30 000 Sk, dáva väčšina dodávateľov možnosť zapožičať si tieto produkty.

Častým problémom počítačových sietí založených na koaxiálnom kábli býva ich priveľká záťaž. Tu spomínané prístroje síce dokážu detegovať, ale na jej odstránenie je potrebné do siete zakomponovať sieťový most (bridge) alebo prepínač (switch). Bohužiaľ, drvivá väčšina mostov a prepínačov má iba konektory vhodné pre štruktúrovanú kabeľžu, a tak sa nedá nespomenúť výnimka. Výnimkou je sieťový most/prepínač Brilan (www.tetrasoft.sk), ktorý je záchranou rozľahlých ethernetových sietí založených na koaxiálnom kábli. Je alternatívou k lacným prepínačom firiem Nortel, 3Com, Cisco, Cabletron a pod.

Náklady na vybudovanie

Počet staníc/počítačov je 5 a ceny sú uvádzané bez DPH.

Koaxiálny kábel	20 m	300 Sk
BNC konektor	8 ks	560 Sk
T-konektor	5 ks	400 Sk
Zakončovací terminátor	2 ks	200 Sk
Sieťová karta NE2000 (combo) TP/Coax	5 ks	2 000 Sk
Spolu		3 460 Sk

Aby sa predišlo poškodzovaniu kábla a možnosti rozpojiť sieť, je vhodné, ak sa káble inštalujú do plastových lišt. Výsledná cena siete sa tým síce zvýši, ale výrazne narastie aj jej spoľahlivosť.

Otázky pre dodávateľa

Žiadne. Pokiaľ môžete, koaxiálne siete si nedávajte inštalovať.

(Poznámka: Hmm...načo som potom toľko o tom písal...)

B. Štruktúrovaná kabeľža

Štruktúrovaná kabeľža je komplexný kabeľžný systém zahŕňajúci rôzne typy kabeľží - od kabeľží založených na krútenej dvojlinke (TP = twisted pair = krútená dvojlinka) cez optické kabeľže až po napr. rozvody káblovej televízie. Dôležitým znakom kvalitnej štruktúrovanej kabeľže je, že všetky systémy tvoria jeden kompaktný štruktúrovaný celok. V bežnej reči sa však pojem štruktúrovaná kabeľža často zužuje iba na kabeľžu založenú na krútenej dvojlinke a používanú najmä na prenos hlasu a dát.

Návrh štruktúrovanej kabeľže

Na rozdiel od koaxiálnej kabeľže sa návrhu štruktúrovanej kabeľže budeme venovať podrobnejšie.

Topológia takejto kabeľže je predovšetkým hviezdicová a pri väčších systémoch hierarchicko-hviezdicová. S týmto aspektom treba rátať už pri návrhu. Znamená to, že každý koncový bod/zásuvka je napojený na nejaké centrum.

3. časť - Základy siete = kabeľž

B. Štruktúrovaná kabeľža

Štruktúrovaná kabeľža je komplexný kabeľžný systém zahŕňajúci rôzne typy kabeľží od kabeľží založených na krútenej dvojlinke (TP = twisted pair = krútená dvojlinka) cez optické kabeľže až po napr. rozvody káblovej televízie. Dôležitým znakom kvalitnej štruktúrovanej kabeľže je, že všetky systémy tvoria jeden kompaktný štruktúrovaný celok. V bežnej reči sa však pojem štruktúrovaná kabeľža často zužuje iba na kabeľžu založenú na krútenej dvojlinke a používanú najmä na prenos hlasu a dát.

Návrh štruktúrovanej kabeľže

Na rozdiel od koaxiálnej kabeľže sa návrhu štruktúrovanej kabeľže budeme venovať viac.

Topológia takejto kabeľže je predovšetkým hviezdicová a pri väčších systémoch hierarchicko-hviezdicová. S týmto aspektom treba rátať už pri návrhu. Znamená to, že každý koncový bod/zásuvka je napojený na nejaké centrum. Samotný návrh dosť často závisí aj od použitého systému štruktúrovanej kabeľže. Na Slovensku

Ako sme už spomenuli, nebudeme sa venovať návrhu komplexných štruktúrovaných kabeľží, na to sú určené špeciálne školenia, ale zostaneme pri malých sieťach a z návrhu štruktúrovanej kabeľže si vezmeme iba nevyhnutné minimum.

Základnými normami pre štruktúrovanú kabeľžu sú americká EIA/TIA568A, európska EN 50173 a svetová IEC 11801. Hlavné rozdiely medzi týmito normami sú uvedené v tabuľke č. 1.

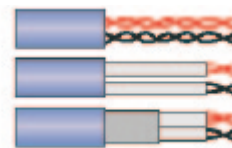
Pre nás, keďže sa snažíme dostať do EU, by mala byť záväzná norma EN 50173. Pokúsime sa teraz vyjadriť sa k jednotlivým riadkom tabuľky.

Prvé tri riadky hovoria o tom, aký typ metalických káblov je možné používať v kabeľži.

Používajú sa štvorpárové káble. Jedinou výnimkou je 150-ohmový dvoj párový kábel.

Rozdelenie káblov podľa tienenia

1. UTP - Unshielded Twisted Pair = netienený kábel
2. FTP - Foiled Twisted Pair = kábel, ktorý je tienенý hliníkovou fóliou
3. S/FTP - FTP kábel, ktorý má okrem hliníkovej fólie aj kovový oplet
4. STP - Shielded Twisted Pair = správne takto sú označované iba 150-ohmové dvoj párové káble IBM typ 1A, kde každý pár je tienенý zvlášť a navyše je kábel tienенý aj celkovo
5. S/STP alebo aj PiMF - Pair in Metal Foil = štvorpárový kábel, kde každý pár je tienенý zvlášť hliníkovou fóliou a zároveň sú tienенé hliníkovou fóliou aj všetky štyri páry spoločne



Používané typy kábla zhora: UTP, FTP, S/STP (PiMF)

Pozn: Nech vás nepomýli počet párov, majú tam byť štyri

Čo sa týka diskusie na tému tienенý alebo netienený, je sa radšej vyhnite. Pravdepodobne neexistuje jednoznačné rozhodnutie. Tienené káble sú preferované najmä v krajinách pod vplyvom Nemecka. Amerika je celá netienená (pozri normu EIA/TIA568A). Pre vaše rozhodovanie by malo stačiť, že v bežných priestoroch vám budú absolútne stačiť netienené káble, sú cenovo výhodnejšie a práca s nimi je jednoduchšia. Máte pochybnosti o funkčnosti? Spýtajte sa Američanov...

Občas sa vám môže stať, že sa stretnete s niekým, kto bude spomínať 120-ohmový kábel. Ten sa na Slovensku inštaluje dosť zriedka. Ak sa vám dostal do rúk, bol to asi Alcatel, pretože 120-ohmové kabeľže sa inštalujú vo Francúzsku a aj v krajinách Beneluxu.

Dalším riadkom je používaný typ optického kábla. Spomenutý je kábel 50/125. Najprv vysvetlíme túto skratku: priemer jadra optického vlákna je 50 mikrometrov (mikrónov) a celková hrúbka vlákna je 125 mikrometrov. Tento kábel nebol tak často inštalovaný ako kábel 62,5/125 mikrónov, no v poslednom čase sa s ním stretnete častejšie. Oba spomínané typy kábla sú multimódové (mnohovidové) typy a vzhľadom na ich dosah, ktorý je maximálne 2 km, sa používajú v sieťach LAN, prípadne na prepojenie budov na krátke vzdialenosti. Keď sme už pri optike, nedá nám nespomenúť aj singlemódový (jednovidový) kábel 9/100, ktorého dosah

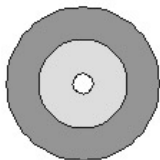
	EIA/TIA 568A	ISO/IEC 11801	EN 50173
100-ohmový kábel	iba UTP	odporúča	odporúča
120-ohmový kábel	nepodporuje	podporuje	podporuje
150-ohmový kábel	podporuje	podporuje	podp. iba v horiz. káb.
50/125 opt. kábel	nepodporuje	podporuje	podporuje
Kategórie komponentov	3, 4, 5	3, 4, 5	3, 5
Káble v zásuvkách	kat. 3 + kat. 5	kat. 3 + kat. 5	kat. 5 + kat. 5
Konektory RJ45	4-párové	2- a 4-párové	2- a 4-párové
Tienené konektory	nepodporuje	podporuje	podporuje
Zapojenie konektorov	T568A/T568B	iba zapojenie párov	iba zapojenie párov

Tabuľka č. 1

sa rozšírilo niekoľko typov štruktúrovanej kabeľže. Predovšetkým sú to systémy AMP, IBDN, IBM, Alcatel, CTSe, Systemax. Toto boli tzv. značkové systémy vyznačujúce sa predovšetkým svojou komplexnosťou a tradíciou. V menších sieťach, povedzme do 200 pripojných miest sa uplatňujú aj iné systémy, ktoré nie sú také komplexné a nemajú také množstvo príslušenstva ako už spomínané značkové systémy, ale ponúkajú veľmi rozumnú alternatívu najmä v prípadoch, keď hlavnú rolu zohrávajú financie. Medzi takéto systémy patria Solarix a napr. BICC Millennium. Samozrejme, rozdiely v systémoch existujú, ale dôležité je, že všetky spomínané systémy spĺňajú potrebné normy.

je až 40 km. V podstate je jedno, ktorý z uvedených káblov použijete.

Rovnako ako s tienením je to aj s kategóriami/triedami. Zatiaľ najvyššia trieda pre metalické káble je trieda D (zodpovedá kategórii 5). Sú však výrobcovia, ktorí ponúkajú triedy E alebo D+ a podobne. Je to v podstate iba snaha o predvídanie vývoja. Takéto predvídanie však nemusí byť správne. Pre káble triedy D, resp. kategórie 5 platí zásada: čím väčšie ACR tým lepšie (ACR – Attenuation to Crosstalk Ratio = rozdiel útlmu a pre-sluhu). Podľa normy musí byť hodnota ACR väčšia ako 10 dB. Dôležité je aj nezabudnúť na fakt, že systém patrí do tej triedy, do ktorej patrí jeho najhorší komponent. Teda



Prierez optickým vláknom od okraja k stredu: ochranný lak, cladding, jadro vlákna

ak mám káble kategórie 5 a konektory alebo zásuvky kategórie 3, tak celý systém je v podstate systémom kategórie 3. Preto je asi správne, že norma EN 50173 nepovoľuje kombinovať v zásuvkách konektory rôznej kategórie, aj keď na telefóny stacia konektory kategórie 3.

Takto sme sa dostali ku konektorom. Štandardným konektorm pre metalickú časť štruktúrovanej kabeláže je RJ-45. Je to 8-pinový modulárny konektor.

Podobá sa na konektory RJ-11, ktoré sa používajú v novších typoch telefónnych prístrojov. Tie sú však iba 6-pinové.

Toľko teória z rýchlika, vráťme sa k praxi.

Tak ako pri koaxiálnej kabeláži aj tu začneme s tým, z čoho sa vlastne štruktúrovaná kabeláž skladá. Hlavnými časťami sú:

1. pripojovací kábel (line-cord)
2. zásuvka
3. horizontálna kabeláž
4. prepojavací panel (patch-panel)
5. prepojavací kábel (patch-cord)

Pripojovací kábel slúži na pripojenie zariadenia/počí-



Modulárny konektor RJ45

tača do počítačovej siete. Názory na vlastnosti pripojovacieho kábla sa rôznia. Zástancovia jedného systému tvrdia, že kábel musí byť lankový, aby sa nelámala, v inom systéme zasa odporúčajú použiť kábel s drôteným jadrom, lebo to má zasa lepšie vlastnosti. Rovnako názory na maximálnu dĺžku sú rôzne.

Zásuvka je ukončením horizontálnej kabeláže na strane používateľa a je vlastne prístupovým bodom do kabeláže. Zásuvka má spredu jeden až 12 konektorov/portov RJ45, do ktorých sa pripájajú pripojovacie káble, a zozadu sa na konektory IDC pripája horizontálna kabeláž. Stretnete sa so zásuvkami na omietku a pod omietku. Tie prvé, ako ich názov už napovedá, sa dajú montovať priamo na stenu. Podomietkové potrebujú na inštaláciu inštaláciu škatulku, podobne ako elektrické zásuvky a dajú sa umiestňovať do steny alebo do žlabu. Keďže sme sa už

zmienili o tienení, ak inštalujete tienenu kabeláž, mali by ste používať tienené zásuvky. Vyskytujú sa dva druhy: celotienené a polotienené. Pre vás by malo byť dôležité to, že obe neprerušujú tienenie. Z hľadiska funkčnosti je jedno, ktorú použijete. Ak inštalujete netienenú kabeláž, použite netienené zásuvky.

Konektor IDC (Insulation Displacement Connector = konektor odstraňujúci izoláciu) je vlastne „zarezávací“ konektor, do ktorého sa vloží izolovaný vodič a pomocou špeciálneho nástroja, nazývaného zarezávací nôž alebo aj boxovací nôž, sa do konektora IDC zatlačí.



Hlavné časti štruktúrovanej kabeláže zľava: koncové zariadenie (počítač so sieťovou kartou, telefón...), pripojovací kábel, zásuvka, horizontálna kabeláž, prepojavací kábel, aktívne zariadenie (HUB, switch, telefónna ústredňa...)

Pozn.: Pripojovací panel, prepojavací kábel a aktívne zariadenie sa zvyčajne nachádzajú v rozvážači (racku).

Horizontálna kabeláž spája zásuvku s rozvážačom, presnejšie povedané, s prepojavacím panelom v rozvážači. Názov horizontálna vznikol z dôvodu, že jedným z princípov štruktúrovanej kabeláže je umiestňovať na každé poschodie budovy samostatný rozvážač. Káble spájajúce rozvážač so zásuvkami sa potom šíria v horizontálnom smere, t. j. neprechádzajú cez poschodia. Rozvážače na jednotlivých poschodiach sa potom spájajú vertikálnou kabelážou. Dĺžka horizontálnej kabeláže nesmie podľa normy presiahnuť 90 m.

Prepojavací panel (alebo aj patch-panel) je ukončením horizontálnej, a ak existuje vertikálnej, aj vertikálna kabeláže v rozvážači. Počet portov/zásuviek na prepojavacom paneli býva v rozpätí od 12 do 48. Pri týchto paneloch sa stretnete s označením ich výšky v tvare napr. 2U. Jednotka U označuje približne 4,54 cm. Teda panel 2U je vysoký asi 9 cm. S jednotkami U sa stretnete aj pri rozvážačoch.

V rozvážačoch (rackoch) bývajú umiestnené prepojavacie panely, aktívne zariadenia a vlastne takmer všetko, čo chcete ako-tak chrániť pred vplyvom vonkajšieho prostredia. Štandardné rozvážače sú 19" (palcov) široké, ak chcete mať väčší poriadok, lepšie sú rozvážače s vonkajšou šírkou 800 mm, lebo je v nich miesto na postranné organizéry káblov. Ich výška a hĺbka varuje v závislosti od ich použitia. Výška sa určuje v U, napr. 42U.

Poslednou základnou časťou štruktúrovanej kabeláže je prepojavací kábel. Všetky systémy uprednostňujú lankový kábel, lebo je predpoklad, že by sa konfigurácia siete mohla meniť, a teda prepojavací kábel musí byť ohybný, aby sa nelámala.

Dôležitým vzorcom pre štruktúrovanú kabeláž je: $A + B + C = 100$ a zároveň $A + B = 10$, kde A je dĺžka pripojovacieho, B dĺžka prepojavacieho a C je dĺžka horizontálneho kábla.

Uvedený vzorec platí pre štruktúrovanú kabeláž triedy D (alebo kategórie 5, ak chcete). Pre ostatné triedy uvádza limitné dĺžky *tabuľka č. 2*.

Inštalácia

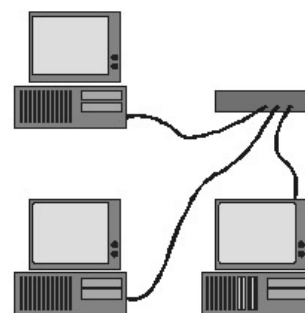
Rovnako ako pri koaxiálnej kabeláži aj pri štruktúrovanej kabeláži určenej pre malú sieť asi 10-20 pripojných miest) nie je inštalácia náročná. V podstate sa skladá z

niekoľkých základných častí: vírtanie a búranie, inštalácia trás, ťahanie káblov, inštalácia zásuviek a prepojavacích panelov a zakryvanie trás.

Prv ako začnete robiť inštaláciu, je dobré pripraviť plány, kadiaľ budete kabeláž viesť. Tieto plány by mali vychádzať z plánov budovy a mali by vyhovovať normám t. j. mali by sa dodržať pravidlá týkajúce sa odstavu trasy od zdrojov rušenia, ako sú elektrické rozvody, žiarivky a pod.

Topológia štruktúrovanej kabeláže je hviezdicová, teda taká istá ako pri telefónoch – ku každému počítaču

ide jeden kábel:



K inštalácii trás sa vyjadrovať nebudeme, je závislá od materiálu, s ktorým pracujete, a od toho, akí ste šikovní...

Ťahanie káblov je pri takýchto malých sieťach nenáročná práca, preto nemá zmysel hlbšie sa mu venovať. Pri väčších sieťach by to bolo zaujímavejšie, lebo treba dávať pozor na to, cez koľko rohov môžete ťahať, koľko metrov môžete zatahnuť naraz a pod. Dôležité je to, že káble sa ťahajú v *označených* zväzkoch smerom od rozvážača k zásuvkám a odporúča sa nechať tak na strane rozvážača, ako aj na strane zásuvky nejakú rezervu – v rozvážači 3-5 m, pri zásuvke 1-2 m.

Na inštaláciu zásuviek a prepojavacích panelov budete potrebovať zarezávací (boxovací) nôž. Niektoré systémy, ako napríklad systém IBDN, umožňujú inštalovať konektory prakticky bez použitia nástrojov, ak však máte slabšie prsty, musíte použiť kliešte... Pri konektorovaní sa používajú dve základné typy zapojenia: T568-A (tzv. ISDN zapojenie) a T568-B (tzv. ALT alebo Token Ring zapojenie). Je prakticky jedno, ktoré použijete. Odporúčame však používať zapojenie T568-A.

Keď si chystáte kábel, ktorý následne ukončíte v konektori IDC, či už na strane zásuvky, alebo na strane prepojavacieho panela *musíte* dodržiavať nasledujúce obmedzenia: rozpletie páru nesmie presiahnuť 13 mm a celkové odblankovanie kábla by nemalo presiahnuť 2,5 cm. V prípade, že potrebujete odblankovať kábel na väčšom úseku ako 2,5 cm, t. j. odstránite ochranný obal kábla, je potrebné uložiť jednotlivé páry tak, aby boli čo najviac pri sebe – akoby ich držal obal.

Po inštalácii zásuvky je vhodné označiť ju jednoznačným číslom, napr. 04X002/1 označuje prvý port druhej zásuvky, ktorá je napojená na rozvážač č. 04. Na označovanie sa často používajú popisovače laminovaných pásov,

pretože sa jednoducho obsluhujú a pásky sú estetické a dobre odolávajú vplyvom prostredia. Takéto popisovače vyrába napr. firma Brother (www.ies.sk/hw/brother).

Dôležitým a často chýbnym komponentom kabeľáže sú prepojenia káblu. Často sa stáva, že sú nesprávne nekonektorované. Pri nich sa používajú už spomínané spôsoby T568-A a T568-B, tak ako sú zobrazené na obrázku. Problémom býva prepojenie dvoch aktívnych prvkov napr. prepínač-HUB, lebo je tu potrebné použiť tzv. prekrižený kábel. Ide o kábel, ktorého jeden koniec je ukončený podľa T568-A a druhý koniec podľa T568-B.

Odstraňovanie problémov v sieťach TP

V podstate platia tie isté princípy ako pri odstraňovaní problémov v koaxiálnej kabeľži, ale pri štruktúrovanej kabeľži sú špeciálne meracie prístroje nevyhnutné, keďže treba merať veličiny ako NEXT a tie sa dajú merať iba týmito prístrojmi. Tieto prístroje sa rovnako dajú použiť na certifikáciu kabeľáže. Príkladom sú výrobky firiem Datacom (www.ies.sk/datacom), Fluke (www.fluke.com) a Microtest (www.microtest.com).

Tabuľka č. 2 Limitné dĺžky pre segmenty podľa normy EN 50173

Médium	trieda A	trieda B	trieda C	trieda D	optická
kábel kategórie 3	2000	200	100 ¹⁾	-	-
kábel kategórie 5	3000	260	160 ²⁾	100 ¹⁾	-
150-ohmová STP kábel	3000	400	250 ²⁾	150 ²⁾	-
Multimódový opt. kábel	-	-	-	-	2000
singlemódový opt. kábel	-	-	-	-	3000 ³⁾

1. Metrová dĺžka zahŕňa aj 10-metrové prepojenie a pripojenie káble. Presná špecifikácia je: max. 90 m pre horizontálnu kabeľáž, 7,5 m pre prepojenie patch-káble a 3 konektory tej istej kategórie.

2. V prípade, že horizontálna kabeľáž by mala presiahnuť 100 m, je odporúčané konzultovať aplikáciu.

3. 3000 m limit je iba limitom z pohľadu normy a nie je fyzickým limitom kábla. Limit kábla je v skutočnosti až 40 km.

Náklady na vybudovanie

Rozpočet je urobený na kabeľáž s 10 dvojzásuvkami. V rozpočte sa použili prvky štruktúrovanej kabeľáže SOLARIX.

Ceny sú bez DPH a pochádzajú z dilerického cenníka.

lišta MK 16/40	20 m	1100 Sk
netienená dvojzásuvka 2xRJ45	10 ks	3050 Sk
netienený prepojený panel 24xRJ45	1 ks	3278 Sk
UTP kábel	150 m	1350 Sk
prepojený kábel 1 m	10 ks	1080 Sk
pripojovací kábel 3m	10 ks	1390 Sk
aktívny prvok - HUB 12-portový	1 ks	asi 10 000 Sk
Spolu		21 248 Sk

Použitie skratky

NEXT, AMP, ACO, UTP, STP, FTP, PiMF, RJ-45, U, IDC, TP

Odporúčania pre odberateľa

- Pri stanovovaní rozsahu kabeľáže sa radšej zamyslite nad budúcnosťou a navrhnete ju aspoň s 10-15 % rezervou.
- Vždy trvajte na tom, aby sa na dodávku uzavrela zmluva o diele.
- Pri porovnávaní ponúk porovnávajte nielen cenu, ale aj množstvo materiálu, ktoré bolo v cene zahrnuté. Cenové ponuky sa málokedy rovnajú, pretože dodávatelia môžu ináč umiesniť zásuvky, použiť iné trasy a pod.
- Trvajte na tom, aby po dodávke bola vypracovaná projektová dokumentácia skutočného stavu.
- Trvajte na tom, aby bola na systém vydaná revízná správa, potvrdená revíznym technikom.
- Trvajte na tom, aby boli na jednotlivých segmentoch vykonané certifikačné merania tej kategórie, do akej dodávateľ systém zaradil. Ak ho zaradil do kategórie 5, resp. triedy D, musí vykonať certifikáciu príslušným

prístrojom. Ak vám dodávateľ ponúkol systém vyššej triedy/kategórie, jeho vlastnosti mal by potvrdiť prístrojom príslušnej triedy.

7. Trvajte na tom, aby sa dodržiavala zásada, že v jednom porte sú ukončené všetky štyri páry. Existujú systémy (napr. AMP ACO), ktoré umožňujú, aby bol jeden kábel využitý súčasne dvoma počítačmi, prípadne telefónom a počítačom. Môže sa vám zdať, že ide o úsporu, ale kabeľáž by vám mala slúžiť dlhšie ako 2-3 roky, a keďže neviete, aké technológie sa budú používať v budúcnosti, neriskujte. Už dnes existujú technológie, ktoré potrebujú na prenos všetky štyri páry. Neznamená to, že systémy, ktoré takúto možnosť ponúkajú, sú zlé. Naopak, v prípade, že súrne potrebujete pridať zásuvku, stačí si na oba konce kábla dokúpiť duálny modul.

8. Dajte si tú námahu a skontrolujte, v akom stave vám bol systém odovzdaný. Ide najmä o stavebné práce, prípadne trasovacie práce. Skontrolujte si, či steny boli dané do pôvodného stavu, či sú lišty uzatvorené a neatvárajú sa, či dodávateľ zrealizoval dielo, tak ako bolo v zmluve uvedené...

a) Huby - zdieľaných 10 Mbit/s

Technológia zdieľaných 10 Mbitov je vhodná pre malé a nenárodné siete, pretože si všetky pripojené stanice delia spomínaných 10 Mbit/s medzi seba takmer rovnomerne. Z toho vyplýva, že na jednu stanicu z 10 pripadá prenosové pásmo 1 Mbit/s, čo nie je veľa. Za také môžeme považovať povedzme siete s 10-15 stanicami, ktoré na 90 % pracujú s bežnými kancelárskymi aplikáciami typu MS Office.

Príklad zariadení: 3Com OfficeConnect, 3Com SuperStack II HUB PS 40, Cabletron SEHi-24, Nortel Networks BayStack 102

Cenová hladina: od 2000,- Sk bez DPH za neznačkový nemanžovatelný 8-portový hub, po viac ako 70 000,- Sk bez DPH za značkový manažovatelný 24 portový HUB.

b) Huby - zdieľaných 100 Mbit/s

Nenechajte sa oklamať číslami. Aj keď $100/10 = 10$ a teda by táto technológia mala byť 10-krát výkonnejšia ako predchádzajúca, nie je to tak. V skutočnosti je to nárast iba asi o 30 % až 40 %, lebo veľkú rolu zohráva množstvo kolízií na sieti. Ak je toto množstvo veľké, čo pri väčšom množstve stanic nie je nič zvláštne, výkon dramaticky klesá a v priemere sa nárast výkonu zdieľaných 100 Mbit/s oproti zdieľaným 10 Mbit/s pohybuje iba na spomínaných 30-40 percentách. Príkladom sietí, v ktorých sa dá používať táto technológia, sú malé siete, kde sa okrem bežných kancelárskych aplikácií používajú aj trošku náročnejšie aplikácie typu rôznych ekonomických balíkov založených na systémoch FoxPro alebo Clipper.

Príklad zariadení: 3Com OfficeConnect DualSpeed HUB, Cisco FastHub, Cabletron SEHi100-24

Cenová hladina: od 10 000,- Sk bez DPH za 8-portový autosensing hub po viac ako 70 000 za značkový 24-portový manažovatelný stohovatelný hub.

Kedysi bolo veľmi populárne stohovanie hubov („HUB stacking“), ktoré umožňuje prepojiť pomocou špeciálnych káblov zbernice hubov. Takto prepojené huby sa potom správajú ako jedno zariadenie, čo má síce plusy najmä z pohľadu zjednodušenia manažmentu takýchto stohov, ale aj výrazné mínusy, lebo v skutočne veľkých stohoch, napr. 3-4 hubov, sa o pásmo 10 Mbit/s delí 60-90 stanic!

Pri huboch stojí ešte za zmienku technológia prepínania portov (port switching). Ide o možnosť rozdelenia stanic pripojených na jedno zariadenie. Princíp spočíva v tom, že hub má namiesto jednej zbernice napríklad štyri. Je potom už iba na správcovi systému, ktorý port na ktorú zbernicu pripojí. Technológia prepínania portov má veľký význam najmä v spojení so stohovaním hubov.

c) Switche – prepínaných 10 Mbit/s

Prechodom od zdieľaného Ethernetu k prepínanému sa situácia výrazne mení. Prepínače dávajú možnosť viacerých súčasných prenosov v rámci jedného zariadenia. Ak má teda zariadenie N portov, môže v ňom prebiehať až N/2 súčasných prenosov. Často sa zdá, že tých prenosov môže byť viac t. j. až N-1, no je to iba zdanie, vznikajúce následkom zavedenia ďalšieho nového prvku, ktorý huby nemali: vyrovnávacej pamäte – bufera. Zjednodušene povedané, vyrovnávacia pamäť sa používa v prípade, keď majú byť dáta odoslané na port, ktorý práve využíva iný prenos. Takýmto odložením dát sa odľahčí vysielacia stanica a výsledný efekt je ten, že sa používateľovi zdá, že prenos je rýchly. Veľkosť takejto pamäte sa pohybuje od niekoľko 100 KB po niekoľko MB.

Áká výkonná je takáto sieť? Čo sa týka počtu používateľov, ten nie je obmedzený. Vyhradených 10Mbit/s bez akýchkoľvek problémov postačuje bežným aplikáciám. Jediným limitom takejto siete je, že pokiaľ privede prenosov smeruje na ten istý port, začína sa prenos brzdiť. Je preto vhodné, aby počet takýchto namáhaných portov bol v rozumnom pomere k celkovému počtu portov (ale čo je to „rozumný pomer“ ?),

9. Záručné otázky:

a) Aké sú záruky kabeľážneho systému, ktorý ponúka? Bežné záručné doby sa pohybujú od 10 do 25 rokov na celý systém.

b) Aké záruky dáva na ostatné časti systému (plastové žlaby, rúrky, rozvádzače ...)? Je dôležité aby aj tieto časti boli kvalitné a správne navrhnuté, pretože sa vám môže stať, že sa začnú veká plastových žlabov otvárať, čo je častá chyba najmä pri lacnejších systémoch hlavne talianskych, českých a, bohužiaľ, aj slovenských výrobcov, alebo sa začnú deformovať vonkajšom vedené rúrky (možno bol použitý UV nestabilný materiál alebo rúrka nebola určená na vonkajšie použitie). Z kvalitnejších systémov by sme si dovolili spomenúť najmä Dietzel-Univolt Tehalit, alebo Obo-Betterman.

c) Záruka na práce

Bežná záručná doba na práce (napr. stavebné) je jeden rok.

10. Vyriešte v zmluve otázku straty záruky, lebo sa môže stať, že v prípade realizácie doplnení/rozšírení systému iným dodávateľom (keďže pôvodný dodávateľ zanikol, nie je schopný splniť požiadavky alebo s ním už nechcete mať nič) stratíte záruku.

4. časť – Aktívne prvky

Keď máme pripravenú kabeľáž, môžeme pristúpiť k oživovaniu siete. Otázky, ktoré sa budú odteraz preberať, nie sú závislé od kabeľáže. To je aj dôvodom, prečo je dobrá kabeľáž dobrou investíciou: je univerzálna.

Prvým krokom bude zapájanie aktívnych zariadení, čo je celkom jednoduchá procedúra za predpokladu, že zapájame rozbočovače (huby) alebo prepínače (switche). Dilemou pri malých sieťach býva aj rozhodovanie o type použitého zariadenia. Keby sme mali zoradiť bežne používané zariadenia podľa vhodnosti ich aplikácie, mohla by vyzeráť asi takto:

čo napríklad znamená, že pri veľkom počte používateľov je vhodné mať viac serverov...

Porty, na ktoré sa pripájajú servery alebo slúžia na pripojenie do chrbticovej siete, sa nazývajú uplinky. Sú zväčša niekoľkonásobne rýchlejšie ako zvyšné porty. Napríklad ak sú bežné porty 10 Mbit/s, uplinky môžu byť 100 Mbit/s alebo 1000 Mbit/s.

Príklad zariadení: Nortel Networks BayStack 310 Switch, Cabletron SmartStack 10, Cisco Catalyst 1900, 3Com SuperStack II Switch 1100

Cenová hladina: od cca 20 000,- Sk po 100 000,- Sk

d) Switche – prepínaných 100 Mbit/s

Ide v podstate o obmenu prepínaných 10 Mbit/s, ale iba s vyššou prenosovou rýchlosťou... Takéto prepínače sú vhodné ako centrálné prepínače, na ktoré sú pripojené servery, výkonné pracovné stanice a iné podradené prepínače.

Príklad zariadení: Nortel Networks Bay Stack 70 Switch, Cabletron SmartStack 100, Cisco Catalyst 2900, 3Com SuperStack II Switch 3300

Cenová hladina: od 25 000,- Sk za značkový nemanažovateľný prepínač po 100 000,- Sk za značkový manažovateľný prepínač

Za zmienku pri prepínačoch stojí ešte päť vecí: autodetekcia, polovičný a úplný, združovanie portov, rozdiel medzi desktop a workgroup prepínačom a prepínanie na tretej vrstve.

1. Autodetekcia

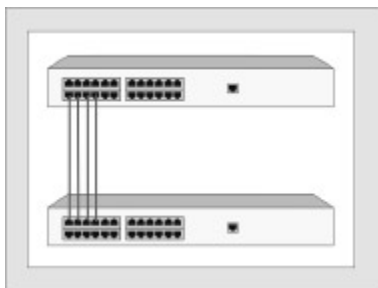
Autodetekcia (alebo aj Autosensing), je vlastnosť, vďaka ktorej sú zariadenia schopné dohodnúť sa na prenosovej rýchlosti, použitom duplexe a pod. Táto vlastnosť je zabudovaná už takmer do každého 100 Mbit/s prepínača. Jej výhodou je, že ak používate staršie sieťové karty, ktoré sú schopné komunikovať iba rýchlosťou 10 Mbit/s, a pripájate ich na 100 Mbit/s prepínač, nemusíte konfigurovať ani jedno zariadenie. Pokiaľ je port prepínača nakonfigurovaný na autodetekciu, s kartou sa dohodne sám... Pozor: táto vlastnosť nefunguje na optických portoch! Keď je teda optický port 100 Mbit/s, tak naň nepripojíte zariadenie komunikujúce iba rýchlosťou 10 Mbit/s.

2. Úplný a polovičný

Pod pojmom duplex sa skrýva označenie smeru prenosu: duplex = obojsmerný prenos. Slovičkami polovičný a úplný sa označuje typ obojsmerného prenosu. V prípade polovičného duplexu je síce možné prenášať dáta oboma smermi, ale v jednom okamihu iba jedným smerom. Vhodným príkladom je komunikácia vysielaciami. Pri zapnutom úplnom duplexe sa dáta prenášajú oboma smermi súčasne. Skutočné množstvo prenesených dát za tú istú jednotku času je potom dvojnásobné. Preto sa aj často stretnete s tým, že ten-ktorý prepínač je schopný prenášať dáta rýchlosťou až 200 Mbit/s – vtedy sa to myslí pri zapnutom úplnom duplexe.

3. Združovanie portov

Táto technológia je označovaná ako port trunking a umožňuje združiť viac fyzických portov do jedného logického prenosového kanála. Týmto je možné získať



pri prepínaní prepínačov kanály so šírkou niekoľko 100 Mbit/s. Pre malé siete je táto vlastnosť v podstate zbytočná.

4. Rozdiel medzi desktop a workgroup prepínačom

Často sa stretnete s pojmami desktop prepínač a workgroup prepínač. Možno sa vám toto rozdelenie bude na prvý pohľad zdať nelogické, veď každý prepínač môžeme použiť aj na pripojenie používateľov (desktop) aj na prepínanie viacerých prepínačov (workgroup). V našich podmienkach máte pravdu. Ak by ste však mali siete s niekoľko sto až niekoľko tisíc stanic, ani tieto pojmy by dostali iný rozmer. Základným rozdielom sú parametre, najmä pamätové: napr. kým desktop prepínač si dokáže uchovať iba niekoľko 100 MAC adries, skupinový prepínač až niekoľko tisíc. Rovnako veľkosť vyrovnávacej pamäte je pri skupinových prepínačoch väčšia.

5. Prepínanie na tretej vrstve

Stáva sa už módou, že každý rozpráva o prepínaní na tretej vrstve (bližšie som o tom písal v predošlom PC REVUE ;-). Váš však budú skôr zaujímať výhody tejto technológie. Najväčšou z nich je implementácia QoS (Quality of Services) do prepínačov, ktorá dá sieťovému administrátorovi do rúk nástroje na dokonalé spravovanie tokov v sieti. Vďaka tejto vlastnosti je napríklad možné uprednostniť dáta z ekonomického softvéru pred dátami z internetu... Treba však dodať, že náročnosť na implementáciu úplného QoS je značná a pre malé siete takmer zbytočná.

Redundantné zdroje napájania

Pretože jedinou časťou, ktorá sa na aktívnych prvkoch môže sama pokaziť, je zdroj napájania, pri kritických aplikáciách je nevyhnutné toto riziko minimalizovať, a to použitím zariadenia s redundantnými zdrojmi napájania. Redundantný zdroj napájania by sme mohli chápať ako záložný zdroj napájania, ktorý začne pracovať vtedy, keď sa primárny zdroj pokaziť. Nemýľte si ho však s UPS.

SNMP manažment

Na záver teórie o aktívnych prvkoch ešte spomenieme manažment aktívnych prvkov. Ten je dnes už neoddeliteľnou súčasťou palety nástrojov, ktoré používa administrátor počítačovej siete. Podpora pre SNMP manažment, zabudovaná do zariadenia, dáva administrátorovi možnosť ovládať každé takéto zariadenie v sieti z jedného bodu bez toho, aby musel byť vo fyzickej blízkosti zariadenia. Na manažovanie sa používajú špeciálne aplikácie, ako sú Optivity od Nortel Networks, SPECTRUM od Cabletron Systems a OpenView od Hewlett-Packard...

Pre malé siete je však využitie takéhoto manažmentu diskutabilné a pravdepodobne aj neúnosne drahé, lebo ceny takýchto systémov sa pohybujú v stotisícoch až miliónoch korún. Keby ste sa predsa rozhodli pre nákup nejakého manažmentu siete do menšej siete, pouvažujte nad nasledujúcimi produktmi: SPEL od Cabletron Systems, Transcend for Windows od 3Com alebo nad CiscoWorks for Windows od Cisco Systems...

Zapájanie

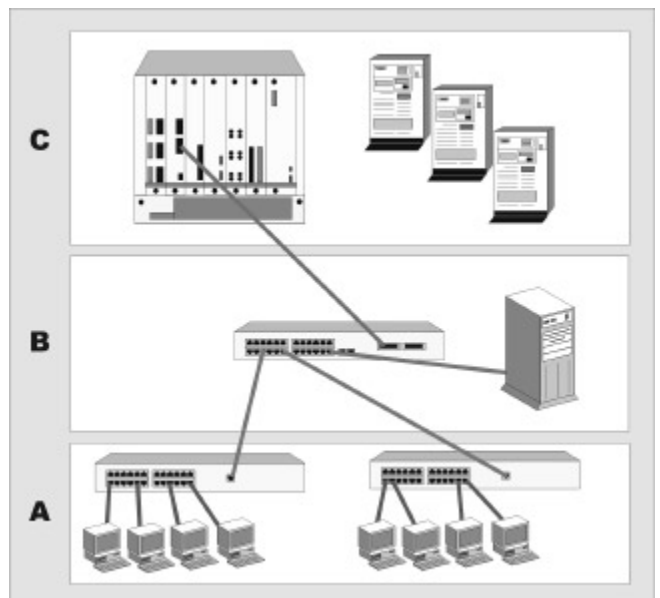
Ako sme spomínali hneď na začiatku tohto článku, zapájanie aktívnych prvkov nie je žiadna veda. Jeden

koniec kábla zasuniete do portu v aktívnom zariadení a druhý koniec do portu na prepíjovacom paneli. A to je všetko. Ak potrebujete prepojiť hub-prepínač, hub-hub, alebo prepínač-prepínač, budete musieť použiť prekrižený kábel. O tom, ako takýto kábel vyzerá, sme hovorili v predošlom čísle PC REVUE.

Prvou kontrolou, či je prvok zapojený správne, je stav LED diódy, ktorá je na drvejšej väčšine prvkov označená ako „LINK“. Za predpokladu, že stanica/počítač je zapnutá a nakonfigurovaná správne a aktívny prvok je tiež zapnutý, táto dióda by sa mala rozsvietiť. Ak sa vám nerozsvieti, skontrolujte, či ste všetko zapojili korektne, prípadne skúste vymeniť kábel alebo použiť iný port na zariadení. Rovnako môže byť tento problém spôsobený nastavením rôznej fixnej rýchlosti na prepíjaných zariadeniach alebo v prípade počítača aj tým, že je nastavený ako komunikačný port BNC, a nie TP...

Ak sa vám dióda ani potom nerozsvieti, skontrolujte alebo si dajte skontrolovať kabeláž. Ak je v poriadku, skúste, ak môžete, vymeniť zariadenie. Ak ani to nepomohlo, volajte technickú podporu....

Modelová situácia:



K obrázku:

A. je úroveň desktop prepínačov, na ktoré sú pripojené priamo pracovné stanice. Na tejto úrovni môžeme použiť ako prenosovú technológiu prepínaný Ethernet 10 Mbit/s alebo 100 Mbit/s. Okrem prepínačov je tu možné použiť aj huby.

B. je úroveň workgroup prepínačov. Prepínače na tejto úrovni zvládajú viac MAC adries, sú modularejšie a, samozrejme, aj drahšie. Zabezpečujú pripojenie na chrbticovú sieť a po nej vlastne pripojenie do hlavného prepínača. Táto úroveň je rovnako vhodná aj na pripojenie serverov lokálneho významu. Čo sa technológií týka, používa sa tu predovšetkým prepínaný 100 Mbit/s Ethernet, prípadne iné technológie podobného výkonu.

C. je defacto najvyššia úroveň. Nachádzajú sa na nej tzv. enterprise prepínače, ktoré zabezpečujú komunikáciu v rámci celej siete. Je vhodné na túto úroveň umiestniť „farmu serverov“, čo je vlastne skupina výkonných serverov poskytujúcich najdôležitejšie informácie. Pripojenie týchto serverov býva zvyčajne realizované FDDI alebo prepínaným Ethernetom 100 Mbit/s. Pripojenie enterprise prepínačov s workgroup prepínačmi často zabezpečuje napríklad skupina 100 Mbit/s portov, kde celková

šírka takto vytvoreného kanála môže byť niekoľko 100 Mbit/s. Pretože sa však prednedávnom prijal štandard pre gigabitový Ethernet, teda 1000 Mbit/s, je možné takéto prepojenia realizovať aj touto technológiou.

Otázky na dodávateľa

1. Dĺžka poskytovanej záruky
2. Rýchlosť záručného servisu
3. Čo urobí v prípade, že v rámci záruky bude treba zariadenie vymeniť: poskytnete dočasne iné zariadenie, aby práca mohla pokračovať nerušená až dovtedy, keď sa vráti opravené zariadenie zo servisu?
4. Má vyškolených technikov na dodávané zariadenie?
5. Dokáže zabezpečiť spätné odkúpenie starých zariadení?
6. Sú ním navrhovaných zariadeniach použité aj proprietárne technológie, ktoré by nemuseli fungovať s pripojením na zariadenia iných výrobcov?
7. Sú ním dodávané zariadenia kompatibilné s rokom 2000?
8. Akým spôsobom je možné manažovať ním navrhnuté zariadenia? Podporujú tieto zariadenia SNMP manažment?

5. časť

Využitie pracovných staníc v sieti

Keďže ste sa už rozhodli sieť vybudovať, tak je asi zbytočné vysvetľovať vám jej výhody a nevýhody, ale napriek tomu sa ich pokúsime zhrnúť.

Výhodou väčšiny operačných systémov pracovných staníc dneška, t. j. MS Windows 95/98/NT a Unix/Linux, je, že dokážu pracovať v režime peer-to-peer. To znamená, že dokážu jednak využívať zdroje iných počítačov, t. j. pracujú v klientskom móde, a zároveň dokážu svoje zdroje poskytnúť iným počítačom, t. j. dokážu pracovať v serverovom móde. Oba spomínané režimy môžu byť aktívne súčasne.

Medzi základné služby, ktoré môžu stanice využiť/poskytnúť, patria:

1. využitie miesta na pevných diskoch iných počítačov – tým sa minimalizuje potreba neustále dokupovať pevné disky a umožňuje sa rozvoj spolupráce medzi jednotlivými používateľmi, pretože majú prístup k dátam toho druhého (samozrejme, iba ak to ten druhý povolí...);
2. využitie tlačiarň pripojených k iným počítačom – toto opätovne prináša úspory investícií, lebo je zbytočné, aby každý používateľ mal vlastnú tlačiareň;
3. využitie modemov a faxmodemov pripojených k iným počítačom – okrem zjednodušenia faxovania to prináša so sebou aj možnosť pripojenia celej siete do internetu.

Počet základných služieb je síce relatívne malý, ale ich využitie je obrovské. Vo väčších sieťach, kde je využitie takýchto služieb realizované vo väčšom rozsahu, treba nasadiť špecializované počítače – servery, ktoré svojím výkonom zvládnu väčšie nároky používateľov. Takéto servery dokážu okrem už spomenutých služieb poskytovať aj ďalšie, napr. spoločný databázový prístup, spoločné zálohovanie a pod.

Pripájanie pracovných staníc do siete

Pod pojmom pracovné stanice teraz chápeme akékoľvek počítače pripojené do siete, teda nie triedu počítačov. Ich príprava je relatívne nenáročná a vyžaduje iba jednoduchú konfiguráciu.

Krok č. 1 – zistenie, či je pracovná stanica vôbec schopná pripojiť sa do siete, t. j. či má sieťovú kartu

Pokiaľ sieťovú kartu „nevidíte“ v konfigurácii operačného systému, neznamená to, že ju určite nemáte. Stačí sa pozrieť na zadnú stranu počítača a pohľadať potrebný konektor: v prípade štruktúrovanej kabeláže

je to zásuvka RJ-45 a pre koaxiálnu kabeláž potrebujete konektor BNC.



Obr. 1 – Konektor RJ-45 a konektor BNC (pohľad spredu a zboku)

Ak tam nájdete takéto konektory – jeden alebo druhý –, váš počítač pravdepodobne sieťovú kartu má. Ak nájdete konektor podobný RJ-45, ale nie ste si istí, či je to konektor počítačovej siete, stačí spočítať počet kovových pinov vnútri konektora: ak ich je 6, je to konektor RJ-21 modemu, ak ich je 8, je to konektor RJ-45 a s najväčšou pravdepodobnosťou je to konektor počítačovej siete.

Krok č. 2 – nemáme sieťovú kartu

Tento krok je pre vás zaujímavý, iba ak sieťovú kartu nemáte, t. j. ak ste nenašli konektory spomínané v kroku 1.

Nebudeme z toho robiť vedu: na trhu sa vyskytuje veľmi veľa výrobcov sieťových kariet, no ak nechcete mať problémy, pridržajte sa osvedčených výrobcov:

Výrobok	Konektor	Zbernica	Rýchlosť
3Com			
3C509 – EtherLink III	koax, TP, AUI	ISA	10 Mbit/s
3C90X – EtherLink XL	koax, TP	PCI	10/100 Mbit/s
Intel			
EtherExpress	TP	PCI	10/100 Mbit/s
Rôzni výrobcovia			
NEZ2000 kompatibilná	koax, TP	ISA/PCI	10 Mbit/s

Ceny sa pohybujú od 800 do 2500 Sk za kus. Ak môžete, kúpte si radšej plug-and-play kartu. Môžete sa stretnúť s označeniami ako TP a Combo. TP znamená, že karta je vhodná výhradne na pripojenie do štruktúrovanej kabeláže pomocou konektora RJ-45. Combo zasa znamená, že karta je „kombinovaná“, t. j. vhodná do koaxiálnych aj štruktúrovanej kabeláží. Čo sa týka rýchlosti karty, koaxové karty sú schopné komunikovať rýchlosťou iba 10 Mbit/s a TP karty pre FastEthernet, t. j. 100 Mbit/s, zasa majú zabudovaný mechanizmus na detekciu prenosovej rýchlosti a dokážu sa prestaviť aj na rýchlosť 10 Mbit/s, takže nie je problém ich pripojiť aj k 10 Mbit/s hubom.

Inštaláciu karty v počítači radšej prenechajte niekomu, kto to už robil. Pokiaľ používate operačný systém MS Windows 95/98/NT, konfigurácia sieťovej karty je dokonale opísaná v návode a v rôznych pomocníkoch, takže sa v tomto bode zdržíme akéhokoľvek komentára. Možno iba poznámka na okraj: Keď máte malú sieť, teda do 20-30 počítačov, pokojne používajte ľubovoľný sieťový protokol, no vo väčších sieťach by ste radšej mali používať TCP/IP, lebo NetBEUI aj IPX/SPX generujú priveľa broadcastov, t. j. paketov určených všetkým staniciam na sieti, ktoré zbytočne zatažujú jednotlivé stanice.

Krok č. 3 – pripájame počítač do siete

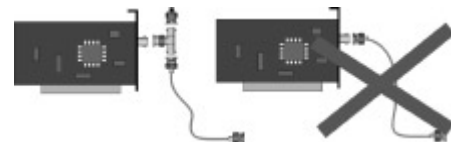
K tomuto kroku pristúpte, ak máte v počítači už nainštalovanú sieťovú kartu a operačný systém s ňou už dokáže komunikovať. Už v tomto bode uvidíte hlavné výhody štruktúrovanej kabeláže.

Pripájanie počítača do koaxiálnej kabeláže

1. Pomocou T konektora pripojte počítač do kabeláže (nikdy sa nesnažte pripájať počítač priamo, na 90 % vám to nebude fungovať a navyše budete spôsobovať problémy ostatným počítačom v sieti...). Pozor na rôzne

bezpečnostné systémy, ako sú TWC a EAD. Pri týchto systémoch sa používajú špeciálne pripojovacie káble, ktoré majú už T konektor zabudovaný.

2. Skúste počítač reštartovať, a ak je všetko v poriadku, mali by ste sa bez problémov prihlásiť do siete. Niektoré karty pre koaxiálnu kabelážu majú pri BNC konektore LED diódu ACT, ktorá bliká, ak je na sieti zistený prenos dát (pozri obr. 3). Ak sieť po reštarte nevidíte, máte problém. Ak sieť nevidíte, ale LED dióda občas blikne, bude pravdepodobne problém v konfigurácii sieťovej karty alebo sieťového softvéru. Skúste postupne skontrolovať



Obr. 2 – Správne a nesprávne zapojenie do koaxiálnej kabeláže

konfiguráciu, vymeniť pripojovací kábel, sieťovú kartu, počítač. Ak stále nič nevidíte, požiadajte o pomoc skúsenejších.



Obr. 3 – Pohľad na LED diódu umiestnenú na sieťovej karte, detegujúcu aktivitu koaxiálnej siete

Pripájanie počítača do štruktúrovanej kabeláže

1. Skontrolujte, či máte zapnutý počítača aktívny prvok, na ktorý chcete počítač pripojiť.

2. Pomocou pripojovacieho kábla pripojte počítač k zásuvke štruktúrovanej kabeláže. Po tomto kroku by sa vám mala rozsvietiť na sieťovej karte v počítači zelená (inej farby som zatiaľ nevidel) LED dióda s textom LINK alebo LNK. Takisto na aktívnom zariadení by sa mala rozsvietiť LED dióda LINK/LNK zodpovedajúca zásuvke, na ktorú ste pripojili počítač. Ak sa diódy rozsvietili, malo by byť všetko v poriadku a po reštarte (systémy Windows to jednoducho potrebujú...) by ste sa mali prihlásiť do siete a druhá LED dióda na sieťovej karte, označená ako ACT/ACTIVITY, by mala z času na čas bliknúť.

3. Ak sa jedna alebo druhá LINK LED dióda nerozsvietili,



Obr. 4 – Pohľad na LED diódy umiestnené na sieťovej karte. Zelená dióda LNK svieti v prípade, ak je počítač pripojený na aktívny prvok a obe zariadenia sú v prevádzke. Dióda ACT bliká, ak je na sieti detegovaná nejaká aktivita (počítač vysiela alebo prijíma dáta). Dióda 100 svieti, ak je prepojenie počítača - aktívny prvok realizované rýchlosťou 100 Mbit/s.

je problém. Skúste vymeniť pripojovacie káble, sieťovú kartu, pripojiť sa priamo na aktívne zariadenie, prípadne do iného portu aktívneho zariadenia, jednoducho musíte skontrolovať celú prenosovú trasu (pozri obr. 5). V každom prípade by ste sa mali snažiť dosiahnuť stav, aby LED diódy LNK svietili. Ak svietia a nevíete sa pripojiť do siete, skontrolujte konfiguráciu operačného systému (nastavenie protokolov, čísel sieti atď.), prípadne sa skúste pozrieť aj do príručky dodávanej k operačnému systému. Ak všetky pokusy zlyhajú, zavolajte niekoho skúsenejšieho.

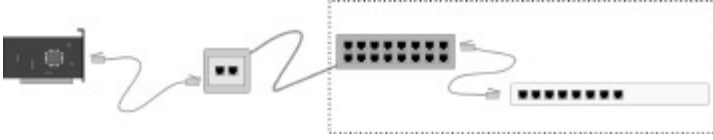
Testovanie pripojenia počítačov do siete

Keďže v predošlom čísle môj kolega opisoval celú problematiku testovania kabeláží, tejto problematike sa

budeme teraz venovať iba v skratke.

Niečo sme už naznačili v predchádzajúcich odsekoch. Odstraňovanie takýchto problémov vyžaduje skôr skúsenosti ako vedomosti, a preto sa dosť ťažko opisuje. Základný postup je však jasný:

1. Ako prvý vždy podozrievajte kábel. Skúste namiesto pripájaného počítača pripojiť iný. Ak to pôjde, problém je v počítači, ak nie, tak je problém v pripojení.
2. Ak je problém v pripojení, vymeňte vymeniteľné káble



Obr. 5 Časti štruktúrovanej kabeľáže, ktoré musíte skontrolovať v prípade problémov (môže ich byť viac, ako je na obrázku, ale to závisí od veľkosti siete). Zľava: sieťová karta v počítači, pripojovací kábel, zásuvka štruktúrovanej kabeľáže, horizontálna kabeľáž, prepojovací panel, pripojovací kábel, aktívne zariadenie siete.

(káble v stenách sa vymieňajú ťažko) za odskúšané. V prípade, že problém pretrváva, asi budete nútení otestovať káble v stenách. Na testovanie káblov existuje viacero testovacích prístrojov, napr. NETcat od spoločnosti Datacom-Textron (www.ies.sk/datacom), pomocou ktorého ste schopní otestovať koaxiálne aj štruktúrované kabeľáže.

Pri testovaní pripojenia treba skontrolovať aj aktívne zariadenie. Najjednoduchšie to urobíte tak, že pripájaný počítač pripojíte k takému portu na aktívnom zariadení, na ktorom predtým bez problémov pracoval iný počítač. Tu by ste mali dospieť ku konečnému riešeniu.

3. Ak bol problém v počítači, najprv skontrolujte konfiguráciu karty, protokolov a pod. Keď je toto všetko v poriadku, skontrolujte to ešte raz a potom vymeňte sieťovú kartu. Ak sa počítač aj po výmene správa rovnako, obviňte operačný systém. Hľadanie chyby v konfigurácii sieťovej karty alebo operačného systému je zložitý postup, pri ktorom vám musí byť úplne jasné, čo hľadáte. Ak vám to jasné nie je, porozmýšľajte o nejakom známom, ktorému to jasné bude, alebo zavolajte dodávateľa.

6. časť - Servery I.

Keď sa spýtam niekoho, čo si predstavuje pod pojmom počítačová sieť, často dostávam odpoveď, že sú to počítače, ktoré sú napojené na server. Vtedy ma vždy napadne ako silne asi pôsobí slovo server. No a preto, že sa tento seriál zaoberá návrhom malých počítačových sietí, teraz sa pokúsím trochu vysvetliť, o čo vlastne ide, a pokúsime sa spoločne vybrať „ideálny server“ pre vašu malú sieť.

Čo je to vlastne server? Hmm, asi neexistuje jednoznačná definícia. V podstate existujú dva pohľady na vec:

- „Server je počítač, ktorý poskytuje služby ostatným počítačom v sieti, najčastejšie súborové a tlačové služby.“ Toto je definícia s ktorou sa stretnete asi najčastejšie. Pri nej sa však môžete dostať do problémov, keď sa vás niekto spýta, kde máte súborový server a kde máte server pre tlač, a vy mu budete musieť ukázať ten istý počítač...

- „Server je proces/aplikácia, ktorá poskytuje svoje služby klientskym aplikáciám bežiacim na iných počítačoch, prípadne aj na tom istom počítači, na ktorom beží serverový proces.“ Toto je už lepšia definícia a v podstate vystihuje problematiku architektúry klient-server.

Aj tak budete musieť používať obe „definície“...

Podme však k reálnemu životu. Mali by sme sa venovať nasledujúcim otázkam:

1. Na čo je dobrý server?
2. Potrebujeme server?
3. Aká by asi mala byť konfigurácia servera?
5. Operačné systémy pre servery.

Na čo je dobrý server?

Je niekoľko hľadísk, z ktorých sa dá na server pozeráť. Niektoré z nich sú:

1. Bezpečnosť

Server zvyšuje bezpečnosť tým, že sústreďuje dáta na jednom mieste, ktoré môže byť jednoduchšie zabezpečené proti výpadkom systému, poškodeniu, zneužitiu dát, odcudzeniu a pod.

Zabezpečujú sa dve časti: fyzická a logická. Fyzické zabezpečenie, ktoré sa týka počítača v

role servera, sa dosahuje napríklad vyhradením špeciálnej miestnosti s ohňovzdornými dverami a s prístupom povoleným iba určeným ľuďom, pravidelným a úplným zálohovaním a pod. Pod logickým zabezpečením sa chápe zabezpečenie údajov uložených na serveri. Opäť existuje množstvo spôsobov, ktorými možno údaje zabezpečiť: vybudovaním systému prístupových práv k údajom, šifrovaním údajov, transakčným spracovaním a pod.

2. Výkon

Tým, že celé spracovanie údajov prenechávame serveru, vlastne odbremeňujeme klientske stanice, ktoré potom môžu poskytnúť svoj procesorový čas aplikáciám, čím sa vlastne výkon celého systému zvyší. Pokiaľ je systém klient-server správne navrhnutý, môžete zvyšovať jeho výkon zvyšovaním výkonu počítača, na ktorom je spustený serverový proces, takže stanice môžu zostať prakticky nedotknuté.

3. Správa dát a aplikácií

Centralizácia údajov na jednom mieste dáva predpoklady na ich jednoduchšiu správu. Toto zahŕňa napríklad inštalácie nových verzií, zálohovanie, sledovanie prístupu k údajom, zabezpečenie integrity údajov...

4. Znižovanie nákladov

Pre majiteľov a riaditeľov spoločností je, samozrejme, toto hľadisko asi najzaujímavejšie. Množstvo investícií vložených do systému založeného na modeli klient-server je vždy menšie ako v systéme bez servera. Toto však začína platiť až pri určitej veľkosti systému. Dôkazom šetrenia by mohli byť už fakty spomínané v predchádzajúcich odsekoch, t. j. zabezpečiť treba iba jeden uzol siete, pri potrebe zvýšenia výkonu, bezpečnosti, spoľahlivosti stačí investovať iba do jedného počítača. Rovnako prevádzkové náklady na spravovanie a údržbu takéhoto systému sú menšie.

Potrebujeme server?

Otázka je správna. Nie vždy je rozumné investovať do servera. Toto platí najmä pre malé organizácie, kde existujúce operačné systémy pracovných staníc (Windows 95/98/NT, Linux) postačujú na všetky činnosti, ktoré organizácia potrebuje. Medzi takéto činnosti patrí zdieľanie súborov a tlačiarň, prístup na internet a e-mail, faxovanie po sieti a pod. Stačí iba použiť správnu aplikáciu...

Pár tipov, kedy nepotrebujete server:

- keď občas potrebujete poskytnúť údaje uložené na jednom počítači,
- keď občas potrebujete poskytnúť svoju tlačiareň kolegovi,
- keď chcete prijímať e-mail a používať internet na jednom počítači (samozrejme, existujú aplikácie, ako

je napr. WinProxy, ktoré umožnia pripojiť na internet celú sieť, ale nie je vhodné používať ich, ak je sieť, alebo pripojenie na internet je časté, pretože zbytočne zaťažujú daný počítač),

- keď chcete, aby vaši 3-4 kolegovia mali možnosť faxovať pomocou vášho faxmodemu.

No a kedy je rozumné zaobstaráť si server:

- keď potrebujete poskytnúť údaje uložené na jednom počítači viacerým používateľom, a to sústavne a intenzívne,
- keď potrebujete zabezpečiť, aby sa k vašim údajom dostali iba oprávnení používatelia,
- keď chcete alebo potrebujete kontrolovať prístup a využívanie zdrojov, ako sú tlačiarne, e-mail, internet, faxmodemy a pod.,
- keď využívate aplikácie náročné na výkon alebo na rýchlosť prístupu k údajom na viacerých počítačoch v sieti (napr. rôzne informačné systémy, či už ekonomické, alebo grafické a pod.).

Operačné systémy pre servery?

Na svete už zostali prakticky len tri sieťové operačné systémy, ktoré sú vhodné aj na nasadenie do prostredia malých sietí: Windows NT, Novell NetWare a Linux.

Windows NT

Windows NT je pravdepodobne najrozšírenejším z nich. K jeho veľkej obľube prispela najmä jeho obrovská vonkajšia podobnosť s operačným systémom pracovných staníc Windows 95/98, a teda jednoduchá inštalácia a konfigurácia.

História Windows NT

Prvým pokusom Microsoftu o vytvorenie sieťového operačného systému bol produkt nazývaný MS-NET. Pretože Microsoft nebol v tom čase dostatočne veľký na to, aby produkt predával sám, nechal, aby ho predávali iní. Takto sa MS-NET predával v rámci IBM. Keďže výkon MS-NET-u bol veľmi malý, začali vznikať konkurenčné produkty, ako napr. NetWare od firmy Novell. V tom čase chcela spoločnosť 3Com predávať produkt, ktorý by bol orientovaný smerom k produktom IBM, a preto zakúpila licenciu na MS-NET a začala ho predávať pod názvom 3+ Open. Pretože spolupráca Microsoft - 3Com bola výhodná, spolupracovali aj na vývoji novej generácie sieťového operačného softvéru, nazvaného LAN Manager. Ten už nebol postavený na operačnom systéme MS DOS, ale na OS/2, ktorý Microsoft vyvíjal v spolupráci s IBM. V tom čase, Intel začal s rapidným vývojom procesorov, a tak sa Microsoft rozhodol, že ich nasledujúci produkt bude nezávislý od platformy, t. j. bude schopný pracovať na akomkoľvek procesore. Týmto si chcel Microsoft zabezpečiť pozíciu, v ktorej bol vtedy Unix.

V roku 1988 Microsoft zamestnal Davida Cutlera, ktorý predtým pracoval vo firme Digital Equipment Corporation (dnes časť firmy Compaq) na vývoji operačného systému VMS a je známy ako „otec Windows NT“. Ich nový produkt mal niesť meno LanManager NT (NT = New Technology). Tento produkt sa nikdy nepredával, no dodnes sa tento názov v systéme Windows NT používa (lanman.drv = sieťový ovládač pre Windows NT a pod.). LanManager NT sa začal predávať pod názvom Windows NT Advanced Server a marketingovo sa spájal s vtedy nastupujúcimi Windows 3.1. Microsoft mu bez výčitiek dal číslo verzie 3.1. Na rozdiel od Windows 3.1 bol Windows NT od svojho začiatku navrhovaný ako 32-bitový operačný systém. Potom prišli verzie 3.5 a 3.51, ktoré posunuli Windows NT o kúsok dopredu v konektivitě a výkone, no až verzia 4.0, uvoľnená v roku 1996, priniesla preň obrovský úspech.

Novell NetWare

Bol a je (zatiaľ?) najvýkonnejším sieťovým operačným systémom na trhu. Od nástupu Windows NT 4.0 však

začala jeho sláva upadať, čo vidieť najmä na zmenšujúcom sa podiele na trhu.

História Novell NetWare

Na rozdiel od Microsoftu je Novell výslovne orientovaný na sieťové operačné systémy a produkty určené pre počítačové siete. Toto bola jeho najväčšia výhoda aj v začiatkoch. Hlavnou ideou firmy Novell je vytvorenie homogénneho systému, ktorý by bolo možné využiť na prepojenie heterogénneho hardvéru.

Sieťový operačný systém NetWare vznikol v roku 1983 pod názvom NetWare 86 a bol určený pre procesory Intel 8086. Jeho základom bol sieťový protokol IPX, zdieľanie tlačiarň a súborov. V porovnaní s MS-NET-om bol niekoľkonásobne rýchlejší a spoľahlivejší. Chyby, ktorých sa dopúšťal Microsoft vo svojom MS-NET-e, umožnili Novellu prakticky ovládnuť trh sieťových operačných systémov na dlhý čas. Takto postupne prišli na svet produkty ako Advanced NetWare, ktorý už obsahoval prístupové práva, NetWare 2.x, NetWare 3.x s vyspelým systémom SFT II (System Failure Tolerance), ktorý umožnil budovanie záložných serverov a dokázal pracovať s TCP/IP a SNA. Systém NetWare 4.x priniesol na svetlo sveta dodnes najvyspelejší systém na spravovanie zdrojov siete, používateľov a vlastne celých komplexov serverov pod názvom NDS (Novell Directory Services).

Istým pokusom o presadenie sa v internete a intranete bolo, keď sa firma Novell pokúsila predávať NetWare 4.11 pod menom IntranetWare. Tento systém už obsahoval také softvérové balíky ako HTTP server, DNS, DHCP, IPX/IP Gateway, FTP, NFS, nástroje na pripojenie unixových staníc a pod. Tento krok sa však nestrelol s pochopením u verejnosti a vo verzii 5.0 sa Novell vrátil k názvu NetWare.

Linux

Linux je dnes zaujímavou alternatívou ku komerčným produktom typu Windows NT a Novell NetWare. Jeho najväčšou výhodou je jeho cena: je totiž zadarmo... Vo svete sa stretáva s čoraz väčšou podporou tak u používateľov, tak aj u výrobcov. Podporu Linuxu už ohlásili aj také kolosy, ako sú Oracle, Informix, Corel a pod.

História Linuxu

História Linuxu sa odvíja od Unixu, takže by si ho asi nezaškodilo trochu pripomenúť. Unix bol vyvinutý po roku 1970 pre minipočítače a mainframy. Bol to najrozšírenejší operačný systém predchádzajúcich rokov. Za zmienku tiež stojí, že to bol a zatiaľ aj je jediný skutočný viacpoužívateľský a viacúlohový systém. Dôvodom, prečo jeho sláva upadá, je, že neexistuje takmer nijaká štandardizácia medzi druhmi Unixu (je ich niekoľko stoviek!), čo rozdeľuje sily vývojárov.

Ale vráťme sa k Linuxu. Linux vyvinul Linus Torvalds počas svojho štúdia na helsinskej univerzite vo Finsku. Systém bol ovplyvnený najmä systémom Minix, ktorý vyvinul Andrew Tanenbaum. Takisto aj prvé debaty o tomto systéme sa viedli v USENET-e v comp.os.minix. Celé úsilie Linuxa bolo najprv zamerané na dokonalé zvládnutie procesora Intel 386, a teda najmä na prepínanie úloh. Celý operačný systém bol najprv napísaný v asembleri. Prvá verzia Linuxu mala číslo 0.01 a obsahovala prakticky iba útržky jadra systému. Predpokladala, že používateľ má prístup k Minixu... Prvá oficiálna verzia bola 0.02, Linus ju uvoľnil na používanie 5. októbra 1991, obsahovala už bash (Bourne Again Shell), čo je alternatíva COMMAND.COM-u v systéme MS-DOS a kompilátor jazyka C.

Linux dnes vyvíja niekoľko tisíc programátorov po celom svete a nie je vlastníctvom žiadnej spoločnosti.

Takže zatiaľ toľko. S vlastnosťami jednotlivých systémov a ich porovnaním budeme pokračovať až v budúcom tisícročí (teda ak môj počítač prežije rok 2000; ja som si už sviečky a zásoby potravín kúpil ;)...

7. časť: Servery II.

Vlastnosti sieťových operačných systémov

Bezpečnosť

Pretože servery, resp. ich médiá neraz obsahujú citlivé informácie, ku ktorým by mali mať prístup iba oprávnené osoby, často diskutovanou otázkou pri operačných systémoch serverov býva ich bezpečnosť. Aj pri nich je možné použiť všeobecný koncept AAA (Authentication Authorization Accounting).

1. Authentication – autentifikácia – zistenie, o koho ide

Vždy, keď sa klient pripája na server, musí operačný systém servera zistiť, o koho ide. Najčastejší spôsob autentifikácie je už obligátny pár meno/heslo. Toto býva aj najčastejším miestom útokov na sieťové operačné systémy. Postupom času sa vyvinulo niekoľko techník, ktorými dokáže server bezpečne určiť klienta:

a) tzv. clear text password – ide o zastaraný spôsob autentifikácie, keď server požiada o heslo a klient mu heslo zašle v tzv. čistej podobe ako text. Keďže takúto komunikáciu medzi serverom a klientom je ľahké „odchytiť“, tento spôsob sa dnes veľmi zriedka používa a moderné sieťové operačné systémy ho vôbec nevyužívajú, prípadne sa používa iba pri tzv. jednorazových heslách;

b) šifrované heslá sa používali na „znemožnenie odchytenia“ prenášaného hesla. Tento spôsob sa takisto používa iba výnimočne. Častejšie sa začína používať vytvorenie šifrovaného kanála;

c) CHAP (Challenge Authentication Protocol) – je často používaný spôsob autentifikácie. Vychádza z predpokladu, že obe strany poznajú kľúč/heslo, to znamená, že server ho má uložené vo svojich systémových súboroch a klient/používateľ vo svojej hlave. Postup je potom približne takýto: server vygeneruje náhodný blok dát a zakóduje ho kľúčom, ktorý má priradený k menu autentifikovaného klienta. Tento blok pošle klientovi. Ten, keďže tiež pozná kľúč, blok rozkóduje a odošle ho späť serveru, ktorý porovná prijatý rozkódovaný blok s pôvodným vygenerovaným blokom, a ak sa zhodujú, server klienta autentifikuje;

(Poznámka: Čo sa týka kľúčov a šifrovania, opäť existujú dva princípy: symetrické a asymetrické šifrovanie. Pri symetrickom sa na dešifrovanie dát použije ten istý kľúč, ktorým boli informácie zašifrované. Pri asymetrickom šifrovaní sa najprv dáta zašifrujú tzv. verejným kľúčom prijímateľa, ktorý ich dešifruje svojím súkromným kľúčom.)

d) jednorazové heslá sú dnes čoraz populárnejšie. Používajú sa najmä pri systémoch obsahujúcich veľmi citlivé dáta. Príkladom systému jednorazových hesiel sú tzv. tokenové/prípustkové kalkulátory. Je to systém, ktorý má dve časti: serverovú aplikáciu a klientsky kalkulátor. Princíp je v podstate jednoduchý, ide o akúsi obmenu CHAP-u pre ľudí: klient po pripojení na server dostane kód, ktorý kalkulátor po zadaní prepočíta na prístupové heslo, po jeho zadaní server klienta autentifikuje.

2. Authorization – autorizácia – riadenie prístupu autentifikovaného klienta k zdrojom

Po autentifikácii je klient pripustený k zdrojom servera, no dobre vieme, že nie všetci klienti sú si rovní. Prichádzajú na rad tzv. používateľské práva, teda kto čo v systéme smie a nesmie. V podstate ide o to, či klient smie alebo nesmie využívať tie-ktoré zdroje, ako tlačiarne, súbory a pod. Existuje množstvo prístupových práv, napr. vytváranie, mazanie, modifikácia súborov, práva vytvárať a modifikovať používateľov, práva na zálohovanie systému atď.

3. Accounting – „účtovanie“ – monitorovanie činnosti klienta

Pre systém je takisto dôležité sledovať, kto čo a kedy urobil. Takéto sledovanie je možné nasadiť napríklad na vymazávanie súborov v kritických adresároch, možno ho využiť na znemožnenie prihlásenia sa napr. cez vikendy a pod. Existuje veľmi veľa možností využitia: napríklad na určenie využívania servera/serverov jednotlivými používateľmi a v prípade, že server poskytuje služby aj tretím subjektom, je ho možné v skutočnosti použiť na účtovanie poplatkov za jeho služby, napr. využitie diskového priestoru u vášho poskytovateľa internetu.

Spoločnosť

Tak ako musí byť sieťový operačný systém bezpečný, musí byť aj spoľahlivý. Spoľahlivosť je nevyhnutnou podmienkou v prípade, ak má byť systém nasadený v tzv. kritických aplikáciách. Pod takýmto aplikáciám sa myslí napr. vnútorný informačný systém podniku, meranie a regulácia procesov, bankové operácie a pod.

Systém musí byť spoľahlivý vnútorne, t. j. kritický stav jednej jeho časti nesmie ovplyvniť funkčnosť ostatných častí. Vonkajšia spoľahlivosť sa meria napríklad schopnosťou systému poskytovať svoje služby aj v kritických situáciách, napr. pri výpadku niektorých častí hardvéru. Medzi takéto citlivé časti patria predovšetkým médiá obsahujúce dáta používateľa, t. j. najmä pevné disky.

Vyvinulo sa niekoľko techník na zabezpečenie funkčnosti aj v prípade takýchto výpadkov. Niektoré z nich sú podporované priamo operačným systémom, iné sú nezávislé od operačného systému. Hoci by sme sa mali venovať čisto operačným systémom, spomenieme ich bez ohľadu na ich závislosť od nich.

1. Mirroring – zrkadlenie diskov alebo ich častí (partícií) – je prvou takouto technikou. Ide vlastne o replikáciu zapisovaných dát na sekundárne médium (zrkadlový obraz). V prípade výpadku primárneho média (disku) potom automaticky alebo poloautomaticky preberá jeho funkciu sekundárne médium. Mirroring využíva na zapisovanie na obe médiá ten istý kanál, čo v praxi znamená, že výkon systému je mierne nižší ako v prípade, že by mirroring nebol aktivovaný. Ďalšou slabinou mirroringu je už spomínaný prenosový kanál, resp. fakt, že je iba jeden. V prípade, že vypadne kanál (t. j. napr. radič disku), systém sa stáva nefunkčným.



Obr. 1 RAID 1 = Mirroring/duplexing je často používaná lacnejšia alternatíva k diskovým poliám

Existuje forma mirroringu, pri ktorej sa používa pre každé sekundárne médium, resp. zostavu médií samostatný kanál. Táto forma sa nazýva aj duplexing.

Mirroring sa môže zabezpečovať hardvérom a/alebo operačným systémom. Odporúčame použiť špeciálny hardvér.

2. RAID – (Redundant Array of Inexpensive Disks = redundantné pole nenáročných diskov) je dnes veľmi populárna technika, ako zabezpečiť výkon a/alebo bezpečnosť systému. Má niekoľko úrovní, z ktorých každá má svoje výhody a nevýhody. RAID môže byť vykonávaný špeciálnym hardvérom alebo ho môže zabezpečovať

operačný systém (pozri softRAID v Linuxe). Preferované riešenie je použitie špeciálny hardvér.

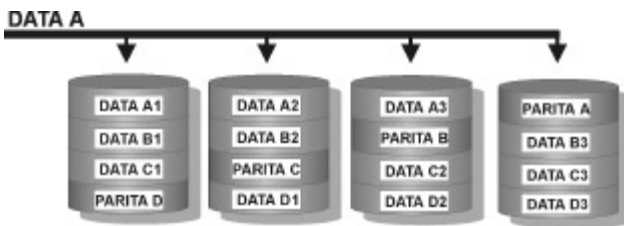
RAID 0 – sa používa v prípadoch, ak je potrebné zvýšiť výkon systému uchovávaného dáta. Pracuje tak, že sa zapisované dáta rozdelia na niekoľko blokov a každý blok je zapísaný pomocou samostatného kanála na samostatný disk. Podobne je to pri čítaní dát z diskov. Takýto paralelný prístup k dátam veľmi zvyšuje výkon systému. Jeho nevýhodou je, že v prípade výpadku jedného média v zostave sú stratené všetky dáta uložené v celej súprave médií, na ktorých bol RAID 0 zapnutý. V žiadnom prípade by sa RAID 0 nemal používať v prostrediach s kritickými aplikáciami. Je vhodný do DTP štúdií, na digitálne spracovanie videa a pod.

RAID 1 – ide o najjednoduchšiu formu zaistenia bezpečnosti dát. Je to už spomínaný mirroring/duplexing.

RAID 2 – tento typ používa rovnako ako RAID 0 viacero dátových diskov, na ktoré zapisuje jednotlivé bloky dát, no zavádza tzv. paritné disky. Paritná informácia je taká informácia, pomocou ktorej je možné rekonštruovať chýbajúcu časť pôvodnej informácie. Na paritné disky sa podobným systémom, ako je to pri dátových diskoch, zapisujú paritné dáta. V prípade výpadku niektorého z dátových diskov sa chýbajúca časť dát doplní z paritného bloku. Tento systém má veľmi vysoké počiatkové náklady, pretože ho možno realizovať iba na veľmi výkonných systémoch.

RAID 3 – je to v podstate modifikácia RAID 2. Rozdielom je však použitie iba jedného paritného disku, je teda lacnejší. Používa sa napríklad vo videoprodukcii a pod. Tento typ RAID-u sa veľmi ťažko implementuje ako čisté softvérové riešenie, lebo operácie použité pri ňom sú veľmi náročné na výkon a veľmi by obmedzovali výkon servera. Odporúčané je hardvérové riešenie.

RAID 4 – na rozdiel od RAID 3 tento typ RAID-u nedelí dáta na bloky, ale umožňuje robiť paralelné zápisy rôznych dát na rôzne dátové disky. Veľmi (ale naozaj veľmi) zjednodušený príklad: dáta A sú zapísané na disk 1, dáta B na disk 2, dáta C na disk 3, dáta D na disk 1, dáta E na disk 2 atď. Paritný blok sa generuje z naraz zapisovaných dát – v našom prípade z A, B a C. Zápis v tomto systéme je veľmi pomalý a spôsob rekonštrukcie dát v prípade výpadku disku nedostatočný, preto sa tento spôsob príliš nepoužíva.



Obr. 2 RAID 5 je najčastejšie používaným typom diskového poľa

RAID 5 – tento typ RAID-u je vďaka svojim vlastnostiam najuniverzálnejší a asi aj najpoužívanejší. Nepoužíva samostatný paritný disk, ale paritné informácie, ako aj dátové bloky sú rovnomerne rozprestreté po všetkých diskoch v RAID-e. Jeho výkon pri čítaní dát je veľmi vysoký. Rýchlosť zápisu je menšia. V prípade výpadku niektorého z diskov v poli sa výkon celého poľa zmenší. Na vybudovanie RAID 5 sú potrebné minimálne tri disky. Využitelný diskový priestor pre používateľské dáta je vždy iba $n-1/n$, kde n je počet diskov v poli, z celkovej kapacity poľa $1/n$ sa využíva na paritné informácie.

Existujú ešte ďalšie typy RAID-ov (6, 7, 10, 53), ale vzhľadom na ich zriedkavosť a veľmi vysokú finančnú náročnosť sa im nebudeme venovať.

3. SFT III – (System Fault Tolerance = odolnosť systému voči poruchám) je proprietárna technológia spoločnosti Novell (t. j. pracujúca iba na platformách Novell NetWare a vyvíjajú mimo štandardov). Bola to pravdepodobne prvá dostupná technológia na budovanie systémov odolných na poruchy.

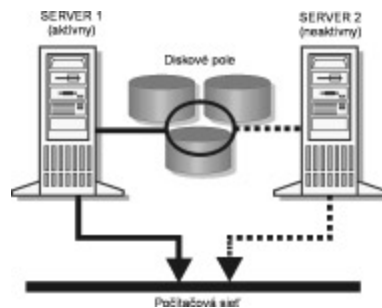
Veľmi zjednodušene povedané: kým RAID 1 zabezpečuje zrkadlenie dvoch diskov, SFT III zabezpečuje zrkadlenie dvoch serverov. Tieto servery môžu byť umiestnené v rôznych lokalitách, vzdialených od seba až 40 km a prepojených optickým káblom. SFT III zabezpečuje, aby obsahy pamäti a diskov oboch serverov boli rovnaké, a teda v prípade výpadku jedného servera druhý automaticky preberá všetky činnosti na seba. Výhoda tohto systému je, že používateľ nestratí ani bajt zo svojich dát a v podstate si ani nevšimne, že porucha nastala.

4. Clustering

Čo je to klastor (cluster)? Je to skupina zariadení (serverov), ktorá sa navonok správa ako jeden systém.

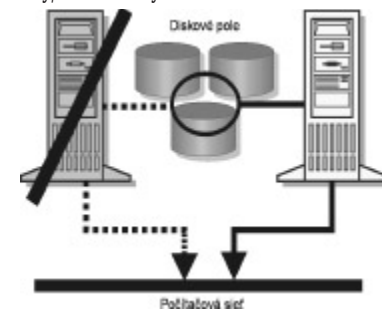
Zatiaľ čo SFT III je technológia proprietárna, pre clustering sa snažia niektorí výrobcovia vytvoriť priemyselný štandard. Clustering má dva základné ciele: poskytnúť systémom maximálnu možnú odolnosť voči poruchám (pozri SFT III) a byť nástrojom na zvyšovanie výkonov systémov.

Odolnosť voči poruchám sa dosahuje – podobne ako to bolo pri SFT III – presmerovaním požiadaviek klientov z nefunkčných serverov na funkčné. Zatiaľ čo v SFT III sa používali iba dva servery, primárny a stand-by, pri clusteringu je možné takto zabezpečiť viac serverov.



Obr. 3 Práca primárneho (aktívneho) a stand-by (neaktívneho/záložného) servera počas normálnej prevádzky

Druhým cieľom clusteringu je vytvoriť prostredie/systém, ktorého výkon by bolo možné zvyšovať pridaním ďalších jednotiek (serverov). Z tohto vyplýva, že v rámci klastra sa jednotlivé servery na rozdiel od SFT III delia o svoju záťaž, t. j. všetky sú aktívne. Takto v prípade, že výkon systému bude v budúcnosti nedostačujúci, bude mať používateľ možnosť výkon zvýšiť buď zvýšením výkonu existujúcich jednotiek/serverov, alebo pridaním ďalšej jednotky/servera do systému.



Obr. 4 Pri poruche/výpadku primárneho servera preberá jeho funkciu stand-by server

Poznámka: Dobrá rada znie: „Neverte nikomu a ničomu a zálohujte, zálohujte a zálohujte.“

Výkon

Dnes, keď sa vývoj vracia k serverovému spracovaniu dát a tenkým klientom, je výkon servera veľmi dôležitý. Veľkú rolu v určovaní výkonu servera zohráva aj jeho operačný systém. Príkladom môže byť porovnanie poskytovania súborových služieb, kde zatiaľ na takej istej konfigurácii počítača vedie Novell Netware. No vždy je potrebné pozeráť sa na konkrétne úlohy, pretože je asi nemožné zovšeobecniť poradie sieťových operačných systémov z pohľadu výkonnosti.

1. Multitasking – viacúlohovosť

V dnešných dobách asi už nemá zmysel vysvetľovať, čo je to multitasking, takže iba spomenieme, že ide o spracovanie viacerých úloh v jednom systéme súčasne. Bez multitaskingu by dnešné sieťové operačné systémy nemohli existovať, lebo väčšina ich služieb v podstate pracuje ako samostatná aplikácia. Príkladom môže byť poskytovanie súborov, tzv. súborový server, obsluha tlačiarň a databázový server na jednom počítači.



Obr. 5 Multitasking

Dôležité je však spomenúť, že existujú dva druhy multitaskingu, používané v dnešných sieťových operačných systémoch: preemptívny a nepreemptívny multitasking.

Preemptívny multitasking je založený na tom, že operačný systém prideliť aplikáciám krátke časové úseky, počas ktorých môžu využívať procesor. Aplikácie sa takto v rýchлом slede striedajú a vytvárajú dojem, že bežia naraz. Výhodou tohto typu je, že čas procesora je rozdelený takmer spravodlivo. Nevýhodou zasa môže byť, že tzv. prioritné aplikácie, napr. databázový server, dostanú toľko času ako akákoľvek iná aplikácia. Samozrejme, existujú spôsoby, ktorými sa dajú určiť priority jednotlivým aplikáciám a tak priradiť jednotlivým aplikáciám viac času. Príkladmi systémov s preemptívnym multitaskingom sú Windows NT a Linux.

Nepreemptívny multitasking je iný. V jednoduchosti povedané, operačný systém odovzdá riadenie aplikácii a tá, keď uzná za vhodné, odovzdá riadenie späť operačnému systému. Už z tejto krátkej informácie môžu vzniknúť pochybnosti o funkčnosti systému založeného na nepreemptívnom multitasking, veď čo ak aplikácia neodovzdá riadenie nikdy?! Samozrejme, takéto operačné systémy majú nástroje na to, aby sa zabránilo „kradnutiu“ času. Takto pracuje napríklad aj Novell Netware.

2. Multithreading – už nie je taký známy ako multitasking, ale v podstate to nie je nič nové. Thread (= vlákno) je samostatne vykonávateľná časť aplikácie. Znamená to, že aplikácia si môže na čiastkovú úlohu vytvoriť akoby podaplikáciu (vlákno), nechať ju na starosť operačnému systému a už iba pozbierať výsledky. Ako triviálny príklad by sme mohli uviesť zobrazovanie aktuálneho času počas behu aplikácie. Menej triviálnym príkladom by bolo prehladávanie dvoch rôznych databáz súčasne. Samozrejme, veľká časť problémov, ktoré sa riešia vytváraním vlákien, by sa dala vyriešiť aj klasickým prístupom, ale vlákna sú podstatne elegantnejšie...



Obr. 6 Multithreading

3. **Multiuser** – viacpoužívateľskosť pri dnešných sieťových operačných systémoch nie je až taká bežná, ako by sa mohlo zdať. Súčasné operačné systémy, umožňujúce spúšťať aj bežné aplikácie, ako je napr. Windows NT, vo svojom návrhu predpokladajú, že klientska strana aplikácie sa bude (asi vzhľadom na ceny bežných počítačov) vykonávať vždy na strane počítača klienta. No uvidíme, ako to bude v budúcnosti, pretože nastupuje asi doba tenkých klientov. Tento trend badať aj na Windows NT, kde sa začínajú objavovať nadstavby ako WinFrame alebo MetaFrame (viac informácií na www.datapac.sk), ktoré stavajú aj systém Windows NT do roly viacpoužívateľského systému. Výnimkou sú operačné systémy založené na architektúre Unixu, ktoré sú viacpoužívateľské už oddávna. Výhodou používania viacpoužívateľských systémov a tzv. tenkých klientov sú predovšetkým nižšie náklady na vybavenie klientských staníc a nižšie náklady aj na samotnú prevádzku systému.

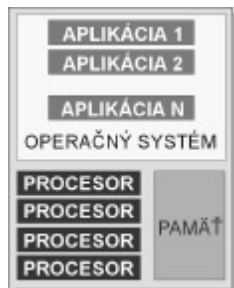


Obr. 7 Multiuser

4. **Multiprocessing** – pri viacpoužívateľských, viacúlohových aplikáciách automaticky prichádza na um otázka, či by nebolo rozumné zvýšiť výkon aplikácie zapojením viacerých procesorov. Tým sa dostávame k multiprocessingu. Spomenieme dva základné druhy: SMP a MPP.

SMP

Symetrický multiprocessing je spracovanie programov viacerými procesormi, ktoré zdieľajú operačný systém a pamäť. Pri SMP systéme počet procesorov málokedy presiahne 16. Výhodou SMP je, že dokáže dynamicky prenášať záťaž na menej vyťažené procesory a tak obsluhovať viac procesov rýchlejšie. Myslím, že hranica v počte procesorov pri sieťových operačných systémoch Novell Netware a Windows NT na platforme Intel je zatiaľ 4. Pri Unixe a aj Windows NT na iných platformách je to viac.



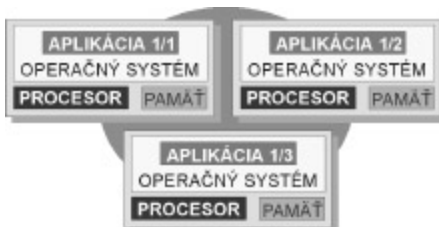
Obr. 8 SMP Multiprocessing

Tu by bolo na mieste podotknúť, že výkon systému s pridaním procesorov nenarastá lineárne a tento nárast je pri rôznych operačných systémoch rôzny.

SMP je vhodné napr. pri databázových systémoch, v ktorých sa používa jedna hlavná aplikácia pracujúca s jednou, aj keď veľkou databázou...

MPP

Masívny paralelný multiprocessing je takisto spracovanie programu viacerými procesormi, ktoré pracujú s rôznymi časťami programu a používajú svoj vlastný operačný systém a pamäť. Takto môže na jednej aplikácii pracovať 200 a viac procesorov. Na komunikáciu používajú spoločné definované rozhranie.



Obr. 9 MPP Multiprocessing

MPP je vhodné viac do prostredí, ktoré umožňujú alebo požadujú súčasné spracovanie viacerých zdrojov dát, napr. databáz, a preto sa používajú v systémoch na podporu rozhodovania alebo pri data warehousingu.

Otvorenosť

Otvorenosť je poslednou z vlastností sieťových operačných systémov, ktorou sa budeme teraz zaoberať. Táto vlastnosť by sa dala charakterizovať ako schopnosť systému spolupracovať so systémami iných výrobcov. Za otvorený systém sa považuje taký systém, ktorý je budovaný iba na štandardoch, a teda je schopný spolupracovať s ľubovoľným systémom budovaným na tých istých štandardoch.

Dnes už otázka otvorenosti nie je taká páčivá, ako to bolo pred pár rokmi, keď každý výrobca vyrábal systémy uzatvorené a schopné komunikovať iba so systémami toho istého výrobcu. Ako príklad by sme mohli uviesť sieťovú architektúru SNA firmy IBM.

Otvorenosť nemusí byť úplná. Niektoré časti systému môžu byť budované na štandardoch, iné na proprietárnych technológiách. Príklad: Compaq buduje systémy, ktoré sú otvorené, ak sa na ne pozeráte zo strany počítačovej siete, ale sú uzavreté zo strany vytvárania klastrov...

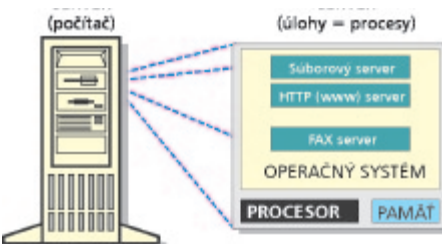
Sieťové operačné systémy, o ktorých sa chceme baviť predovšetkým, t. j. Windows NT, Novell Netware a Linux, môžeme považovať vo väčšine aspektov za otvorené.

8. časť – Servery III.

Služby servera

Dôležité je uviesť si, že základnou funkciou každého servera je poskytovanie služieb. Serverom sa teda nazýva aj každá aplikácia/úloha, ktorá zabezpečuje obsluhu požiadavky klienta. Vzniká takto zaujímavé a často máttuce spojenie:

server = počítač a server = úloha.



Obr. 1 Server je počítač, ale server je aj proces/úloha

Súborový server (file server)

Poskytovanie súborov bolo pravdepodobne prvou službou, ktorú začali servery poskytovať. Jej základným princípom je umožniť používateľom prístupovať k spoločným súborom. Súborové servery využívajú rôzne optimalizačné techniky na to, aby poskytli požadované údaje čo najrýchlejšie. Medzi takéto techniky patria už spomínané technológie RAID, využívanie vyrovnávacej pamäte (cache), optimalizácia prístupu na disky pomocou prioritizácie požiadaviek atď.

Výhodou súborových serverov je aj, že umožňujú zdieľať súbory v nehomogénnych prostrediach, napríklad používateľom používajúcim Unix alebo Linux umožnia prístupovať k súborom používateľov používajúcich MS Windows a naopak.

Dnes je pravdepodobne najvýkonnejším súborovým serverom Novell Netware, ktorý zároveň podporuje asi najširšie spektrum klientov, počnúc DOS-om, Windows 95/98/2000/NT, pokračujúc Apple Macintoshom a OS/2 a Unixom končiac.

Rovnako Windows NT je možné použiť ako súborový server. Množstvom vlastností nezaostáva za Netware, no na dosiahnutie rovnakého výkonu potrebuje výkonnejšiu hardvérovú konfiguráciu. Treba si však uvedomiť, že dnešné požiadavky používateľov na poskytovanie súborových služieb klesajú, a teda samotný výkon súborového serveru nie je primárnym kritériom výberu sieťového OS. Pokles požiadaviek na výkon súborového servera je spôsobený napríklad aj nástupom databázových serverov, ktoré nahrádzajú klasický súborový prístup k databázam napr. v súboroch DBF prístupom na základe SQL požiadaviek...

V malých sieťach, čo je náš prípad, je možné s úspechom použiť Linux, ktorý okrem štandardného NFS dokáže emulovať Netware (pomocou balíka mars-nwe) a aj Windows NT server (pomocou balíka samba). Spomínané dva balíky, najmä samba, svojím výkonom postačujú pre siete do 10 používateľov. Ich výhodou je, že bežný používateľ nerozpozná, že ide o Linux.

Špeciálnym typom súborového servera je CD-ROM server. Najčastejšie ide o samostatné zariadenie obsahujúce niekoľko CD-ROM mechanik (napríklad 7) a poskytujúce ich obsah veľkému množstvu klientov. Je vhodné použiť tieto zariadenia v prípade, že používatelia potrebujú veľmi často prístupovať k veľkému množstvu statických informácií, ktoré sú obsiahnuté na niekoľkých CD-ROM médiách. Pri menších množstvách požiadaviek možno využiť na zdieľanie CD-ROM mechaniky ľubovoľný zo spomínaných operačných systémov, napr. Windows 98.

Tlačový server (print server)

Tlač je ďalšia často požadovaná služba. Je pravda, že v súčasnosti ceny tlačiarň klesajú a je občas diskutabilné, či má zmysel inštalovať spoločnú sieťovú tlačiareň alebo je jednoduchšie kúpiť každému používateľovi vlastnú, no používanie sieťovej tlačiarne je jednoznačne ekonomickejšie a v konečnom dôsledku aj efektívnejšie.

Čo vlastne tlačový server robí? Zjednodušene povedané: zbiera požiadavky používateľov na tlač a pomocou tlačiarň pripojených k nemu ich vybavuje. Jednoduché, však? No jeho možnosti sa týmto nekonia: dokáže obsluhovať niekoľko desiatok tlačiarň, vie zabezpečiť, aby v prípade, keď tlačiareň je obsadená, sa dokument vytlačil na inej, administrátorom definovanej tlačiarň, dokáže zabezpečiť, aby určité tlačiarne mohli používať iba určití používatelia, vie sledovať využívanie jednotlivých tlačiarň používateľmi, v prípade výpadku jednej tlačiarne dokáže automaticky presmerovať výstup na inú tlačiareň. Výpočet funkcií tlačového servera by mohol ešte dlho pokračovať.

Všetky spomínané sieťové operačné systémy majú možnosť spustenia tlačového servera, no v prípade,

že ste veľká organizácia, najkvalitnejšie tlačové služby poskytujúce Novell Netware. Pre menšie siete je možné využiť zdieľanie tlačiarňou vo Windows 95/98/NT alebo použiť Linux s balíkom samba.

Databázový server

Ako sme už spomínali, databázové servery postupne nahrádzajú v niektorých typoch aplikácií, napr. informačné systémy podnikov, klasický súborový prístup. Prečo je to tak, vyplýva z nasledujúcich vlastností: dáta sú spravované a spracúvané centrálné, čo zvyšuje ich bezpečnosť a jednoducho umožňuje zabezpečiť konzistentnosť, databázové servery sú optimalizované na manipuláciu s dátami, a teda dokážu efektívnejšie splniť požiadavky, keďže klientovi odosielať iba dáta, ktoré potrebuje, výrazne znižujú záťaž komunikačného média, napr. počítačovej siete, a tým aj celého systému...

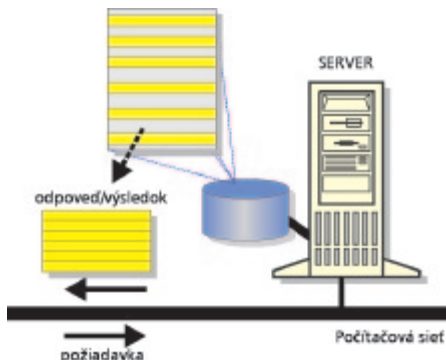
Dnes najčastejšie využívaným typom databázových serverov sú tzv. SQL servery (SQL = Structured Query Language). Príkladom komerčných serverov môžu byť Oracle (www.oracle.com), Microsoft SQL Server (www.microsoft.com) a Sybase (www.sybase.com) alebo aj Adabas D (www.softwareag.com). Z menej často využívaných databázových serverov by sme mohli uviesť mySQL (www.mysql.com) a zadarmo distribuovaný PostgreSQL (www.postgresql.org).

Nás, samozrejme, zaujíma predovšetkým to, ako databázový server ovplyvní správanie našej siete, a preto nasleduje malý príklad:

Dajme tomu, že potrebujeme v tabuľke s 10 000 riadkami, obsahujúcej údaje o zákazníkoch, nájsť všetkých zákazníkov, ktorí majú viac ako 20 a menej ako 30 rokov. Nech táto tabuľka má veľkosť 10 MB. Teda na jedného zákazníka pripadá presne 1000 bajtov. Povedzme, že takýchto zákazníkov je v tabuľke 100.

Pri súborovom prístupe existujú dve možnosti. Prvá je, že mám tabuľku zoradenú podľa veku zákazníkov. Potom aplikácia musí prečítať tú časť súboru, kde sa nachádzajú zákazníci mladší ako 30 rokov. Táto časť súboru je v najlepšom prípade, t. j. zákazníci sa nachádzajú na začiatku, veľká 100 000 bajtov. V najhoršom prípade je to o pár tisíc bajtov viac. Takýto „optimálny“ prípad, teda že tabuľka je zoradená, je však skôr výnimkou. Druhá možnosť je, že tabuľka nie je zoradená. V tomto prípade sa musí zo servera preniesť po sieti všetkých 10 000 riadkov, čo je obrovský nárast oproti skutočne potrebnému množstvu.

Použitím databázového servera sa komunikácia redukuje na odoslanie požiadavky, ktorá je veľká niekoľko sto bajtov, a prijatie odpovede, ktorá je v našom prípade spomínaných 100 000 bajtov.



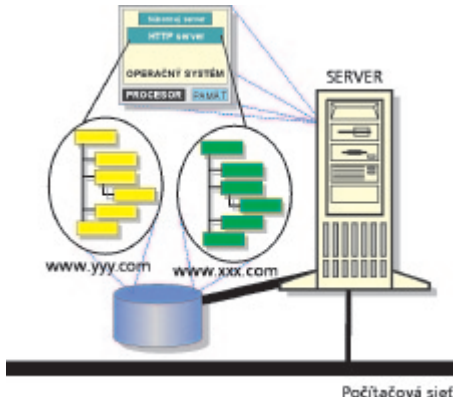
Obr. 2 Databázový server na základe požiadavky vytvorí z tabuľky uložené na jeho disku odpoveď, resp. výslednú tabuľku, ktorú potom odošle klientovi, ktorý poslal požiadavku.

V poslednom čase sa databázové servery začínajú čoraz častejšie využívať ako zdroje dát pre intranetové a internetové servery. Je to spôsobené tým, že okrem

klasických dát typu refazec, číslo, dátum a pod. pribudla možnosť uchovávať aj multimediálne dáta ako zvuky, obrázky, animácie...

HTTP server

Protokol HTTP (HyperText Transfer Protocol) a aplikácie s ním spojené, t. j. WWW servery, spôsobili boom internetu. Rozdiel medzi HTTP serverom a WWW serverom je nasledujúci: WWW server je vlastne súbor stránok s presne určenou štruktúrou. HTTP server tieto stránky dokáže čítať a poskytovať ich klientom. Jeden HTTP server môže obsluhovať viacero WWW serverov.



Obr. 3 Na serveri bežiaci HTTP server môže obsluhovať jeden alebo viac WWW serverov, ktoré sú uložené na disku servera

Medzi najpoužívanejšie HTTP servery patria Apache, Microsoft Internet Information Server a Netscape Enterprise Server.

Čo sa týka podporovaných platforiem, najrozšírenejší z nich, Apache, sa používa najmä na systémoch Linux a Unix, ktoré sú jeho materskou platformou. (Poznámka: Kdesi som videl krásnu definíciu Linuxu, súvisiacu práve so spomínaným serverom Apache: „Linux is like a wigwam. No Windows, no Gates, just Apache inside.“) Existuje však aj verzia pre Windows. Microsoft IIS je čisto windowsová záležitosť a Enterprise Server firmy Netscape existuje na všetkých troch spomínaných platformách, t. j. Linux, Novell Netware aj Windows NT.

HTTP servery sa začali, čo je pre nás zaujímavejšie, používať na budovanie vnútorných, intranetových WWW serverov. Na takýchto serveroch je možné jednoduchým spôsobom sprístupniť všetky od základných informácií, ako sú vnútorný telefónny zoznam, organizačná štruktúra podniku, organizačné normy podniku až po komplexné aplikácie pracujúce s databázovými servermi poskytujúcimi informácie napr. o záväzkoch a pohľadávkach, finančnej situácii a pod.

FTP server

Úlohou FTP servera je poskytovanie súborov. Možno sa niekomu bude zdať, že je to zbytočná činnosť, pretože to isté zabezpečujú aj súborové servery, no nie je to úplná pravda. FTP servery sa používajú predovšetkým v prostredí internetu, teda vo veľmi heterogénnom prostredí. V tomto prostredí nie je definovaný štandardný protokol, teda okrem HTTP a FTP (File Transfer Protocol), ktorý by umožňoval prenášať súbory medzi takými rozdielnymi systémami, ako sú napríklad Unix a Apple Macintosh. FTP má zabudované vlastnosti, ktoré zabezpečia, že FTP server a jeho obsah budú totožné pre všetkých klientov.

Príkladom takej vlastnosti môže byť funkcia na vypísanie obsahu adresára: v systéme MS DOS a Windows sa táto funkcia nazýva DIR, no v systéme Unix/Linux je to ls. FTP server tiež používa príkaz DIR a zabezpečí, že v prípade, keď beží na Linuxe, sa po zadaní tohto príkazu vypíše obsah adresára napriek tomu, že Linux príkaz DIR nepozná.

Najčastejšie využitie dnes nachádzajú FTP servery v spojení s HTTP servermi, ktoré síce tiež dokážu prenášať súbory, no FTP servery to robia efektívnejšie.

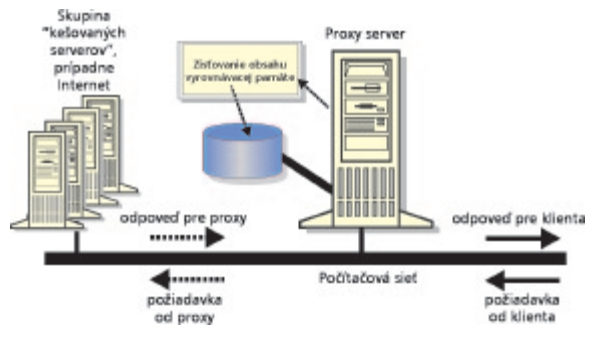
FTP server je podporovaný všetkými spomínanými platformami OS.

Proxy server

Veľmi špeciálnym typom serverov sú proxy servery. Ich úlohou je totiž vystupovať voči iným serverom v mene klientov. Možno som sa vyjadril trochu zložito, ale je to jednoduché. Zjednodušené si to vysvetlíme na príklade: Povedzme, že máme klienta, ktorý chce z FTP servera ftp.yyy.com prevziať súbor pokus.txt. Tento klient sa obráti na svoj proxy server a povie mu, že chce daný súbor z daného FTP servera. Proxy server sa potom pripojí na zvolený FTP server a prevezme vybraný súbor a následne ho odovzdá klientovi, ktorý oň žiadal.

Čo nám to prinesie? Pozitív je dost:

- vyššia bezpečnosť – pretože proxy server „maskuje“ aktivitu klienta, o klientovi sa nik za proxy serverom nedozvie
- lepšia kontrola – v prípade, že všetci klienti prístupujú do vonkajšej siete iba cez proxy server (čo sa veľmi



Obr. 4 Princíp práce proxy servera

ľahko dá urobiť), je možné sledovať, kto a čo robí, prípadne obmedziť prístup na vybrané servery vybraným používateľom

- zníženie záťaže prenosových liniek – veľmi často, prakticky je to pravidlo, sa do proxy serverov zabudováva vyrovnávací pamäť (cache), ktorá zachytáva najčastejšie navštevované stránky WWW serverov a najčastejšie prenášané súbory z FTP serverov. Keď potom klient požiadava o stránku, ktorá sa už medzičasom nahrala do vyrovnávacej pamäte proxy servera, tak proxy server iba skontroluje, či objekty na stránke na WWW serveri sú zhodné s objektmi na danej stránke v jeho vyrovnávacej pamäti, a klientovi potom odošle stránku z pamäte. Veľkosti vyrovnávacích pamätí proxy serverov sa pohybujú od niekoľko desiatok MB po niekoľko GB
- zníženie záťaže na často používaných serveroch – ide v podstate o využitie vyrovnávacej pamäte v opačnom smere, t. j. keď má niekto záujem o stránku, ktorú obsahuje jeden z kešovaných serverov, a stránka alebo súbor sa nachádza vo vyrovnávacej pamäti, proxy server poskytne stránku z pamäte a nezaťažuje server

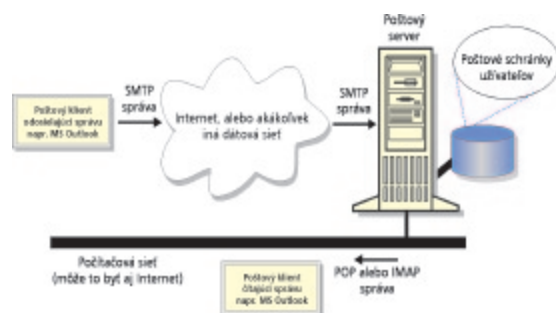
Konkrétnymi príkladmi proxy serverov by mohli byť Novell Border Manager pre Novell NetWare, Microsoft Proxy Server pre Windows NT a Squid pre Linux. Pri jednoduchších konfiguráciách je možné vo windowsovom

prostredí použiť softvér WinProxy, ktorý už obsahuje aj jednoduchý poštový server.

Poštový server (mail server)

Jednou z najčastejšie požadovaných vlastností dnešných sietí je, aby boli schopné prenášať elektronickú poštu. Túto činnosť zabezpečuje poštový server. Elektronickou poštou je možné poslať akúkoľvek správu, napríklad textovú, obrázok, program aj zvukový záznam.

V súčasnosti sa bežne používajú tri základné protokoly na prenos elektronickej pošty: SMTP, POP a IMAP. SMTP je protokol, ktorý sa používa na odosielanie správ a na ich doručenie do používateľských poštových schránok. POP vo verziách POP2 a POP3 a IMAP vo verziách IMAP3 a IMAP4 sa používajú na čítanie správ z používateľských poštových schránok.



Obr. 5 Prenos správ pomocou SMTP, POP a IMAP protokolov. Poštový server prijíma od odosielateľa správu pomocou protokolu SMTP a uloží ju do poštovej schránky. Prijímateľ si ju potom môže kedykoľvek prečítať pomocou protokolov POP alebo IMAP.

Z poštových serverov sa dnes vyvinuli tzv. groupware servery podporujúce skupinovú prácu. Tieto servery dokážu udržiavať skupinové kalendáre, sledovať plnenie úloh jednotlivých používateľov, manažovať stretnutia a pod. Príkladmi takýchto serverov môžu byť Novell GroupWise pre Novell NetWare, Microsoft Exchange pre Windows NT a napríklad aj Netscape Collabra a Messaging server pre Unix a Novell NetWare.

Skupinové nástroje nie sú zatiaľ prístupné zadarmo, no pokiaľ by ste chceli vynikajúci poštový server pre Linux, môžete použiť Sendmail. Jednoduchý poštový server pre Windows je už spomínaný WinProxy.

Faxový server

Popularita faxových serverov dnes postupne klesá, pretože ich nahrádza elektronická výmena dokumentov, napr. pomocou už spomenutej elektronickej pošty, no sú prípady, keď je kvalitný faxový server veľkým skvalitnením práce. Čo je vlastne také dobré na faxových serveroch? Bežný prístup k faxovaniu poznáte: vytlačíte si stránku a odošlete ju faxom. Pokiaľ nemáte inteligentný fax a máte smolu, že číslo je stále obsadené, pri faxovaní strávite veľa času. Rovnako vám bežný fax nepomôže, keď sa nepodarí odfaxovať iba časť strán. Problémov pri faxovaní by sa dalo vymenovať viac.

Faxové servery odstraňujú potrebu manuálnej manipulácie s dokumentmi. Dokument sa jednoducho priamo z aplikácie pošle na faxový server, čo je úkon rovnako náročný ako tlačenie, faxový server sa pýta na adresáta alebo skupinu adresátov a postará sa o odoslanie dokumentu. Na zabezpečenie komfortu je možné nastavovať isté parametre, napr. koľkokrát sa má pokúšať odoslať dokument, aké časové intervaly musia uplynúť medzi týmito pokusmi, či má odoslať iba neodslaný zvyšok alebo celý dokument a pod.

Uvedené funkcie dokážu však aj inteligentné faxy (poznámka: za cenu približne 60–100 000 Sk), no faxový server môže byť užitočný aj pri prijímaní faxov. Na

základe ID odosielateľa alebo na základe zadaného kódu pomocou DTMF, prípadne na základe iných znakov dokáže faxový server prijaté dokumenty priamo smerovať k príjemcovi, a to napríklad vo forme správy v elektronickej pošte, prípadne sa mu dokument vytlačí na tlačiarňu... Takýmto spôsobom možno ušetriť prácu recepčnej alebo sekretárky, ktorá by musela došlé faxy roznieť po kanceláriách, a zabezpečiť sa aj to, že fax si prečíta iba oprávnená osoba, t. j. prijímateľ.

Čo sa týka konkrétnych aplikácií, pre Novell Netware a aj pre Windows NT je dostupný kvalitný faxový server FaxWare od nemeckej firmy Tobit, ktorý dokáže podstatne viac, ako sme tu spomínali. Pre Linux je zadarmo dostupný balík Mgetty, ktorý sa dá použiť ako jednoduchý faxový server.

Zálohovací server

Základné pravidlo spokojného správcu siete znie: „Zálohovať, zálohovať, zálohovať.“ Veľkým pomocníkom pri zálohovaní sú zálohovacie servery. Tie umožňujú bezproblémovo zálohovať všetky potrebné údaje na všetkých počítačoch vo vašej sieti, či už sú to servery, alebo klientske stanice.

Prvým problémom zvyčajne býva, čo zálohovať. Riešenie je triviálne: Zálohovať treba všetko, čo by mohlo chýbať, keby sa to stratilo... Napríklad minuloročné cenníky je zbytočné zálohovať. So zálohovaním je často spojený tzv. recovery plan, teda plán obnovy, ktorého základ tvorí snaha o obnovenie prevádzky kritických častí informačného systému podniku v istom stanovenom časovom limite.

Aj keď je možné pomocou zálohovacích serverov zálohovať aj klientske stanice, najčastejšie sa zálohujú iba disky serverov, keďže sa nedá zaručiť, že používateľ napríklad nevyčne počítač... A preto používateľom radšej odporúčate, aby si dôležité dokumenty odkladali na disky servera, napríklad do svojho domovského adresára.

Druhým problémom je, ako zálohovať. Tento problém je už trochu náročnejší, lebo zahŕňa voľbu technológie záložného média a aj voľbu metódy zálohovania. Práve pri riešení tohto problému sa robí najviac chýb.

Voľba záložného média sa v menších spoločnostiach často končí kúpením CD zapisovača. To je chyba. Jeho obrovskou nevýhodou je, že kapacita je veľmi malá (650 MB), je veľmi pomalý a médiá sú relatívne drahé. V prípade, že je teda potrebné zálohovať celý server, ktorého kapacita je niekoľko GB, asi nebude nikoho zálohovanie na CD zapisovač baviť, a teda sa zálohovať nebude. Rovnako je to nevhodné zálohovacie zariadenie aj na bežné použitie na klientských počítačoch. CD zapisovač je vhodný na jednorazové uchovávanie statických, t. j. nemeniacich sa dát, ako sú napríklad cenníky, ponuky, prezentácie a pod.

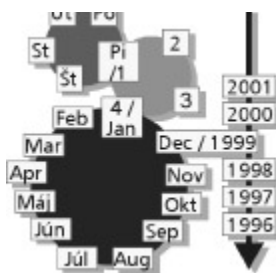
Lepšou alternatívou sú magnetické alebo magneto-optické médiá. Ich kapacita je väčšia, sú rýchlejšie, ale sú takisto relatívne drahé (napríklad ZIP, JAZZ, výmenné disky a pod.).

Najlepšou alternatívou sú magnetické pásky. Ceny za médiá sú niekoľko sto korún, kapacitne sú postačujúce (4 – 40 GB) a sú aj dostatočne rýchle (4 MB až niekoľko desiatok MB za minútu). Pre menšie spoločnosti postačujú klasické QIC mechaniky, ktoré sú cenovo najprístupnejšie. V prípade, že je potrebné zálohovať niekoľko GB až niekoľko desiatok GB, možno použiť digitálne pásky DAT (DAT DDS3 umožňujú uchovať až 12 GB nekomprimovaných dát). Ak ide o veľkú organizáciu s potrebou zálohovať desiatky GB dát, odporúča sa mechanika DLT.

Výhodou magnetických pásov je, že ich možno použiť namiesto jednoduchej mechaniky tzv. changer – výmenníkový automat, ktorý sa stará o automatické zakladanie pásov v prípade, že práve používaná páska sa naplní. Takýto „changer“ bežne obsluhuje do 10 pásov, čo napríklad v prípade DAT DDS3 znamená 120 GB zálohovaných dát.

Pri voľbe metódy zálohovania sa takisto robí veľmi veľa chýb. Väčšina administrátorov si, bohužiaľ, myslí, že na zálohu stačí mať dve médiá, ktoré sa striedajú. Počet potrebných médií je závislý predovšetkým od toho, akým chybám chceme zálohovaním predísť. Pri už spomínaných dvoch striedajúcich sa médiách síce zachránime údaje v prípade výpadku pevného disku alebo celého servera, no v žiadnom prípade sa nám nepodarí zachrániť údaje, ktoré niekto poškodil náhodou alebo úmyselne, pretože na takéto poškodenia sa prichádza často po niekoľkých dňoch až týždňoch. Rovnako je dôležité uvedomiť si, že žiadny výrobca softvéru nám nedáva záruku na to, že aj jeho softvér naše dáta nepoškodí...

Najlepšie by bolo na každý deň mať samostatné médium, čo by však napríklad v prípade DAT pásov znamenalo, že za médiá počas roka zaplatíte približne 400 000 Sk. Verím, že v prípade úplnej straty dát by ste možno boli ochotní túto sumu zaplatiť, no je to prívysoká suma. Preto sa vyvinuli rôzne metódy zálohovania, z ktorých najznámejšia je asi metóda prarodič – rodič – potomok.



Obr. 6 Zálohovanie metódou prarodič – rodič – potomok

Princíp tejto metódy je jednoduchý: na každý deň v týždni okrem posledného dňa je potrebné vyhradiť samostatné médium. Takto nám vznikne súprava tzv. denných médií. Posledný deň v týždni sa bude uchovávať na špeciálne týždňové médium. Počet týždňových médií je 4 až 5, na každý týždeň v mesiaci zvlášť. Posledný týždeň v mesiaci sa uchová ako mesačná záloha, a teda potrebujeme 11 médií na rok. Ročná záloha sa robí na samostatné médium a je to vlastne mesačná záloha posledného mesiaca v roku. Celkový počet médií používaných počas roku je pri tejto metóde je v intervale od 19 do 22.

Samozrejme, toto všetko sa dá urobiť aj bez zálohovacích serverov, tie sú však dobré na to, aby celý tento zložitý postup automatizovali a dohliadali naň...

Príkladom zálohovacích serverov môžu byť TapeWare a ArcServe pre Novell Netware a Windows NT a balík Amanda pre Linux.

Aká by mala byť konfigurácia servera?

Hneď na začiatok vyložíme karty na stôl: Ideálna konfigurácia, vhodná pre všetky požiadavky, neexistuje. Rozoberme si však základné časti postupne:

Pamäť – ak váš server má plniť iba funkcie súborového a tlačového servera, pri kapacite diskov do niekoľko GB by mohlo 64MB RAM stačiť (pre 15-20 GB potrebujete aspoň 128 MB RAM pre súborový server). Ak je vašim operačným systémom Windows NT, množstvo pamäte

radšej zdvojnásobte. Pokiaľ by ste však chceli na serveri spúšťať ďalšie aplikácie, napr. HTTP server, FAX server atď., tak je spomínaných 64 MB iba začiatok. V prípade inštalácie databázového servera platí pravidlo: čím viac pamäte, tým lepšie, no nemalo by to byť menej ako 256 MB (pre malé databázové servery by mohlo stačiť aj 128 MB).

Pevné disky – čo sa týka kapacity, tá je určená iba požiadavkami používateľov a používaných aplikácií. V dnešnej situácii, keď najmenšie predávané disky majú 4 GB, nie je problém získať potrebnú kapacitu. Je však rozumné neinvestovať priveľmi do kapacity, veď disky možno dokúpiť vždy a okrem toho zaplniť napr. 10 GB disk rozumnými dátami (nemáme na mysli MP3, MPEG či podobné „rozumné“ údaje) je celkom náročné. Vhodné je však investovať do používanej technológie. IDE a EIDE disky a radiče nie sú príliš vhodné do serverov, a preto ich používajte iba vo veľmi malých a nenáročných sieťach. Odporúčanou technológiou je SCSI. Životnosť (a aj záručné doby) diskov sú približne 5 rokov, ak teda nechceme, aby po dvoch rokoch bol náš disk v serveri nevyhovujúci a pomalý, je rozumné kúpiť hneď na začiatku niečo, čo sa považuje takmer za špičku. Napríklad dnes sa neoplatí kupovať FastSCSI s prenosovými rýchlosťami do 10 Mb/s, keď o niekoľko desiatok percent drahšie radiče UltraWide2SCSI poskytujú rýchlosti do 80 Mb/s. Optimálne riešenie je však výkonné diskové pole.

Processor – tu platí to isté ako pre pamäť. Ak chcete iba súborový server bez náročných aplikácií, postačuje akékoľvek Pentium II, povedzme 350 MHz. Toto vám bude stačiť aj v prípade menej zaťažovaných HTTP, FTP, poštových či databázových serverov. Ak plánujete inštalovať databázový server s databázou s veľkosťou niekoľkých GB a s niekoľkými desiatkami pripojených klientov, je každý procesor a každý MHz taktu procesora dobrý, a teda treba k voľbe pristupovať podobne, ako to bolo pri výbere technológií pevných diskov: nešetriť a radšej kúpiť 2 – 4 výkonné procesory naraz.

Sieťová karta – jednoznačne aspoň 100 Mb/s.

Ostatné časti nie sú podstatné, a teda je jedno, akú videokartu, monitor, klávesnicu, CD-ROM alebo myš použijete.

Na záver ešte niečo o tom, ako by asi mohol vyzerat server pre malú spoločnosť s počtom staníc 5 – 10: 128 MB RAM, 10 GB pevný disk UW2SCSI, procesor Pentium II 450 MHz, 100 Mb/s sieťová karta, zálohovacia mechanika DAT DDS2 8 GB, 1-2 MB PCI videokarta, 40× CD-ROM, klávesnica, 14" monitor. Výber operačného systému už nechám na vás.

Takýto server by mal v pohode zvládnuť rolu súborového, tlačového, HTTP, FTP, faxového aj zálohovacieho servera. Ak uvažujete o tom, že váš informačný systém implementujete na platforme niektorého z komerčných databázových serverov, tak preň radšej vyhradte samostatný počítač a nesnažte sa ho natlačiť do existujúceho súborového servera.

Dúfame, že sa na nič nezabudlo, a tak môžeme oblasť serverov konečne uzatvoriť.

9. časť – Spájanie sietí

Postupom času sa každá sieť dostane do štádia, keď sa musí spojiť s inou. Príčiny sú rôzne, počínajúc potrebou pripojiť sa na centrálu či pobočku spoločnosti alebo umožniť používateľom v lokálnej sieti prístup do internetu. Na prepájanie sietí sa používa mnoho technológií v závislosti od toho, či má byť spojenie rýchle, spoľahlivé alebo ekonomicky výhodné.

Základné pohľady na používané technológie by sme mohli rozdeliť buď podľa použitého média na drôtové a

bezdrôtové technológie, alebo podľa toho, kde sú umiestnené zariadenia, t. j. na terestriálne a neterestriálne.

Drôtové spoje sú zároveň bez výnimky terestriálnymi, pozemnými spojmi, pretože všetky zariadenia sú umiestnené na zemskom povrchu.

Komutované linky

Krátke vysvetlenie pre tých, ktorým nie je tento pojem známy: Komutované linky sú klasické telefónne linky vo verejnej telefónnej sieti. O tomto type spojov sa nebudeme príliš rozpisovať, lebo na prepájanie sietí sa používa už iba zriedka.

Jeho základnou výhodou je veľká fyzická aj finančná dostupnosť, veď telefónne linky sú prakticky všade, na ich využitie postačujú akékoľvek dva modemy a peniaze na úhradu telefónnych poplatkov. Nevýhodami sú predovšetkým kvalita, ktorá so vzdialenosťou priamo úmerne klesá, a cena, ktorá s dĺžkou využívania a so vzdialenosťou komunikujúcich bodov rastie.

ISDN

Kvalitatívne podstatne lepšou a finančne takisto nenáročnou alternatívou je použitie ISDN. Na rozdiel od komutovaných liniek je ISDN už digitálnou formou komunikácie, s čím súvisí nižšia chybovosť prenosov a možnosť vyšších prenosových rýchlostí.

Na Slovensku sa používajú dva typy rozhraní ISDN: BRI (Basic Rate Interface) a PRI (Primary Rate Interface).

Poznámka: Slovenské telekomunikácie ich označujú ako BRA (Basic Rate Access) a PRA (Primary Rate Access). Základným rozdielom je prenosová šírka kanála a, samozrejme, cena pripojenia.

BRI je určené predovšetkým domácim používateľom a malým spoločnostiam. Jeho pásmo je rozdelené na tri kanály: dva B kanály, každý so šírkou 64 kb/s, slúžiace na prenos hlasu, dát, videa a pod., a jeden D kanál so šírkou 16 kb/s, ktorý zabezpečuje signalizáciu medzi komunikujúcimi bodmi. Kanály B je možné používať samostatne alebo ich možno zlúčiť do jedného kanála širokého 128 kb/s. Dôležité je uvedomiť si, že žiadny z kanálov B nie je nijako vyhradený na dáta alebo na prenos hlasu, a teda je možné v oboch kanáloch nezávisle prenášať hlas, údaje alebo ich prenos ľubovoľne kombinovať.

PRI je so svojimi 30 B kanálmi a jedným 64 kb/s D kanálom určený pre väčšie spoločnosti, prípadne na náročnejšie prenosy. Platia pri ňom rovnaké pravidlá ako pri rozhraní BRI.

Spoplatňovanie služieb ISDN je podobné ako pri bežných telefónnych linkách: platí sa mesačný paušál a poplatky za pretelefonované impulzy. Mesačný paušál sa platí za celé rozhranie (600 Sk za BRI a 11 000 Sk za PRI) a používanie každého kanála sa tarifkuje samostatne, ako keby každý kanál bol samostatnou telefónnou linkou. Poplatky za impulzy sú rovnaké ako pri telefónnych (komutovaných) linkách.

Prenajaté okruhy

Najčastejším spôsobom spájania sietí je prenajať si kábel alebo časť kábla od telekomunikačnej spoločnosti (v našom prípade asi od Slovenských telekomunikácií). Existujú dva základné typy prenajatého okruhu: analógový a digitálny.

Napríklad Slovenské telekomunikácie delia analógové okruhy podľa kvality na dva základné typy: M1025 a kvalitnejší M1020. Tie sa potom ďalej delia na dvoj- a štvordrôtové.

Čo sa týka použitia analógových prenajatých okruhov, vzhľadom na ich kvalitu sa hodia iba na použitie v nenáročných aplikáciách. S bežnými modemami na nich možno dosiahnuť maximálnu prenosovú rýchlosť 33,6

kb/s, čo je približne 4 KB/s. Takýto okruh sa dá použiť aj na vytvorenie rýchlejšieho kanála, napr. 2 Mb/s, no treba zmeniť používanú technológiu, a teda aj koncové zariadenia. Potom je však výhodnejšie prenajať si digitálny okruh.

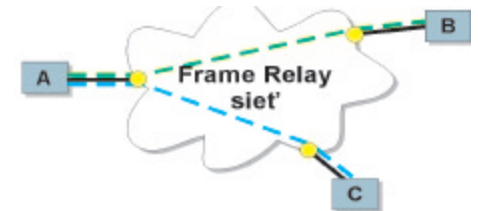
Základným rozdielom medzi analógovým a digitálnym okruhom je, že poskytovateľ digitálneho okruhu garantuje požadovanú šírku pásma. Fyzicky sa často použije ten istý kábel, ktorý bol predtým použitý na analógový prenajatý okruh, no zmení sa technológia. Dnes sa najčastejšie používajú tzv. xDSL technológie (HDSL, VDSL, ADSL...). Pomocou nich je možné na bežných kábloch dosahovať rýchlosti až niekoľko Mb/s. Bežné sú rýchlosti do 2 Mb/s.

Na rozdiel od analógových okruhov, kde sa platilo za kvalitu okruhu a bolo jedno, akou rýchlosťou sa dáta prenášajú, na digitálnych prenajatých okruhoch sa platí za rýchlosť, čo znamená, že zákazník si môže určiť, akou rýchlosťou bude na linke komunikovať, napr. 64 kb/s a potom bude platiť za 64 kb/s...

Používanie prenajatých okruhov, napr. digitálnych, síce poskytujú garanciu, že celé prenajaté pásmo je vaše, a dáva aj najväčšiu voľnosť v konfigurácii, ale v prípade, že je potrebné prepojiť viac ako dva body medzi sebou, sa prepájanie pomocou prenajatých okruhov stáva finančne veľmi náročným. Zaujímavou alternatívou je Frame Relay.

Frame Relay

Zatiaľ čo pri prenajatých okruhoch sa prenajímali fyzické prepojenia, Frame Relay umožňuje medzi komunikujúcimi bodmi vytváranie virtuálnych, teda logických ciest s vlastnosťami fyzických prepojení.



Obrázok č.1 Pripojenie koncových bodov do siete Frame Relay

Základným predpokladom budovania prepojenia pomocou Frame Relay je existencia poskytovateľa tejto služby. Na Slovensku sú to napríklad Slovenské telekomunikácie a EuroTel. Prvým krokom je plánovanie virtuálnych okruhov, t. j. počtu spojení medzi bodmi. Dôležitým parametrom každého virtuálneho okruhu je garantovaná prenosová rýchlosť – označuje sa CIR (Committed Information Rate). Ďalším krokom je vybudovanie pripojenia do siete poskytovateľa, t. j. vybudovanie prístupového okruhu. Na vytvorenie prístupového okruhu sa používajú prenajaté okruhy. Rýchlosť prístupového okruhu by mala byť vyššia ako súčet CIR rýchlostí virtuálnych okruhov privedených do daného prístupového okruhu. Napríklad na obrázku č. 1 máme vytvorené dva virtuálne okruhy z A do B a z A do C. Nech ich CIR je 64 kb/s. Potom rýchlosť prístupového okruhu v bode A by mala byť aspoň 128 kb/s. Rýchlosti prístupových bodov v B a C musia byť aspoň 64 kb/s. Za zmienku stojí, že CIR je rýchlosť, ktorú poskytovateľ garantuje pri plnej záťaži. Pokiaľ je záťaž siete Frame Relay nižšia, môže byť reálna prenosová rýchlosť medzi bodmi vyššia ako CIR a môže sa prakticky vyrovnáť rýchlosti prístupového okruhu. Preto v prípadoch, keď plánujete robiť veľké prenosy dát mimo špičkových hodín, teda napr. v noci, oplatí sa mať rýchlosti prístupových bodov vyššie, ako je CIR.

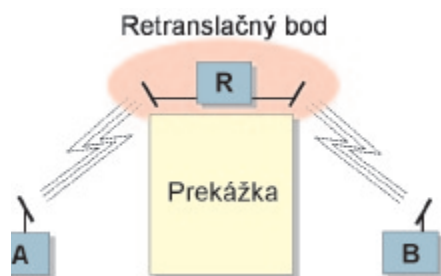
Internet

Internet dnes môžeme tiež považovať za prenosové médium. Použitie je podobné, ako sme uviedli pri Frame Relay, t. j. prenajímajú sa iba pevné okruhy k prístupovým uzlom internetu, a nie celá trasa napr. z bodu A do bodu B. Na rozdiel od Frame Relay však v internete neexistuje garantovaná prenosová rýchlosť. Okrem samotného prenosového média internet poskytuje aj iné služby, a preto pokiaľ sa používa iba ako prenosové médium, je jeho použitie relatívne drahé a neefektívne.

Mikrovlnné spoje

Čoraz populárnejším spôsobom budovania sieťových spojov je použitie bezdrôtových mikrovlnných spojov. Ich popularita súvisí s tým, že poskytujú vysokorychlostné spojenie ekonomicky efektívnou formou, ktorá zahŕňa iba náklady na zriadenie a zanedbateľné ročné poplatky.

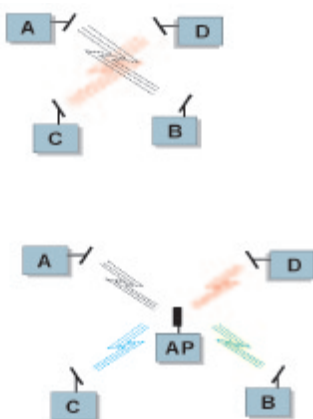
Medzi nevýhody mikrovlnných spojov patrí predovšetkým ich závislosť od viditeľnosti prepájaných bodov. V prípade, že medzi bodmi nie je priama viditeľnosť, treba budovať tzv. retranslačné body a cena spoja sa zvyšuje.



Obrázok č. 2 V prípade, že medzi bodmi neexistuje priama viditeľnosť, je potrebné vybudovať retranslačný bod

Z pohľadu počtu bodov, ktoré sa zúčastňujú na komunikácii, sa dajú mikrovlnné spoje rozdeliť na dve základné skupiny: komunikácia bod-bod a komunikácia bod-multi-bod.

Komunikáciu bod-bod znázorňuje obrázok č. 3, ktorý zachytáva dve komunikujúce dvojice bodov A-B a C-D. Medzi komunikujúcimi bodmi sa pri spojení bod-bod vyžaduje priama viditeľnosť.



Obrázok č. 3 Komunikácia bod-bod
Obrázok č. 4 Komunikácia bod-multi-bod

Komunikácia bod-multi-bod (obrázok č. 4) sa používa v prípade, že treba spojiť viac bodov ako dva. Výhodou tejto komunikácie je, že nie je nevyhnutné, aby sa koncové body „videli“, stačí, ak každý z bodov vidí centrálny tzv. prístupový bod (Access Point), ktorý zabezpečuje komunikáciu medzi koncovými bodmi. Nevýhodou komunikácie bod-multi-bod je jej vyššia finančná náročnosť oproti komunikácii bod-bod.

Poznámka: Viac informácií o rádiových spojoch môžete nájsť na stránke www.ies.sk.

Satelitné spojenie

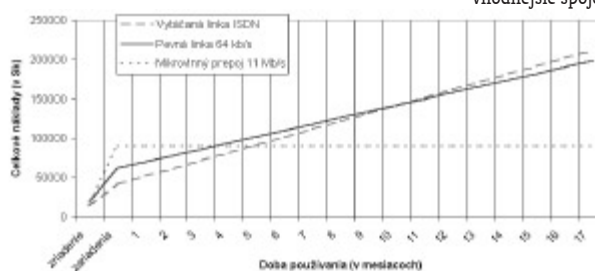
Využitie satelitov na prenos dát na Slovensku zaznamenal značný nárast najmä začiatkom 90. rokov, keď potreba komunikácie prudko narastala, no infraštruktúra komunikačných kanálov na Slovensku bolo úbohá. Dnes sa spojenia sieť pomocou satelitov už nerealizujú v takom rozsahu, lebo kvalita terestriálnych komunikačných trás zaznamenala značný nárast. Stále však existujú aplikácie, v ktorých sa nájde uplatnenie aj pre satelitné spoje: zálohovanie pozemných trás, prepojenia veľmi vzdialených miest, pripojenie miest, v ktorých neexistuje možnosť pozemného spojenia, a pod.

Medzi výhody satelitného spojenia sa dá počítať napr. pokrytie obrovského územia, takmer okamžitá možnosť nasadenia, nezávislosť od počasia.

Satelitné spojenie má však aj nevýhody: poplatok za prepojenie dvoch bodov rýchlosťou 64 kb/s je približne 80 000 Sk mesačne, vzhľadom na dĺžku trasy, ktorú musí signál prekonať, vznikajú nepríjemné, aj niekoľkosekundové oneskorenia, ktoré sú napríklad v terminálových aplikáciách neakceptovateľné.

Porovnanie použitia jednotlivých technológií na spojenie v rámci mesta

Na mestské spojenie dvoch bodov sa používajú takmer všetky spomínané technológie, azda okrem Frame Relay a internetu. Graf č. 1 ukazuje finančnú náročnosť použitia jednotlivých technológií a môžeme ho využiť pri rozhodovaní o výbere technológie.



Graf č. 1 Náklady na prepojenie dvoch bodov v rámci mesta

Graf č. 1 predpokladá nasledujúce skutočnosti: prepojenie medzi dvoma bodmi musí trvať aspoň 8 hodín denne a v prípade mikrovlnného spoja musí existovať priama viditeľnosť koncových bodov, koncové body nie sú vzdialené viac ako 6 km a pre mikrovlnný spoj je použité frekvenčné pásmo 2,4 GHz. Z tohto grafu vyplýva, že za daných podmienok sa oplatí použiť mikrovlnný spoj, pretože sa náklady na jeho vybudovanie vrátia už po 5 mesiacoch používania a jeho výkon je oproti ISDN a 64 kb/s linke neporovnateľne vyšší. V prípade, že medzi bodmi neexistuje priama viditeľnosť (náklady na retranslačný bod mikrovlnného spojenia za daných podmienok by boli asi 100 000 Sk), je pri používaní dlhšom ako 10 mesiacov výhodnejšie zriadiť pevnú linku, lebo náklady na prevádzku ISDN po 10 mesiacoch prekročia náklady na pevnú linku.

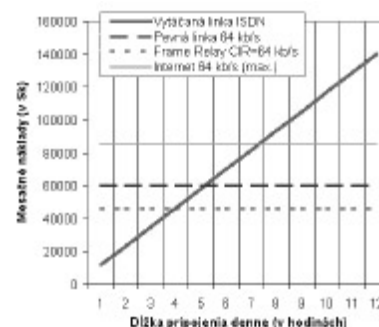
Porovnanie použitia jednotlivých technológií na pripojenie na internet

Pripájanie na internet je pravdepodobne najčastejší spôsob, keď sa spájajú siete (konkrétne: LAN sa pripája na internet). Pripojenie na sieť internet sa najčastejšie realizuje v rámci mesta, a preto môžeme odkázať na spomínaný graf č. 1. Tento graf však odzrkadľuje iba telekomunikačné náklady a nezahráva poplatky poskytovateľovi internetu. Pri zarataní poplatkov ISP sa výhody pevných liniek oproti vytáčaným linkám začínajú pre-

javovať približne pri 6-8 hodinách pripojenia denne. Finančný efekt (úspora) mikrovlnného prepojenia sa oproti prenajatým okruhom prejaví približne po 10 mesiacoch pripojenia.

Porovnanie použitia jednotlivých technológií na spojenie troch vzdialených miest

Pre tento prípad sme si zvolili nasledujúce podmienky: spoločnosť XYZ, s. r. o., má svoje pobočky v Bratislave (BA), Banskej Bystrici (BB) a Košiciach (KE). Používa on line informačný systém, a teda potrebuje komunikovať s pobočkami po celý pracovný čas.



Graf č. 2 Spojenie BA-BB a BA-KE pomocou rôznych technológií

Graf č. 2 jednoznačne ukazuje, že pre daný prípad je najvhodnejšie spojenie pomocou Frame Relay. Pokiaľ by však stačilo komunikovať denne menej ako 4 hodiny, je výhodnejšie použiť ISDN. Zaujímavosťou je aj využitie internetu, kde mesačné poplatky sú vyššie ako pri prenájme pevných okruhov a skutočná prenosová rýchlosť nie je garantovaná.

Záver

Samozrejme, existuje ešte mnoho iných spôsobov prepojenia sietí (napr. laserové systémy a pod.) a ich rôzne kombinácie, ktorým sme sa dnes nevenovali, no našim cieľom bolo veľmi stručne opísať bežne dostupné technológie a ich nasadenie v podmienkach malých sietí.

10. časť: Spájanie sietí II

V predošlej časti seriálu sme sa venovali technológiám používaným na spájanie sietí a ich všeobecnému porovnaniu. Teraz sa zameriame na konkrétne riešenia. Hneď na začiatku by som vás však chcel upozorniť, že v príkladoch bude kladený dôraz iba na základnú funkcionálnu spojenia, čo v niektorých prípadoch (napr. cenové porovnanie produktov Cisco a Zyxxel) môže spôsobovať drobné nedorozumenia.

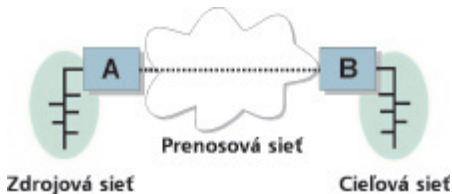
Základné časti spoja

Každý spoj sa skladá z niekoľkých základných častí: zdrojová a cieľová sieť, vstupno-výstupné brány siete a prenosová sieť.

Zdrojová a cieľová sieť sú siete, ktoré chceme spojiť. V princípe je jedno, o aké siete ide. Dnes sú to najčastejšie siete LAN, založené na technológii Ethernet a používané prenosový protokol TCP/IP. V ďalších prípadoch budeme používať práve takéto siete.

Pod prenosovou sieťou budeme chápať akúkoľvek sieť, ktorá fyzicky spojí naše dve siete. Fyzicky môže ísť o prenajatý kábel, verejnú dátovú sieť, mikrovlny,

internet a pod. Pretože prenosová sieť je často založená na iných technológiách a/alebo protokoloch, ako sú technológie použité v zdrojovej a cieľovej sieti, treba použiť zariadenia, ktoré zabezpečia po trebnú konverziu. Pod pojmom vstupno-výstupná brána si môžeme predstaviť veľké množstvo zariadení, počínajúc sieťovým mostom, smerovačom pokračujúc a sieťovou bránou končiac. Vstupno-výstupné brány majú presne špecifikované komunikačné rozhrania, t. j. technológie + protokoly, ktoré je možné na ne pripojiť. Keďže sme túto veľmi dôležitú oblasť zabudli v predchádzajúcej časti spomenúť, dovolíme si trochu odbočiť k teórii.



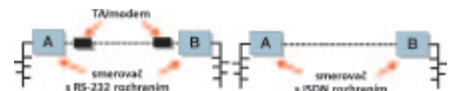
Obr.1 Základná sieť spojenia dvoch sietí

Komunikačné rozhrania

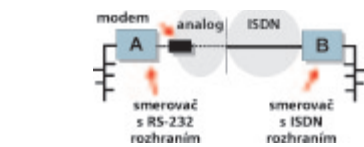
Základné rozdelenie rozhraní je jednoduché: každá V-V brána musí mať minimálne dve – jedno na komunikáciu s pripájanou sieťou a druhé na pripojenie sa k prenosovej sieti. Komunikačné rozhranie, na ktoré pripájame spájané siete, budeme v ďalšom texte nazývať rozhranie LAN, rozhranie na pripojenie prenosovej siete zasa rozhranie WAN. (Poznámka: Rozdelenie na rozhranie WAN a LAN je iba umelé, pretože tieto rozhrania sú rovnocenné.)

Rozhranie LAN je najčastejšie špecifikované ako ethernetové, t. j. 10Base-T alebo 100Base-TX (konektor RJ-45) a 10Base-2 (konektor AUI). Iba zriedka sa dnes používa iné.

Pri rozhraní WAN je to už pestršie. Najmä pri



Obr. 2 Prepojenie pomocou komutovanej alebo ISDN linky si vyžaduje iba minimálne investície



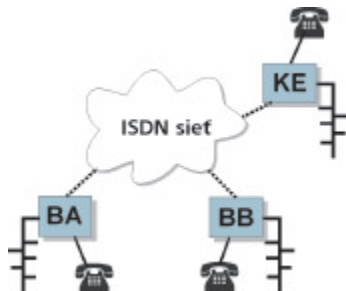
Obr. 3 Takto to fungovať nebude

smerovačoch sa bežne používa niekoľko rozhraní. Na naše účely by sme rozhrania WAN mohli rozdeliť na dve skupiny: sériové rozhrania a ostatné (ATM, SONET, FDDI...). V našich podmienkach nás najviac budú zaujímať práve sériové rozhrania. Tie môžeme ďalej deliť na asynchrónne a synchrónne. Princíp sériového prenosu je zachovaný pri oboch: po kábli je v jednom okamihu prenášaný práve jeden bit. Asynchrónny prenos by sa dal zjednodušene charakterizovať ako náhodný prenos, lebo prijímacia stanica nikdy nevie, kedy jej vysielacia stanica pošle ďalší bit. Tento prenos je vzhľadom na uvedený spôsob práce relatívne pomalý. Pri asynchrónnych rozhraniach sa používajú rýchlosti do 128 kb/s.

Tab. 1		
tri nové smerovače Zyxel Prestige 153X + káble	66 900,-	
alebo tri nové smerovače Cisco 1601-R + ďalší sériový modul pre BA + káble	230 000,-	
alebo upgrade dvoch smerovačov Cisco 1603-R + jeden smerovač Cisco 1601-R + sériový modul + káble	130 400,-	
zariadenie dvoch 64 kb/s línií BA-BB, BA-KE	80 000,-	

Asynchrónne prenosy sa používajú takmer výlučne na prenos časovo necitlivých údajov, ako sú napr. prenosy údajov medzi počítačmi. Ako fyzické rozhranie sa používa RS-232 (v počítačoch sa RS-232 používa v tzv. COM portoch). Na toto rozhranie možno pripojiť štandardné modemy.

Z hľadiska komunikácie sú zaujímavejšie synchrónne prenosy. Pri nich už nejde o náhodný prenos. Princíp sa dá zjednodušene opísať takto: komunikujúce zariadenia sa najprv zosynchronizujú a až potom začne prebiehať prenos. Po zosynchronizovaní prijímacie zariadenie vie, presne kedy príde nasledujúci bit, a preto sa nemusí zdržiavať detekciou a môže sa sústrediť na spracovanie. Synchrónne prenosy môžu preto dosahovať podstatne vyššie rýchlosti ako asynchrónne. Bežnou rýchlosťou sú 2 Mb/s. Okrem vyššej rýchlosti synchrónne prenosy garantujú aj plynulosť prenosu, a preto sa môžu po užívať na prenos hlasu a videa. Rozhrania, na ktorých je možné uskutočňovať synchrónne prenosy, sú napr. V.35, X.21 a G.703. Najčastejšie sa používajú rozhrania V.35 a X.21.



Obr. 4 Prepojenie pobočiek pomocou siete ISDN s použitím ISDN smerovačov Zyxel Prestige 100 alebo Cisco 775M/803. Analogové zariadenia, ako telefón, fax alebo telefónna ústredňa, sa pripájajú priamo na smerovač

(Poznámka: Z pohľadu používateľa je úplne jedno, ktoré rozhranie sa použije, je to skôr otázka, ktoré rozhrania vám poskytne váš poskytovateľ telekomunikačných služieb, napr. Slovenské telekomunikácie.)

Spojenie sietí vytáčanou komutovanou linkou



Obr. 5 Schéma zapojenia digitálneho okruhu. Namiesto rozhrania V.35 možno použiť napr. rozhranie X.21

Spojenie vytáčanou komutovanou (bežnou telefónnou) linkou alebo vytáčanou ISDN linkou je asi najčastejší typ spojenia používaný na spájanie sietí, pretože ide o najlacnejšie a najrýchlejšie realizovateľný typ.

Kedy použiť tento typ?

Vytáčaná komutovaná alebo vytáčaná ISDN linka sa používa v prípadoch, keď je potrebné na relatívne krátky čas vytvoriť spojenie medzi dvoma bodmi. Kva lita tívne parametre tohto spojenia sú vhodné na relatívne nenáročný prenos. V bežných podmienkach je tento typ spojenia vhodný na prenos elektronickej pošty, prenosy malého množstva dát (rádovo niekoľko MB denne), prístup na internet a pod. Finančne najnáročnejšou časťou takéhoto spojenia sú nakoniec mesačné poplatky za spojenie...

Čo potrebujeme?

Na to, aby sme mohli spojiť siete komutovanou linkou, potrebujeme dva smerovače a dva

modemy alebo terminálové adaptéry v prípade ISDN. (Poznámka: Pre smerovače, ktoré majú možnosť priameho pripojenia na ISDN, nepotrebujeme terminálový adaptér, lebo je zabudovaný priamo v smerovači.)

Ako smerovač sa dá použiť aj počítač s inštalovaným vhodným softvérom. V tom to prípade možno použiť akúkoľvek 486-ku s inštalovaným Linuxom. Podmienkou je mať jadro skompilované s podporou IP forwardingu a mať inštalované napr. balíky diald, mgetty a pppd.

Pokiaľ dávate prednosť osvedčeným zariadeniam alebo nemáte chuť konfigurovať Linux, existuje relatívne široká paleta HW smerovačov rôznych výrobcov. Spomeniem iba najpoužívanejšie: Cisco 800 (ISDN-BRI), Cisco 1600 (ISDN-BRI aj RS-232) a Zyxel Prestige 100 (ISDN-BRI).

Zapojenie:

Tak ako ukazuje obrázok č. 2, riešenie je viac. V prípade, že chcete vytvoriť spojenie cez klasickú telefónnu sieť, potrebujete okrem smerovačov s RS-232 rozhraním aj dva modemy. Ak máte na oboch stranách k dispozícii ISDN linku, je možné zakúpiť priamo smerovače s rozhraním ISDN a priamo ich na linku pripojiť. No pretože zapojenie ISDN linky do smerovača pri väčšine typov smerovačov úplne znemožní jej využitie napr. na telefonovanie, pri malých inštaláciách je rozumnejšie použiť smerovače s rozhraním RS-232 a zapojiť pred ne ISDN terminálový adaptér. Toto riešenie umožní použiť ISDN linku aj na iné ako dátové prenosy.

POZOR! Používateľ má často predstavu, že v prípade, keď na jednom z prepájaných miest má zavedenú ISDN linku, bol by hriech ju nevyužiť. Preto sa občas urobí



Obr. 7 Prepojenie dvoch bodov (sietí) použitím adaptérov inštalovaných priamo v počítači

zapojenie, ktoré je znázornené na obrázku č. 3. Bohužiaľ, nefunguje to.

Ukážkový prípad:

□ Situácia:

Spoločnosť XYZ, s. r. o., pôsobí v troch lokalitách: v Bratislave, v Banskej Bystrici a v Košiciach. Potrebujú zabezpečiť prístup z pobočiek v BB a v KE do centrálnej databázy v BA. Tento prístup bude viac-menej sporadický. Priemerná denná dĺžka pripojenia sa odhaduje na jednu hodinu. Keďže všetko stojí peniaze, neplánujú ani v jednej pobočke investovať do nových komunikačných línií, ale chcú využiť existujúce ISDN linky, ktoré používajú aj na faxové a hlasové prenosy.

□ Riešenie:

Pretože pripojenie je denne pomerne krátke, t. j. 1 hodina, neoplatí sa rozmýšľať nad pevným pripojením či už prenajatou linkou, pomocou Frame Relay, alebo pomocou internetu. Technológia je viac-menej daná existujúcou situáciou: ISDN. Keďže treba zachovať použitie existujúcich línií ISDN aj na prenos hlasu, je nevyhnutné použiť ISDN smerovač s analogovými portami, tzv. POTS portami, do ktorých možno pripojiť klasický telefón alebo fax, alebo je potrebné použiť smerovač s rozhraním RS-232 a na pripojenie na ISDN použiť ISDN terminálový adaptér.

Smerovače je potom možné nakonfigurovať tak, aby sa na základe používateľovej požiadavky automaticky pripojili na požadovaný bod. Obrázok č. 4 zobrazuje výsledné riešenie pomocou smerovačov Zyxel Prestige 100, Cisco 775M alebo Cisco 803. Rozpočet takéhoto riešenia je asi 40 000 Sk bez DPH pri použití smerovačov

Zykel Prestige 100 a približne 117 300 Sk bez DPH pri použití smerovačov Cisco 803. Pokiaľ však budete dostatočne prezieravi a budete očakávať nárast prevádzky medzi pobočkami (a nárast je vždy takmer istý), zaobstaráte si radšej smerovače s možnosťou zapojenia aspoň dvoch rozhraní WAN, prípadne modulárne smerovače, pri ktorých možno typ rozhrania podľa potreby zmeniť. Pri kladom vhodných zariadení sú smerovače Cisco 1603-R, ktoré sú osadené jedným ISDN-PRI portom, ale majú možnosť prídania ďalšieho rozhrania. Takýto „špás“ vás v prípade realizácie vyjde asi na 195 000 Sk bez DPH.

Spojenie sietí prenajatým okruhom

V prípade, že predpokladaná denná doba spojenia dvoch miest presiahne istú hranicu, je ekonomicky výhodnejšie začať uvažovať o stálom prepojení. (Poznámka: Analýzu toho, kedy začína byť pevné spojenie výhodnejšie, sme robili v predošlom čísle.)

Existuje niekoľko spôsobov, ako pevne prepojiť dva body: prenajatým telekomunikačným okruhom (prenajatá linka, pevná linka, leased line), rádiovo-reléovým spojom (mikrovlnný spoj), pomocou verejnej dátovej siete alebo pomocou satelitných terminálov VSAT.

Najjednoduchším (a na krátke vzdialenosti aj najlacnejším) spôsobom je realizovať stále prepojenie pomocou prenajatého okruhu. Existujú dva typy prenajatých okruhov: analógový, ktorý bude, bohužiaľ, vinou Slovenských telekomunikácií v dohľadnej dobe prakticky fikciou, a digitálny. Zjednodušene povedané, v podstate ide takmer vždy o ten istý kábel, ale raz vám dajú iba kábel (analógový okruh) a garantujú iba fyzikálne parametre (od por, šum, frekvenčné pás mo) alebo vám dajú kábel aj so zariadením (digitálny okruh) a garantujú prenosovú rýchlosť.

Ako sme už spomínali, pri analógových okruhoch vám ich poskytovateľ vyvedie na stôl iba dva alebo štyri drôty a zariadenie si musíte zabezpečiť sami. Najjednoduchším spôsobom, ako využiť analógový okruh, je pripojiť naň bežne dostupné asynchrónne modemy, ktoré, samozrejme, musia mať možnosť práce na prenajatých okruhoch. Maximálna rýchlosť, ktorá sa dá použitím takýchto modemov dosiahnuť, je 33,6 kb/s. Nie je to síce nijaká úžasná rýchlosť, ale ako alternatíva namiesto vytáčaného spojenia to stačí.

V prípade, že chcete na analógovom okruhu dosiahnuť vyššie rýchlosti, musíte použiť niektorú z xDSL technológií. Bežne používané HDSL modemy (toto sú už synchronne prenosy) dosahujú rýchlosti 2 Mb/s. Ich ceny sú však podstatne vyššie ako ceny asynchrónnych modemov.

Digitálne okruhy sú síce drahšie, ale poskytovateľ na nich garantuje prenosovú rýchlosť (a hlavne budú dostupné aj po 31. 3. 2000). Pri ich zriaďovaní sa definuje typ rozhrania (V.35, X.21, G.703) a prenosová rýchlosť. Rýchlosť sa určuje ako násobky 64 kb/s. (Poznámka: Často sa môžete stretnúť so zápisom $N \times 64$, ktorý vyjadruje práve prenosovú rýchlosť linky.)

Kedy použiť tento typ?

Vtedy, keď je to ekonomicky výhodnejšie ako používanie vytáčaného komutovanej linky; prakticky vtedy, keď spojenie medzi dvoma bodmi trvá viac ako 10 hodín denne v rámci mesta. Pri medzimestských spojeniach sa tento

limit skracuje. Ešte k jednotlivým typom okruhov: na analógový zabudnite, používajte digitálne okruhy.

Čo potrebujeme?

Na prepojenie dvoch sietí pomocou digitálneho prenajatého okruhu potrebujeme: prenajatý okruh (pozor, chvíľku trvá, kým vám ho pridelia, takže oň požiadajte zavčasu), dva smerovače so synchronnými sériovými portami, dva káble s ko nektormi podľa typu rozhrania, ktoré bude mať prenajatý okruh. Je samozrejme, že ak dostaneme okruh V.35, musíme mať kábel, ktorý sa bude na jednom konci dať pripojiť na okruh a druhý koniec bude možné pripojiť na sériový port smerovača.

Zapojenie

Na počudovanie je zapojenie jednoduchšie ako zapojenie pri vytáčanom spojení pomocou komutovanej linky (pozri obrázok č. 5). Ešte je asi dôležité podotknúť, že si netreba robiť starosti s typom rozhrania na smerovači. Pretože rozhrania X.21 aj V.35 sú synchronne sériové rozhrania, vie takmer každý smerovač podľa použitého kábla určiť, o aké rozhranie ide, a do káže mu svoj sériový port prispôbiť.

Pokiaľ teda správne nastavíte adresy jednotlivých portov smerovačov, nastavíte rovnaký komunikačný protokol (napr. PPP) a správnu rýchlosť, mal by sa vám takýto spoj rozbehnúť okamžite.

Ukážkový prípad

□ Situácia

Vráťme sa k situácii firmy XYZ, s. r. o., no predĺžme čas spojenia na 5-7 hodín/deň.

□ Riešenie

Za uvedených podmienok prenosy už značne finančne zaťažujú spoločnosť. Rovnako blokujú aj komunikačné linky. Takže prišiel čas na prechod na trvalé spojenie. Tu však treba rátať s relatívne vysokými počiatocnými nákladmi. Pokiaľ ste však pôvodne zakúpili modulárne smerovače, napr. už spomínané Cisco 1603-R, tak iba doplatíte za dokúpenie potrebných modulov – existujúce ISDN porty je možné použiť ako záložné porty v prípade výpadku prenajatého okruhu. Okrem samotných smerovačov a káblov je však potrebné počítať aj s poplatkami za zriadenie prenajatého okruhu. Roz počet by mohol vyzeráť, ako je uvedené v tab. 1.

Takže počiatocné náklady budú približne 146 900 Sk bez DPH pri použití zariadení Zykel a približne 310 000 Sk pri použití zariadení Cisco.

Spojenie sietí mikrovlnným rádiovým spojom

Mikrovlnné spoje sú vynikajúcou alternatívou k prenajatým okruhom, najmä na kratšie vzdialenosti a pri nutnosti zabezpečiť vysoké komunikačné rýchlosti, lebo poplatky za ich používanie sú v porovnaní s poplatkami za prenajaté okruhy podstatne nižšie.

Pri rozhodovaní sa o tom, či použiť mikrovlnný spoj, je základnou otázkou, aké pásmo sa použije: voľné alebo chránené. Rozdiel medzi nimi je v tom, že pri použití voľného pásma (na Slovensku je to 2,4 GHz) nie je síce potrebné platiť poplatky, ale vaše prenosy môžu byť rušené inými spojami (problematickým miestom po čase bude napr. centrum Bratislavy). V chránenom pásme, t. j. 10 GHz a vyššie (pásmom je niekoľko), máte síce istotu, že váš spoj je zaručene „čistý“, ale treba vybavovať rôzne legislatívne povolenia a platiť poplatky. Nehovoriac o tom, že vytvorenie spoja bod-bod v chránenom pásme stojí rádovo viac ako v nechránenom pásme. Minimálna cena spoja bod-bod v chránenom pásme je približne 400 000 Sk, priemerná sa pohybuje

nad 600 000 Sk, a pokiaľ chcete použiť špičkové zariadenia, zaplatíte asi 1,5 milióna Sk za spoj. Už z týchto odhadov je jasné, že chránené pásmo je určené skôr na profesionálne po užitie a pre náročných zákazníkov, ako sú podniky, banky a pod.

Keďže tento seriál sa venuje malým sieťam, budeme sa orientovať na voľné pásmo 2,4 GHz.

Kedy použiť tento typ?

Pri tomto type spojenia je veľmi ťažké zovšeobecniť vhodnosť jeho použitia, pretože existuje množstvo parametrov, ktoré môžu ovplyvniť vhodnosť nasadenia. Uvedieme aspoň základné pravidlo, ktoré musí platiť pri jednoduchých spojoch:

- Musí existovať priama viditeľnosť medzi spájanými bodmi, prípadne z koncových bodov musí byť viditeľný jeden spoločný bod, na ktorý možno umiestniť retranslačný uzol (v ceste nesmú stáť ani stromy).

Čo potrebujeme?

Výhodou zariadení používaných v tomto pásme je, že väčšinou pracujú ako ethernetové mosty, a teda majú zabudované priamo ethernetové rozhranie. To znamená, že okrem dvoch zariadení nepotrebuje už nič viac. V prípade, že chcete vytvoriť spoj na vzdialenosť väčšiu ako 300–400 metrov, budete pravdepodobne potrebovať aj externú anténu s príslušenstvom. Často sa však medzi tieto zariadenia a lokálnu sieť vkladajú ešte smerovače, tie však nie sú nevyhnutné.

Zapojenie

Zapojenie je skutočne jednoduché. Pri použití externej antény a inštalácii vysokofrekvenčného koaxiálneho kábla si treba dať pozor na kvalitu ukončenia konektorov a na správne nasmerovanie antény. Pokiaľ je vzdialenosť krátka, tak 200–300 metrov (občas aj viac), nie je potrebné použiť externé antény, čo maximálne uľahčuje celú inštaláciu. Pri zapojení bez externých antén by sa však mali zariadenia vidieť, t. j. mali by byť nanajvýš za sklom.

Tento fakt je predpokladom na vytvorenie najlacnejšieho možného spoja, a to použitím ISA adaptérov, ktorý je určený najmä pre nenáročných zákazníkov (obrázok č. 7).

Ukážkový prípad

□ Situácia

Nám chronicky známa firma XYZ, s. r. o., má v jednom meste dve prevádzky. Sú vzdialené asi 2 km. Našťastie zo strechy objektu A, v ktorom sídli jedna z prevádzok, vidieť strechu objektu B, teda sídla druhej prevádzky. Požiadavky sú jednoduché: treba sprístupniť používateľom v objekte B servery inštalované v objekte A.

□ Riešenie

Toto je priam ideálny prípad na vytvorenie mikrovlnného spoja. Približný rozpočet je v tab. 2.

Pokiaľ by však chcela firma ušetriť, tento spoj je možné vybudovať aj s podstatne nižšími nákladmi, a to s použitím dvoch linuxových PC smerovačov, do ktorých by sa inštalovali mikrovlnné adaptéry.

Pri rozpočtoch boli použité zariadenia WaveLAN spoločnosti Lucent Tech no logies (www.ies.sk/lucent).

Samozrejme, spôsobom, ktorými možno siete spájať, je veľmi veľa. Mohli by sme uviesť aktuálnu technológiu Point-to-Multipoint, ktorú prednedávnom spustila spoločnosť EuroTel, alebo využitie káblov káblových televízií na pripojenie na internet, alebo napríklad pokusy s využitím káblov na prenos elektrickej energie na prenos dát, no ako sme už spomínali, tento seriál sa venuje malým sieťam a spo miané technológie svojou finančnou náročnosťou presahujú rozpočty malých sietí.

Tab. 2

dva mikrovlnno-ethernetové mosty	170 000,- Sk bez DPH
dve externé 12 dB antény s príslušenstvom	35 000,- Sk bez DPH
dva PC smerovače (486, 16 MB RAM, 80 MB HDD)	14 000,- Sk bez DPH
dva mikrovlnné ISA adaptéry	44 000,- Sk bez DPH
dve externé 12 dB antény s príslušenstvom	35 000,- Sk bez DPH

11. časť: Problémy v počítačových sieťach

V záverečnej časti tohto seriálu sa budeme venovať chybám a problémom, s ktorými sa môžete stretnúť pri počítačových sieťach.

Problémy s kabeľmi

Problémy s kabeľmi a prenosovými médiami patria medzi najčastejšie ťažkosti v počítačových sieťach. Výhodou je, že sa im možno vyhnúť pri inštalácii kabeľmi. Na odstraňovanie takýchto chýb sa používajú špeciálne testovacie nástroje, schopné zmerať požadované vlastnosti trás, prípadne aj nájsť miesta, ktoré spôsobujú problémy. Najčastejšie poruchy sú: nesprávne zapojenie koaxiálnych konektorov, nesprávne konektory, fyzické porušenie káblov, nesprávna dĺžka segmentov kabeľmi a rušenie trás.

1. Nesprávne/chybné zapojenie konektorov

Tento typ chyby je asi najčastejší. Týka sa všetkých druhov kabeľmi, či už ide o koaxiálnu, alebo o štruktúrovanú kabeľmi, založenú na krútenej dvojlinke (ďalej len TP kabeľmi). Pri koaxiálnych káblach ide predovšetkým o skratovanie konektorov. Podstatne zložitejšie je to pri konektoroch po užívaných pri TP kabeľmi. Chybné zapojenie môže byť spôsobené prehádzaním vodičov, ne dokonalým zatlačením IDC kontaktov konektora, ne správnou polaritou párov ale bo napr. skratovaním vodičov.

Indikácia – pri zásadných chybách nesvietia LED diódy na zariadeniach, označujúce spojenie koncových bodov (tzv. LINK diódy). Ak ide o problém s nesprávnou polaritou, LINK diódy svietia. Na polaritu nie sú všetky zariadenia rovnako citlivé. Niektoré iba oznámia problém, ale pracujú spoľahlivo ďalej, iné prestanú pracovať úplne. Zaujímavým problémom je nesprávne zapojenie párov, ktoré sa prejavuje napríklad tým, že spojenie vypadáva alebo má problémy pri vyšších rýchlostiach: pri 10 Mb/s pracuje spoľahlivo, ale pri zvýšení rýchlosti na 100 Mb/s nastávajú problémy.

Riešenie – najčastejšie treba konektor znovu zapojiť. Pre istotu uvádzame náčrt správneho zapojenia konektora RJ-45, používaného pri TP kabeľmi.

2. Nesprávne konektory

Táto chyba vzniká najčastejšie z nevedomosti, no nie je výnimkou, že sa nesprávne konektory použijú preto, lebo sú „lacnejšie“ ako konektory, ktoré systém vyžaduje. Ko konektory sú pritom jedným z najdôležitejších prvkov, lebo napr. veľmi ovplyvňujú útlmové charakteristiky segmentu. Neraz sa stáva, že sa pri konektorovaní podcení význam týchto prvkov a použijú sa konektory s horšími parametrami, ako si vyžaduje kabeľmi, napr. sa použijú konektory kategórie 3 v kabeľmi kategórie 5 alebo sa pri horizontálnej kabeľmi s drôtenými vodičmi použijú konektory určené pre lankové vodiče.

Indikácia – zhoršené prenosové vlastnosti trasy spôsobujú výpadky pri vyšších prenosových rýchlostiach, prípadne príde k úplnému odpojeniu vodiča od konektora.

Riešenie – opäť pomôže iba ich výmena.

3. Porušenie káble

Fyzickým poškodením káblov sa najčastejšie poruší kontinuita vodičov alebo tienenia.

Indikácia 1 – pri poškodení kontinuity vodičov LINK diódy na koncových zariadeniach nesvietia, zariadenia nie sú schopné komunikovať.

Riešenie 1 – bohužiaľ, treba vymeniť celý kabeľ. Teoreticky sa dá uvažovať o odstránení poškodenej časti a vložení novej nepoškodenej časti. Pri menej náročných systémoch a aj pri koaxiálnych kabeľmi je to možné,

no toto riešenie, keďže sa pri ňom vkladajú do spojenia ďalšie konektory, zhoršuje celkové prenosové charakteristiky trasy, a preto pri profesionálnych systémoch sa odporúča vymeniť celú trasu. Samozrejme, vzhľadom na prácnosť výmeny takejto trasy je lepšie poškodeniam predchádzať tým, že sa káble uložia v listách alebo rúrkach.

Indikácia 2 – pri poškodení kontinuity tienenia môžu vzniknúť vplyvom rušenia, ktoré takto poškodené tienenie nedokáže izolovať, problémy pri vyšších prenosových rýchlostiach.

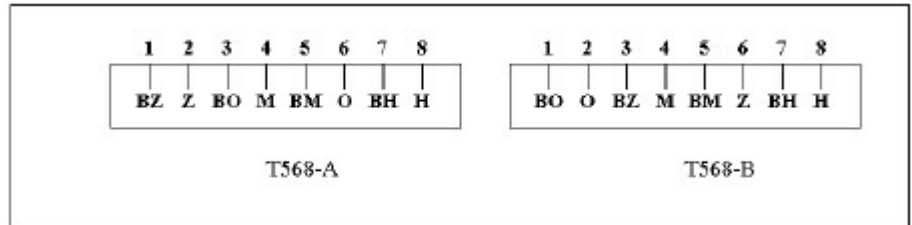
Riešenie 2 – toto nie je kritická chyba a možno ju riešiť bez výmeny celej trasy. Jednoducho stačí vhodným spôsobom tienenie zaceliť (napr. hliníkovou fóliou). Nie je to úplne profesionálne, ale bude to fungovať.

4. Dlhé segmenty

Tento problém je častý najmä pri koaxiálnych kabeľmi, ktoré boli v minulosti rozširované bez celkovej predstavy o tom, ako celá sieť vlastne vyzerá. Osobne som videl inštalácie s 10Base-2 segmentmi dlhými vyše 500 m napriek tomu, že norma hovorí o max. 182 m! Občas sa stáva, že aj pri štruktúrovaných kabeľmi sa dĺžka „prešvihne“, ale je to veľmi zriedkavý jav a je ho možné zistiť pri preberaní kabeľmi na základe vyhotovených protokolov.

Indikácia – pri štruktúrovaných kabeľmi vznikajú s takýmito segmentmi problémy najmä pri vyšších rýchlostiach, napr. 100 Mb/s. Ak sa táto chyba vyskytne pri koaxiálnej kabeľmi, jednou z jej indikácií je to, že vzdialení používateľia majú problémy s komunikáciou po sieti. Vcelku sa takáto sieť správa veľmi zle.

Riešenie – cieľom riešenia musí byť skrátenie segmentu. To sa najčastejšie realizuje vložением aktívneho zariadenia niekde doprostred problematickeho segmentu. Zvyčajne sa používa opakovač alebo hub. Namiesto opakovača je vhodné najmä pri sieťach s väčším počtom po užívateľov použiť radšej sieťový most, ktorý nielen



Zapojenie konektorov RJ-45 používaných v štruktúrovaných kabeľmi. K = odovodanie farieb vodičov je nasledovné: B - biela, Z - zelená, O - oranžová, M - modrá, H - hnedá

vyrieši problém s dlhým segmentom, ale aj rozdelí sieť na niekoľko kolíznych domén. Takisto je možné použiť iné prenosové médium (napr. namiesto UTP kábla sa použije optický kabeľ).

5. Rušenie

Rušenie prenášaného signálu je najzákernejšia chyba, pretože sa môže vyskytovať kedykoľvek a na ktoromkoľvek mieste kabeľmi. Pokiaľ toto rušenie nie je trvalé, ale iba občasné, veľmi ťažko sa odhaľuje zdroj rušenia. Rušenie vzniká tak, že signál prenášaný káblom interferuje (skladá sa) so signálom, ktorý je vysielaný zdrojom rušenia. Najčastejšími zdrojmi rušenia sú vedenia elektrického napätia 220 V, žiarivky, elektromotory, transformátory a pod.

Indikácia – problémy pri komunikácii po sieti, problémy pri vyšších rýchlostiach, zvýšený výskyt kolízií a pod.

Riešenie – neexistuje jednoznačné riešenie. Ro zumným opatrením je už pri inštalácii kabeľmi eliminovať možné vplyvy prostredia vhodným tienením či už celých trás za pomoci kovových alebo pokovovaných trás, po užitím tienenej kabeľmi, vhodným vedením káblov mi mo miest s možnosťou rušenia, dodržiavaním predpísaných minimálnych vzdialeností od zdrojov rušenia a pod. (tab.1).

Problémy s aktívnymi zariadeniami

Zaberať sa budeme iba základnými problémami, ako sú problémy so spojením, s prenosovou rýchlosťou a s duplexnou komunikáciou. Situáciu pri riešení spomínaných problémov uľahčuje fakt, že už takmer všetky zariadenia zapájané do počítačovej siete majú kontrolné LED diódy, pomocou ktorých sa dajú zistiť základné údaje o spojení: či existuje (LINK dióda), aká je jeho rýchlosť (10/100 dióda), či sa používa polovičný alebo úplný duplex a či zariadenie práve komunikuje (ACTIVITY dióda).

Indikácia 1 – zariadenie nemôže v sieti komunikovať.

Riešenie 1 – najčastejším problémom je, že zariadenie nemá so sieťou spojenie. Dôležitým ukazovateľom existencie spojenia na zariadeniach pripojených do počítačovej siete je LED dióda LINK. (Po známka: Je ne funkčná pri koaxiálnych kabeľmi.) Ak táto dióda nesvieti, pravdepodobne je poškodený kabeľ alebo kábel vôbec neexistuje. Skúste vymeniť všetky prepojovacie a pripojovacie káble, prípadne aj otestovať trasu meracím prístrojom.

Indikácia 2 – komunikácia je pomalá, prípadne vznikajú výpadky spojenia.

Riešenie 2 – v prípade, že nejde o poruchu kabeľmi, čo sa dá dokázať jej otestovaním, môže byť tento stav spôsobený nezhodou komunikačných parametrov, ako sú prenosová rýchlosť a typ duplexu. Sú známe prípady, keď sa zariadenia renomovaných výrobcov nevedeli automaticky dohodnúť na komunikačných parametroch a začali

pracovať správne, až keď sa im parametre nadefinovali ručne. Preto ak chcete skutočne spoľahlivé riešenie, nespoliehajte sa priveľmi na to, že sa zariadenia dohodnú. Ak vaše zariadenia nemajú možnosť manuálneho nastavenia (t. j. ušetrili ste na manažovacom module), stojte pred tvrdým orieškom. Zvyčajne sa takýto problém rieši tak, že strana, ktorá sa nastaviť dá, sa natvrdo prispôbi strane, ktorá sa nedá konfigurovať. Známe sú problémy so sieťovými kartami 3Com a ich pripojením na prepínače Cisco alebo Cabletron, prípadne problémy s 3Com OfficeConnect Swit chom a sieťovými kartami Intel Et herExpress.

Tab. 1
Vyhodenie káblov

	Prenášaný výkon po nn káblach		
	< 2 kVA	2 – 5 kVA	> 5 kVA
Netienený kabeľ UTP a neodtinený nn kabeľ	127 mm	305 mm	610 mm
Tienený kabeľ STP a neodtinený nn kabeľ	64 mm	152 mm	305 mm
Dátový kabeľ oddelený od nn kábla vodičovo priehradkou	-	76 mm	152 mm

Problémy s výkonom siete

Časté sú aj problémy s výkonom siete. Tie sú dost jednostranné: vždy je problém s malým výkonom siete. Riešenie je neraz komplikované a pri jeho hľadaní je potrebný špeciálny hardvér a softvér (paketové analyzátory, RMON sondy a pod.). My si spomenieme iba základné typy problémov s výkonom.

❑ Indikácia 1 – pri použití koaxiálnej kabeľáže alebo pri použití hubu je sieť pomalá a na opakovači alebo hube takmer vždy svieti LED dióda COLISION.

❑ Riešenie 1 – sieť je riešená ako jedna kolízna doména a pravdepodobne premávka na nej už dosahuje maximum. Toto môže byť spôsobené buď veľkým množstvom používateľov, alebo veľkými prenosmi na sieti (napr. kopírovanie veľkých súborov, generovanie veľkých zo stáv a pod.). Riešenie je relatívne jednoduché: sieť treba rozdeliť na viac kolíznych domén. Rozdelenie možno uskutočniť pomocou sieťových mostov alebo prepínačov.

❑ Indikácia 2 – napriek tomu, že je sieť rozdelená pomocou prepínačov na samostatné kolízne domény, jej výkon sa zdá používateľom nízky.

❑ Riešenie 2 – toto už nie je triviálna situácia, ale prvotné kroky sa dajú urobiť: Skontrolujte, či nie sú servery pripojené do siete pomalými trasami 10 Mb/s, prípadne ich, ak vám to, samozrejme, sieťové prvky dovoľia, nastavte natvrdo na 100 Mb/s a úplný duplex. Potom skúste nahradiť „utárané“ protokoly, ako NetBEUI a IPX, protokolom TCP/IP, lebo oba spomínané protokoly používajú v dost veľkom rozsahu všesmerové vysielanie (broadcasting), ktorým zaplavujú celú sieť.

❑ Indikácia 3 – niektoré počítače sú veľmi pomalé na priek tomu, že ich konfigurácia je dobrá.

❑ Riešenie 3 – pravdepodobne to bude mať „na svedomí“ už spomínaná autodetekcia parametrov prenosovej linky (autosensing). Skúste parametre nastaviť na pracovnej stanici aj na aktívnom prvku manuálne.

Vybrané problémy so softvérom

Úplne najzložitejšie sú ťažkosti týkajúce sa sieťových operačných systémov. Spome nieme niekoľko základných parametrov, ktoré ovplyvňujú ich výkonnosť vzhľadom na sieť.

Novell Netware

❑ Indikácia 1 – práca so súbormi, najmä ich otváranie je veľmi pomalé.

❑ Riešenie 1 – tento stav nastáva najmä po reštarte servera a je spôsobený ne správne nastaveným parametrom určujúcim počet Directory Cache Buffers. V tom prípade je dobré zistiť, ako vysoko sa tento parameter do stane bez nastavenia, a po tom nastaviť Minimum Directory Cache Buffers na toto číslo a Maximum Directory Cache Buffers na toto číslo + 500. Otváranie súborov po reštarte servera by sa malo výrazne urýchliť.

❑ Indikácia 2 – presun veľkých objemov dát na server je veľmi pomalý.

❑ Riešenie 2 – príčinou môže byť zle nastavený parameter určujúci maximálny počet súčasných zápisov na disk. Ak je ten to parameter prímalý, serveru rastie počet neobslužených požiadaviek a výsledkom môže byť až jeho úplné zahltenie. Parameter Maximum Concurrent Disk Writes sa dá pri diskoch UltraWide SCSI na staviť bez problémov na hodnotu 500 a pri použití diskového poľa na 700 a viac.

Windows NT

❑ Indikácia 1 – práca so súbormi po výmene Novell Netware za Windows NT je pomalá.

❑ Riešenie 1 – tak na toto si musíte začať zvykať. Istou nevýhodou Windows NT je, že prístup k jeho súborom je pomalší. Je to spôsobené tým, že Windows NT sa snaží byť všeobecnou serverovou platformou.

❑ Odporúčanie 1 – veľkosť virtuálnej pamäte na serveri Windows NT nastavte minimálne na odporúčanú veľkosť. Výrazne tým pomôžete celému systému.

Linux – Samba

❑ Indikácia 1 – práca so súbormi je po malá.

❑ Riešenie 1 – Samba nie je superrýchly súborový server, jej výkon sa dá azda porovnať s Windows NT, takže nečakajte zázraky. Dôležité je udržiavať množstvo súborov v jednom adresári na rozumnej úrovni – osvedčilo sa do 500 súborov. Rovnako je veľmi dôležité množstvo RAM v serveri. Pod 64 MB sa príliš neoplatí ísť, najmä ak vám tam beží ešte pár iných procesov.

Záver

Takže toto bola posledná časť nášho seriálu. Je dobré, ak bol pre vás čo len trošku užitočný. Ak nie, je to vaša chyba – mali ste sa ozvať ;-)). Prajem veľa úspešne nainštalovaných sietí.

■ Jozef Šovčík

