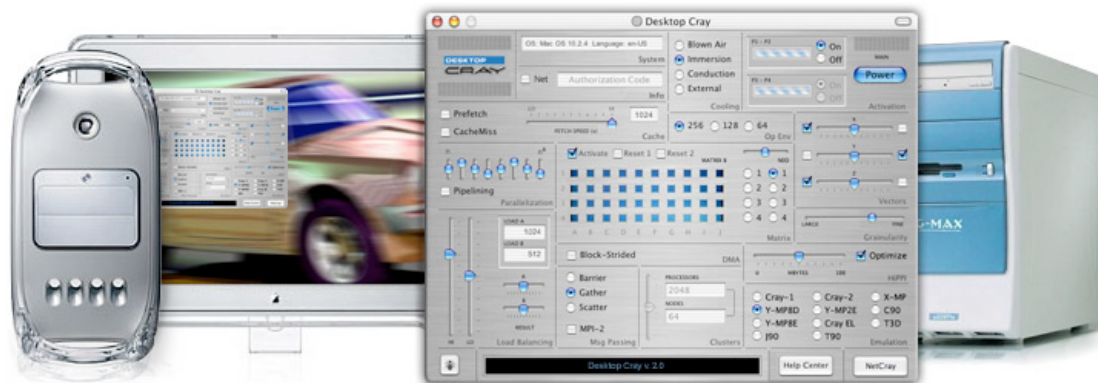


Serverování s Applem



Věnováno všem, které to zajímá

Obsah

Slavnostní bootstrap

Přehled typů

AppleTalk

LocalTalk

Ethernet

A/UX

Jak vznikl MacOS X a nový Mac

Síťování v MacOS X

Software pro Mac OS X

Klony Macintoshů

Software pro MacOS classic

Návrh sítě

Příklady sítí

Hacking

Slavnostní bootstrap

Nepotřebujeme pana Einsteina k tomu, abychom si všimli, že čas běží. Všechno na světě stárne, a co se starými věcmi? Většinou se zahazují nebo prodají. Tak se dnes DTP studia, firmy i jednotlivci zbavují strojů od firmy Apple.

Počítačů, které vlastně nedávno za obrovské peníze koupili, strojů, které ještě nedávno byly špičkou toho, co bylo možno mezi počítači nabídnout.

A zbavují se jich proto, že k nim nemohou připojit digitální fotoaparát přes USB či si na nich nezahrají nejnovější hru s nesmyslnými hardwarovými nároky, případně proto, že na zpracování efektu v Photoshopu musí čekat třicet sekund místo patnácti.

Počítače této firmy byly koncipovány tak, aby se daly zapojovat do sítí, a to včetně "osmibitu" Apple II GS. A tato schopnost je zajímavá i dnes. Teprve se sítí počítačů je možné dělat opravdu neuvěřelné věci, a nebo, jak to vyjádřila firma Sun, "sít' je počítač".

Dle mého názoru nabízí starší stroje Apple za málo peněz spoustu muziky.

Jsem přesvědčen, že Apple víc než jiní myslí na uživatele, a to i v oblastech administrace sítí, které jsme zvyklí přisuzovat pouze profesionálům.

Nevadí, že jde o starší stroje, vyřazené z firmy.

Nevadí, že na nich neběží nejnovější systém.

Jednoduchost a přívětivost je vlastnost všech těchto počítačů. Přímo součástí operačního systému je celá řada potřebných nástrojů a jiné se nabízejí zdarma. Jejich společným jmenovatelem je vysoká spolehlivost a většinou přehledné a snadné ovládání.

To, co u Applu najdete jako standardní vybavení, bývá jinde už považováno za nadstandard.

Informace, které tu uvedu, budou určeny především uživatelům klasického Mac OS 6 až 9. Nový, UNiXový OS X, vyžadující procesory G3 a vyšší, se starých počítačů Macintosh příliš netýká, je tedy zmíněn jen okrajově.

Předem upozorňuji, že Macintosh a Mac jsou dnes vlastně dva různé druhy počítačů, označení Macintosh bylo oficiálním označením do roku 1998, od roku 1998, po výrazné změně hardwarové architektury i operačního systému, se oficiálně užívá dřívější neoficiální zkrácené označení Mac.

Všimli jste si toho někdy?

Přehled typů

Nejstarší **68000 Macintoshe** jsou vhodné nanejvýš jako terminály, především textové, v omezené míře i jako fileservery. Záleží na tom, jak vysokou verzi systému se na daném stroji podaří zprovoznit, většinou ale nebude nároky aplikačního software splňovat.

Z hardwarového hlediska je zajímavé, že první Macintoshe neměly sběrnici ADB (*klávesnice a myš byla připojována jinak*), neobsahovaly SCSI (*to až Macintosh plus*) ani rozšiřovací sloty (*to až Macintosh SE*).

Názvem, ale nikoliv architekturou a typem procesoru, do této řady patří SE/30 (*odvozen od IIx*), Classic II, Color Classic a Color Classic II (*odvozené od řady LC*).



Stroje s procesory 68020 a 68030, většinou označované jako řada **Macintosh II** (*patří sem ale i některé LC stroje a jejich odvozeniny*), se dají, kromě funkce textového terminálu či fileserveru, použít i jako X Window terminály.

Protože zejména LC stroje mívají omezenou paměť, nebývají moc vhodné pro provoz WWW browseru, nejvhodnější není ani použití procesoru 68020 na nižší taktovací frekvenci. Relativně dlouho pak trvá příprava stránky pro zobrazení a manipulace s grafikou.

Silnější stroje s procesorem 68030 a větší pamětí už dosahují při použití vhodného browseru přijatelných výsledků.

Taktovací frekvence nad 25 MHz je výhodou.

Podle rychlosti konkrétního počítače mohou hostovat servery typu FTP nebo Gopher, případně provozovat BBS, stroje s procesory 68030 mohou hostovat i WWW, pokud postačí 2 Mbit připojení do sítě.

WWW je oproti třeba FTP náročnější v tom, že v rámci jedné WWW stránky je třeba načíst, překódovat a poslat větší počet souborů, jako je případná grafika a podobně, zvětšení dostupné paměti, pokud je možné, výrazně zrychlí práci.

Serverové aplikace většinou nevyžadují přítomnost FPU.

Na typu počítače závisí možný použitelný systém, většinou na strojích s procesory 68020 běží OS 7.5.3 či 7.5.5, na strojích s procesory 68030 OS 7.6.1. Na některé z těchto strojů je možné nainstalovat i A/UX.



Nové označování, které se týká, jak už jsme si všimli, i strojů s procesory 68020 a 68030, přineslo názvy LC (*lowcost color*) pro nejlevnější řadu počítačů (*osazených procesory 68030 nebo 68040*), Performa pro spotřebitelskou řadu (*často osazovanou "odlehčenou" verzí procesoru 68LC040 bez FPU, bohužel s chybami v některých málo používaných instrukcích, později procesory PowerPC nižších řad*), Quadra (*pro počítače vyšší třídy s plnou verzí procesoru 68040*) a Centris (*střední kategorie*).

Počítače s procesory 68040 se dělí zhruba na Performy (*s 68LC040, tato spotřebitelská řada ale nesla i jiné procesory*) a Quadry (*s plnou verzí procesoru 68040 vybavenou FPU*), patří sem i řada Centris.

Většina softwaru na nich funguje bezproblémově včetně WWW browserů, rychlost je uspokojivá. Limitující faktory se tak přesouvají na rychlost síťového připojení (*2 Mbit Ethernet*) a rychlost komunikace se SCSI disky.

Některé stroje (*580, 630*), obsahují sběrnici IDE, která umožňuje instalovat do nich běžně dostupné IDE disky velkých kapacit.

Quadra 950 má oproti tomu dvě SCSI sběrnice, Mac OS ovšem pracuje jen s disky na jedné sběrnici (*označuje disky pozicí na sběrnici, ne ale číslem sběrnice*) a je potřeba použít specializovaný software nebo UNiXový operační systém A/UX.

Na stroje s procesorem 68040 a 68LC040 jde instalovat Mac OS 8.1, s výjimkou některých (*Perforem*) pak i A/UX, případně BSD 68k nebo Linux mk68.



Macintoshe s klasickou architekturou, vybavené procesory **PowerPC**, se dělí na výkonnější řadu PowerMacintosh a spotřebitelskou řadu Performa.

Hardwarová vybavenost těchto strojů je poměrně pestrá, některé mají současně se sběrnici SCSI i diskovou sběrnici IDE, umožňující připojit běžné IDE disky a levně tak získat dostatečně velkou diskovou kapacitu.

Ethernetové přípojky těchto strojů většinou běhají na 10 Mbit a jsou tak použitelné i tam, kde je kladen požadavek na vyšší přenosové rychlosti.

Kompatibilita se starším software je velmi vysoká, jen zanedbatelné procento programů na PowerPC procesorech neběží. Naopak se nabízí používat software, které existuje jenom pro PowerPC stroje,

škoda je, že nelze použít A/UX a v případě instalace UNiXu je třeba sáhnout po BSD PPC nebo použít Linux.

Na počítačích s procesory 60x lze instalovat maximálně Mac OS 9.1.

Problematické jsou klony od firem Motorola, PowerComputing a UMAX, které se instalací systému vyššího jak 8.1 brání, je ovšem možné nainstalovat systém vhodným způsobem na jiném podobném počítači, klony jsou pak schopné takto instalovaný systém nabootovat (8.1 se však zdá stabilnější).

Běžové PowerMacintoshe G3, desktop a tower, jsou už schopny provozu systému 9.2 nebo Mac OS X.



Macy "nového světa", stroje s novou architekturou ATA/USB/FireWire, se dělí na výkonnější řadu PowerMac a spotřebitelskou řadu iMac/eMac (řada eMac vznikla v době, kdy řada iMac přestala používat CRT monitory a byla osazována LCD displayi; eMac je v podstatě stejný, jako iMac, jeho cena je ovšem nižší díky použití CRT monitoru, který je levnější, než LCD).

Jejich síťové karty jsou 100 Mbit, u nejnovějších potom i 1 Gbit (tuto rychlost ovšem využijete spíš v lokální síti, i rychlé linky pro připojení do internetu běžně nedosahují 10 Mbps).

Většina strojů je připravena na bezdrátové WiFi síťování pod názvem AirPort (IEEE 802.11b) nebo AirPort Extreme (IEEE 802.11g s vyšší rychlostí). Základem AirPort jsou PC karty (PCMCIA) pro WiFi, použitelné i v notebookech staré architektury, a AirPort Base Station (zastupitelná WiFi vysílači jiných výrobců) s dosahem 50-150 metrů podle typu, zprostředkávající funkce routeru a gatewaye na telefonní či Ethernetové síťové připojení (nejstarší verze má jedinou Ethernet přípojku a kapacitu 10 uživatelů, ostatní mají Ethernety dva a kapacitu 50 uživatelů).

Je možné používat disková pole a RAID připojované přes USB či FireWire, rozšiřitelné PowerMacy umožňují připojit další hardware přes rozšiřující sběrnici PCI.

Zvláštním případem jsou pak specializované servery X Serve, určené k montáži do racků a sdružování do uzlů.

Na těchto strojích lze provozovat Mac OS 9.2 nebo Mac OS X (či jen jeho jádro Darwin, případně doplněné některým window managerem) a pochopitelně Linux.



Klony Macintoshů

Originální stroje Apple nabízejí výběr z poměrně široké škály různých verzí Mac OS či Mac OS X, nepočítaje v to nejrůznější distribuce Linuxu, Darwin či BSD.

Bohužel, klony (*Motorola, Power Computing, UMAX*) nemají tak dobře provedenou identifikaci stroje, takže na nich lze často instalovat nejvyšš OS 8.1 a vyšší verze na ně dostanete jenom složitým trikem, jinak se hlásí jako nepodporované počítače.

U serveru to příliš nevadí, pro někoho bude ale těžké pochopit, proč na svém PowerPC dělu máme starší systém, když by tam mohlo být něco jiného, a tomu, že od staršího systému dostaneme vyšší výkon, většinou nebude rozumět (*běžní PeCaři si prostě neuvědomují, že na Pentiu 500 MHz jim Windows 3.1 pojedou jako totální drak, zatímco Windows XP jako podprůměrný šnek*).

Zrada je také v tom, že počítačů Apple si na burzách a v bazarech (*či odložených u popelnic, ano*) snadno všimnete a zachráníte je, ale klony často vypadají jako obyčejné PeCe v levných plastických kastlích, takže je lze snadno přehlédnout.



AppleTalk

Kromě případné implementace UNiXových síťových protokolů TP/IP mají počítače Apple zabudovanu především podporu vlastního protokolu AppleTalk.

Systém tvorby adres není totožný s IP adresami. Adresa v síti AppleTalk se skládá z dvoubajtového čísla sítě (network), jednobajtového čísla uzlu (node) a jednobajtového čísla zásuvky (socket).

Číslo sítě se pohybuje od 1 do 65535, ovšem rozsah 255.0 až 255.254 (65280 až 65534) se nepoužívá – slouží pro přihlašování do sítě po dobu, než počítač dostane přiděleno skutečné číslo sítě, do které patří. Síť se myslí řada počítačů na společném kabelu spravovaná jedním routerem, přidělování skutečného čísla sítě a jména zóny provádí router, je-li dostupný.

Sítě je možné spojovat do zón, kterých může být na jednom kabelu 255 a označují se jmény, jedna zóna je defaultní (*). Počítač na síti s více zónami může patřit do libovolné dosažitelné zóny.

Každý z počítačů je uzlem a má vlastní číslo, teoreticky může být v jedné síti 254 počítačů. Procesy a programy, které chtějí komunikovat přes síť, si na svém počítači (nodu) otevrou zásuvku, opět rozlišenou číslem, které procesu přiděluje systém.

Je-li tedy adresa 73.194/250/129, značí to, že proces, očekávající síťové spojení na zásuvce (socketu) 129 běží na uzlu (nodu) 250 v síti 73.194.

Uživatel se ovšem s tímto adresováním nesetká. Systém adresy překládá a uživateli nabízí jmenné adresy s názvy zón, dostupné přes NBP (*name binding protocol*). Místo 73.194/250/129 bude objekt označen jako Gutenberg:LaserWriter@univ-Melbourne. Gutenberg je jméno objektu a LaserWriter typ, jde tedy o tiskárnu jménem Gutenberg, univ-Melbourne je jméno zóny. Každá část síťového jména může být dlouhá 32 znaků (standardní délka jména na starších verzích operačního systému MacOS).

LocalTalk

První možností, jak počítače fyzicky propojit, fungující i u velmi starých Macintoshů, je přímé propojení sériovým kabelem, nejlépe mezi dvěma modemovými porty. Jsou sice zhruba stejné jako tiskárenské porty, ale mají vyšší prioritu, což je při komunikaci důležité, zatímco tiskárna si na data počkat může. Navíc si mnemotechnicky lépe zapamatujete, kam máte co připojeno, provozujete-li spolu se síťovým propojením i tiskárnu.

Pouhé dva počítače propojíte kabelem podobným, jako se používá k připojení tiskárny a jiných periférií. Můžete použít i tiskárenský kabel, zapojení je stejné, specializovaný LocalTalkový kabel bývá delší a má silnější stínění.



Více počítačů a periférie, které se s nimi po LocalTalku baví, se dají spojit do "PhoneNetové" sítě pomocí PhoneNetových krabiček (*stále se dají koupit i v našich obchodech*).

Princip je stejný jako při použití kabelu s osmikolík miniDIN na obou koncích, jen v tomto případě připojíte k počítači kratičkový kabel s jediným osmikolíkem miniDIN, zakončený na druhé straně krabičkou s nápisem PhoneNet a dvěma "telefonními" konektory RJ. Je to vlastně rozvojka sériového kabelu, můžete se připojit ke dvěma počítačům a každý z nich pak zase k dalšímu počítači. Propojení přes PhoneNetové krabičky dovoluje i vypnout libovolné počítače, aniž by to znamenalo ztrátu spojení pro počítače, mezi kterými vypnutý stroj leží (*nesmíte ale rozpojit kabely, které vedou od jedné krabičky ke druhé*).

PhoneNet je prostě skutečnou vstupenkou do světa sítí.

Softwarová obsluha je jednoduchá:

Pro sdílení disků stačí nastavit v ovládacím panelu AppleTalk použití modemové zásuvky, v programu Připojení (Chooser) pak můžete případně tiskárně přisoudit tiskárenskou zásuvku a v možnostech AppleShare si zvolíte počítač a jeho disky, které si přejete přes síť připojit. A pak s nimi pracujete stejně, jako kdyby se nacházely lokálně na vašem počítači.

V ovládacím panelu Sdílení souborů (File sharing) můžete zapnout sdílení vlastních disků nebo adresářů. Vzhledem k tomu, že existuje, podobně, jako v UNiXu, možnost definovat uživatele a skupiny uživatelů, chránit se hesly, posle nastavení ve Finderu pak sdílet jen určité oblasti disků a nastavovat uživatelská práva (*pravda, mnohem jednodušeji a přehledněji než v UNiXu*), nemusíte se strachovat o to, že se k citlivým datům dostane někdo nepovolaný, ani se starat o pracnou distribuci hesel k datům, která chcete mít veřejně přístupná.

Komunikace se ale neomezuje jen na protokol AppleShare, je například možné mít na jednom stroji spuštěnou BBS a z druhého se na ni přes některý z terminálových programů připojit. Přes ovládací panel MacTCP (*nebo volbou MacIP v ovládacím panelu TCP/IP*) lze do AppleTalku enkapsulovat i TCP/IP a přes gateway (*počítač, připojený přes modem nebo pevnou linku k internetu, vybavený příslušným softwarem*) se dostat na internet i z ostatních počítačů, či se přímo přes modem (*třeba*

pomocí FreePPP) připojit k některému z poskytovatelů internetového připojení, případně komunikovat pomocí TCP/IP mezi jednotlivými počítači v LocalTalkové síti a využívat TCP/IP služeb (*Finger, Gopher, NTP, FTP, Telnet, WWW, ...*).

Apple navíc měla vlastní řešení připojení k poskytovateli internetového připojení (ISP), které je rovněž přímo součástí systému, nazvané ARA (Apple Remote Access).

Jednu nevýhodu LocalTalk má, a tou je relativně pomalá komunikace v lokální síti. Ve své době se jednalo o rychlou komunikaci, datový tok byl srovnatelný s přímým přístupem na disketu (*první Macintosh ani jiná disková média neměly*), uživatelé tedy mohli být jedno, zda přistupuje na síťový disk na serveru či na svou vlastní disketu, rychlost byla stejná. Postupně však začali uživatelé požadovat něco rychlejšího.

Pokud se ovšem připojujete k Internetu do rychlosti 512 kbps, LocalTalk vás zpomalovat nebude.

Postavit síť (nebo část sítě) na LocalTalku má význam tehdy, pokud

- chcete akutně a dočasně propojit dva počítače mezi sebou
- chcete do sítě zahrnout "osmibit" Apple IIGS, který jiné možnosti komunikace nemá
- rychlost vašeho připojení k Internetu výrazně rychlost komunikace po LocalTalku nepřevyšuje
- chcete připojit do sítě či k internetu jiný velmi starý počítač nebo počítač, který nemá Ethernet (*či se stane, že váš počítač má dnes nestandardní výstup AAUI-15 a vy nemáte redukci, která je mimochodem velice drahá*)

Pokud do sítě připojujete starší pomalý stroj, uvědomte si, že LocalTalk byl na svou dobu opravdu rychlým způsobem komunikace (*necelý megabit za sekundu*). Dvoumegabitový Ethernet, který je na většině starších Macintoshů k dispozici, je jenom asi třikrát rychlejší. Podle dokumentace Apple je LocalTalk dostačující dokonce i na provoz internetového serveru.

Pokud nebudete takto připojený stroj používat na přenosy velkých objemů, nemusíte se snížením výkonu sítě (připojení k Internetu) vůbec obávat. Rychlost LocalTalku i starých strojů postačí k provozování Telnet serveru (chat, síťové hry, ...), BBS, Gopher serveru a dalších méně frekventovaných služeb jako Finger, Whois či NTP.

Za jistých okolností je možné použít tento typ připojení i pro WWW a FTP, pokud nabízejí spíše kratší soubory než velké objemy dat (stahovat na necelém megabitu DivX filmy nebude to pravé).

Ethernet

Jak už bylo naznačeno, nižší rychlost sériového přenosu se kompenzovala převedením AppleTalkového protokolu na jiný druh kabelu, který technicky umožňoval vyšší přenosové rychlosti, a to TokenRing (TokenTalk) a Ethernet (EtherTalk). TokenRing je řešení zastaralé a pomalejší než běžněji užívaný Ethernet, a firma Apple do svých počítačů zabudovávala standardně právě Ethernet.

Máte-li počítač vybaven Ethernetovou kartou a příslušným softwarovým vybavením, zjistíte, že ovládání je podobné LocalTalku.

V ovládacím panelu AppleTalk zvolíte Ethernet, s ostatními ovládacími panely a Připojením (Chooserem) se pracuje stejně, jako při použití LocalTalku, takže za pár okamžiků si můžete přes EtherTalk připojit nějaký vzdálený disk nebo nechat sdílet ten svůj. Můžete nastavit svou IP adresu (v ovládacím panelu *MacTCP* nebo, pokud máte instalován *OpenTransport*, v panelu *TCP/IP*) nebo aspoň způsob jejího přidělování, a pracovat pak se službami, používajícími TCP/IP protokol.

Všimněte si, že AppleTalk a TCP/IP se nastavují zvlášť, je tedy například možné nasměrovat AppleTalk na sériák a TCP/IP na Ethernet.

Výhodou proti LocalTalku je možnost přímého připojení do heterogenní TCP/IP sítě nebo třeba k UNiXovému počítači (*ačkoliv některé takové stroje, třeba Atari TT či Silicon Indy, bývají vybaveny i osmikolíkovou miniDIN zásuvkou pro LocalTalk*) nebo k PeCi.

Existují ovšem utility, implementující na UNiXu AppleTalk, takže i bez použití TCP/IP na klientech může UNiXový stroj sloužit jako fileservr nebo tiskárenský server.

Od MacOS 8 výše je dokonce webový server spolu s dalšími utilitami přímo součástí systému a i AppleShare umožňuje připojení TCP/IP klientů.

Co se týče rychlosti, Ethernetové karty zabudovávané do prvních 68k Macintoshů jsou omezeny rychlostí sběrnice na asi 2 Mbit/s, pozdější stroje s PowerPC procesory už mají plnohodnotné 10Mbit/s připojení. Nové stroje Mac mají 100 Mbit/s, ty nejnovější dokonce 1 Gbit/s.



A/UX

Vraťme se teď k Macintoshům s procesory 68k.

Jako servery do sítí dodávala firma Apple silné stroje s mnoha diskovými pozicemi a sloty na streamerové kazety, vybavované navíc akceleračními kartami (*urychlujícími grafiku a komunikaci s disky*), označované jako Workgroup Server.

Jako operační systém na nich byl ve valné většině případů dodáván standardní MacOS, doplněný o zálohovací software a podobné utility.

Výjimkou se stal Apple Workgroup Server 95, jehož hardwarovým základem byla akcelerovaná Quadra 950. Firma Apple totiž tou dobou měla připravený vlastní UNiX, označovaný zkratkou A/UX, který se stal základem softwarového řešení Workgroup Serveru 95.

Jednalo se o standardní UNiX, odvozený z distribuce BSD 4.3 (*kteřá tehdy byla lepší, než UNiX System V od AT&T*) pro procesory 68k. Vedle možnosti spouštět ho v textovém režimu nebo v grafické session s okenním manažerem twm existovala i možnost použít jako grafické prostředí normální Finder (*standardní 32 bitový nebo 24 bitový, kompatibilní s dnes již prehistorickými aplikacemi pro nejstarší modely Macintoshů*).

Toto provázání nejenom že poskytuje důvěrně známý vzhled a ovládání, ale UNiX je s upraveným Systémem 7.0.1 tak provázán, že lze spouštět běžné programy pro MacOS, a to na Macintosháckých i UNiXových discích, oba formáty lze sdílet přes AppleShare i jinak (FTP, TFTP, UUCP, ...), ve Finderu jdou kromě přístupových práv pro AppleShare nastavovat i přístupová práva UNiXová, součástí systému jsou konzola a terminály, na pozadí běží UNiXové démoni...

Je to prostě ušlechtilý kříženec MacOSu a UNiXu, je víceuživatelský (*lze se k němu vzdáleně připojovat*), snadno ovladatelný a hlavně výkonný (*firemní prameny uvádí, že pod A/UX běží sdílení až 10x rychleji, než pod MacOS*).

Kromě twm k A/UX firma Apple dodávala X11 server MacX, který jen umocňuje celkový dojem, po připojení k A/UX stroji z jiného Macintoshe, vybaveného MacX, můžete využívat UNiXové X Window aplikace přímo na svém stroji s normálním Macintosháckým vzhledem.

Ze shellu, který se tváří jako Macintoshácká aplikace, máte kontrolu nad UNiXovou částí, ve skutečnosti však běží MacOS tak trochu "jakoby pod UNiXem". Shell a celý UNiX je z pohledu Finderu aplikace, která zabere svou část celkového strojového času, zbytek se dělí mezi ostatní aplikace běžící pod MacOS.

Distribuce Workgroup Server 95 není vázána jen na Quadru 950, naopak ze všech verzí A/UX je spustitelná na nejširší paletě strojů s procesory 68030 a 68040.

Pokud se chcete seznámit s UNiXem, vyzkoušet jeho možnosti, nebo využít provázanosti s prostředím MacOS, je A/UX asi to nejlepší, co pro tyto starší počítače existuje, především značně usnadňuje ovládání systému.

Z vlastní zkušenosti můžu říct, že na něm lze provozovat současně UNiXové programy (*FTP, SMTP, vzdálené přihlašování, X Window aplikace*) spolu s Macintosháckými (*dokonce třeba i WWW server pro MacOS*) naprosto bez kolizí.

S ukončením podpory procesorů 68k a s přechodem na procesory PowerPC byl A/UX opuštěn a pro další řešení Workgroup Server byl dodáván opět MacOS (*doplňovaný o software typu AppleShare IP či Apple Internet Server Solution*).

Apple sice přišla s profesionálními superservery (*Network Server 500 a Network Server 700*), které byly vybaveny UNiXem, tentokrát to byl čistý AIX od firmy IBM (*používaný v serverech IBM, které mají stejné PowerPC procesory, jako Apple*), ale zájem o Network Servery byl malý.

Nicméně dnes by bylo velmi zajímavé je někde potkat.

Jak vznikl MacOS X a nový Mac

Ještě dávno předtím, než se Apple začala zabývat A/UX, představil Steve Jobs po svém odchodu z Apple vlastní platformu NeXT s operačním systémem NextStep, založeným právě na UNiXu, opět upraveném tak, aby byl snadno a jednoduše ovladatelný.

Nepochybně se to povedlo.

Vznikl tak jednoduchý, ale mocný okenní manažer WindowMaker, který při práci na lokálním monitoru nepoužíval protokol X11, ale PostScript, stejný, jaký se potom posílal na laserovou tiskárnu. Tím bylo dosaženo skutečného WYSIWYG režimu.

Stroje NeXT jsou pro historii sítí důležité nejen tím, že tady si Steve Jobs a jeho technici vyzkoušeli návrh UNiXového systému, ale také tím, že právě jednoduché ovládání a velké síťové možnosti těchto strojů umožnily vznik prvního WWW serveru a WWW browseru.



V době, kdy Applu hrozil krach a zánik, Steve Jobs se do firmy vrátil, a s ním i jeho technici z firmy NeXT.

Musíme si připomenout, že firma Apple vznikla původně pro nadšence a kutily, kterým dodávala levné počítačové systémy (Apple I a Apple II), a ač bývala technicky vždy na výši, mívala v nabídce počítače na úrovni za přijatelnou cenu. I samotné uvedení Macintoshe bylo pokusem přinést grafické okenní prostředí z Lisu, určené pro bohaté velké firmy, i normálním lidem, včetně těch, co by se jiného počítače báli.

Po Jobsově odchodu se ale začala stále více věnovat "velkému obchodu" a "významným zákazníkům", z jejích počítačů se stále více stávají obrovská monstra v maxitowerech s nadupanými parametry, a to, jak ukazuje příklad Network Serverů, bez výrazného finančního úspěchu.

Snaha inspirovat se světem PeCí a rozprodávat licence na stavbu klonů se ukázala být nesmyslná. Ve světě PeCí dominuje Microsoft, což není dodavatel počítačů, ale softwaru, Apple by se tedy musela stát monopolní softwarovou firmou.

"Mateřská" firma PeCe, IBM, na licenční výrobě na Tchajwanu naopak trátí, její pokusy o comeback s modely PS/2 a podobnými byly neúspěšné. A do podobné situace se tehdy Apple řítit.

Jobs po svém návratu zastavil vše, na čem se tehdy pracovalo, mimo jiné i PDA Newton, což mu mnozí nemohou dodnes zapomenout (*firma Palm, se kterou Apple na Newtonu spolupracovala, se osamostatnila a vydala vlastní řešení PDA*), a všechny síly soustředil na uvedení Macu – nové platformy s novým operačním systémem, zrozeným ze zkušeností s MacOSEm a NextStepem.

Jobs zahodil SCSI a začal používat ATA (později SATA).

Zahodil ADB a začal používat USB, a to i pro připojení klávesnice a myši.

Opustil sériové zásuvky, zavedl FireWire a stomegabitový Ethernet.

A hlavně slavnostně pohřbil dosavadní MacOS a uvedl nový, založený stejně jako NextStep na mikrokernelu Mach a BSD UNiXu (*jádro systému je dokonce volně šiřitelné a OpenSource*), jen místo PostScriptu použil pro kreslení oken na obrazovce o generaci lepší technologii PDF a pro volání služeb zase API podobné tomu z původního MacOSu (Carbon) a nové objektové rozhraní (Cocoa).

Jednoduchý okenní manažer NextStepu, WindowMaker, byl opuštěn a pro Mac bylo vytvořeno nové grafické prostředí Aqua, zajímavá byla i dohoda s Microsoftem, která zajistila pro první léta existence nového systému potřebný software – Internet Explorer a Microsoft Office.

Síťování v MacOS X

Protože všechny modely nových Maců (a iBooků) mají standardně stomegabitový Ethernet, případně modem nebo možnost připojit PCMCIA WiFi kartu, zvanou AirPort, a protože Apple dodává základnové WiFi/Ethernet/modem stanice s funkcemi routeru a gatewaye, je síťování v takovém prostředí radost sama.

K dispozici jsou všechny standardní UNiXové programy a utility (FTP, NFS, cgi a perl skripty, PHP, webový server Apache přímo jako součást systému). Navíc se příslušná nastavení provádějí přímo v grafickém prostředí Mac OS X (tak se nový operační systém jmenuje), takže je všechno dokonale jednoduché.

Bez velkých úprav lze takové stroje používat jako servery, serverová řešení Applu spočívají spíše v instalaci více než jedné Ethernetové karty, připojení diskových polí a hlavně v distribuci Mac OS X Server - jde o multiuživatelskou licenci obohacenou o síťové utility pro zálohování, vzdálený přístup k pracovní ploše pod názvem Apple Remote Desktop (od verze ARD 2 obsahuje i vlastní VNC server, takže je s VNC kompatibilní), a sdílení výpočetní kapacity nevytížených počítačů v rámci sítě pomocí XGrid.

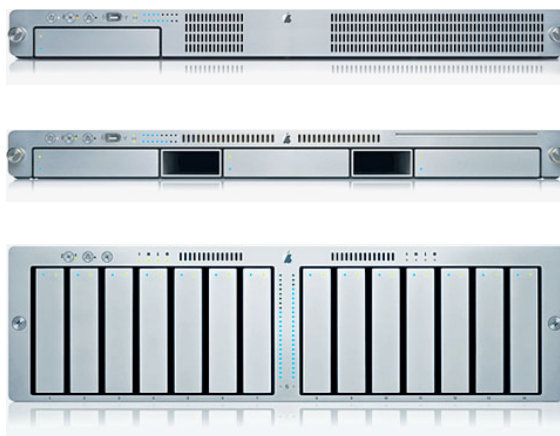
Přestože se Apple profiluje spíše jako výrobce spotřební elektroniky (*a Steve Jobs ví proč, superserverů se nikdy neprodá tolik, jako stolních počítačů, ještě lépe jdou na odbyt notebooky, nejvíc se ovšem prodá harddiskových MP3 přehrávačů iPod*), objevilo se v jeho nabídce i komplexní serverové řešení zvané X Serve.

Jde o rackovou stavebnici, sestávající z jednotlivých serverů X Serve (*vysokých jednu jedinou rackovou pozici*), přídatných diskových polí a uzlů X Serve Cluster Node, které propojují několik X Serve serverů do jednoho výpočetního clusteru. Jako software se dodává Mac OS X Server, případně lze využít jinou UNiXovou nebo Linuxovou distribuci pro procesory PowerPC (*Darwin či Yellow Dog Linux*).

Koneckonců doba, kdy je všechno ve firmě Apple postavené na jejích vlastních počítačích, se zas vrátila.

O možnostech hardwaru Apple a Mac OS X vypovídá i to, že velký superpočítač (simulátor globálních atmosférických jevů a celoplanetárního počasí) byl vyroben prostým propojením několika set obyčejných PowerMaců obyčejnou Ethernetovou sítí, a sedmý nejvýkonnější superpočítač světa tvoří 1100 dvouprocesorových XServe G5 (<http://www.tcf.vt.edu/systemX.html>).

To je srovnatelné jedině s příhodou, kdy Apple zakoupil superpočítač CRAY pro simulaci nově vyvíjených počítačů. Vyšlo najevo, že Cray naopak pro simulaci staršího počítače CRAY-3 používá počítač od Applu!



Software pro Mac OS X

Na MacOS X je možnost vybrat si mezi různými programy, ale Apple většinu aplikací dodává přímo se systémem a většinou není důvod místo nich používat nějaké jiné.

Takto je k dispozici e-mailový klient **Mail**, SMTP server je součástí UNiXového jádra (**smtp**, **Postfix**), jako browser je přiloženo **Safari**, odvozené od KHTML (Konqueroru) nebo **Camino**, odvozené od Mozilly, a jako webserver UNiXový **Apache**, jako SQL server potom **MySQL**, balík programovacích jazyků včetně **PHP**. Protože jde většinou o UNiXové aplikace, a komunikace s nimi probíhá z větší části na úrovni příkazové řádky (Apple poskytuje vlastní uživatelské rozhraní jen pro základní funkce, jako je spuštění Apache, nebo v rámci správcovských nástrojů v rámci Mac OS X Server), vzniklo několik utilit, které tvoří frontend k těmto UNiXovým programům (**PureFTPd Manager**, **Postfix enabler**, **RapidoSMTP**) nebo doplňují jejich funkci (**Apache protect**).

X11 jako systémová utilita poslouží nejen jako terminál, ale i při spuštění X Window aplikací na vlastním počítači, FTP server (**ftpd**) a další služby jsou součástí UNiXu. Standardní videokonferenční program je **iChat**.

Spolu s tím se dodává kancelářský balík AppleWorks, prezentační program KeyNote a DTP program Pages, balík systémových služeb iMac a multimediální balík iLife, zahrnující iTunes, iPhoto, iMovie, iDVD, iWeb a GarageBand.

A to všechno je opravdu přímo součástí systému, který dostanete s počítačem (včetně instalačních CD, tohle není jako OEM Windows od Microsoftu) nebo si ho za necelých 5 000 korun koupíte. Windows za podobnou cenu dostanete tak akorát v nějaké ořezané verzi Home a navíc obsahují úplný prd.

Součástí systému Mac OS X ovšem není třeba populární Microsoft Office nebo programy od Adobe, taky si je musíte dokoupit zvlášť.

Nabídka programů pro OS X se utěšeně rozrůstá i proto, že kromě aplikací komerčních vzniká spousta freeware a OpenSource projektů, navíc je možné portovat programy z Linuxu, který se OpenSource programy jen hemží, a jiných UNiXů.

Na druhou stranu, programy pro klasický MacOS, jakožto "mrtvou platformu", byly firmami většinou uvolněny. Tento osud potkal i takové aplikace, jako Corel WordPerfect, uvolněn byl i MI/X, jehož PC verze je dodnes prodávanou komerční aplikací. Bohužel, časem tyto uvolněné staré programy z firemních webů zmizely, velmi obtížné je třeba sehnat Symantec Think C, které bylo před lety na firemním webu volně k dispozici.

Často se i pro klasický MacOS nabízí slušná šíře výběru softwaru, takže je možné se například rozhodovat, zda použít integrované řešení jako je NetPrensz, nebo mít raději FTP i WWW server jako dva oddělené programy.

I dostupnost potřebného softwaru spolu s dalšími otázkami, týkajícími se použitého softwaru, je faktor, který je nutno při výběru vhodného serveru a rozvržení sítě brát v potaz.



Návrh sítě

Při stavbě sítě je potřeba si především uvědomit, co na ní budete provozovat.

Ne ani tak co byste na ní provozovat chtěli, ale to, co na ní nejspíš opravdu provozovat budete.

Dále zvažte, jak a zda ji budete připojovat k vnějšmu světu.

Vycházejte z toho, co máte k dispozici, tedy jaké počítače, jak velké disky a jaký typ připojení k vnějšku, co můžete snadno ke stávající sestavě doplnit nebo co je pro vás naopak nedostupné.

Součástí návrhu síťového řešení by měla být relativně přesná a konkrétní představa

- jaké počítače by se měly v ideálním případě použít
- jaké počítače budou (*oproti ideálnímu stavu*) vlastně k dispozici
- jak bude řešení data-flow (*hardwarově i softwarově*).

Nedoporučuji ovšem plánovat strukturu sítě a poskytované služby jen na základě toho, že můžete něco použít. Méně znamená více, proto si rozmyslete, které služby nevyužijete, a pro které se naopak vyplatí vyčlenit samostatné prostředky.

Například instalovat na Web server síťovou hru typu Multi User Dungeon jenom proto, že ji máte a že se může někdy hodit, nemá smysl ani tehdy, když využívání MUD bude malé (*aplikace zůstane nevyužitá a její přítomnost nemá smysl*), ani když bude velké (*zbytečně ubírá strojový čas a systémové prostředky mnohem důležitějšímu webserveru, v takovém případě se vyplatí provozovat MUD na samostatném počítači*).

Předem si určete, zda budete využívat AppleTalk, nebo jen TCP/IP.

Pokud se v jinak Ethernetové síti má objevit počítač, který má jen LocalTalk, pak se tam nutně musí objevit i jeho router, pro který nelze použít nový Mac (*nemá sériový port*) a je nutné sáhnout po modelu se sériákem.

Je výhodou vybavit server víceuživatelským systémem s vyřešeným multitaskingem a nejlépe i s možností vzdáleného přístupu:

- pokud některý stroj, který máte k dispozici, je vybaven procesorem 68030 či 68040, stojí za to zamyslet se, zda by se nehodilo použít A/UX místo MacOS
- pokud máte PowerPC, na kterém A/UX nepojede, zvažte, zda by se dal nainstalovat nějaký UNiX (BSD) nebo Linux
- i UNiX či Linux lze doplnit o podporu protokolu AppleTalk a služby s tím související (<http://www.cs.mu.OZ.AU/appletalk/>)
- Pro 68k Macintoshe se tedy nabízí A/UX, NetBSD, OpenBSD, Linux m68k, Debian, Minix.
- Pro PPC Macintoshe se nabízí FreeBSD, NetBSD, OpenBSD, Debian, Yellow Dog Linux (*považují ho za velice zdařilý*), PPC/Linux (*pro počítače s NuBus*), mkLinux a další, od G3 výše i Darwin a Ubuntu Linux..

V případě klasického MacOSu, vyhněte-li se požití některého UNiXu, se vyplatí zamyslet nad verzí instalovaného systému:

- Nižší verze systému má menší nároky na systémové prostředky a běží rychleji, ale má hůře řešený multitasking, některé důležité doplňky chybí a některé programy vůbec nefungují.
- Systémy mají také svoje nároky – 7.0 až 7.5.3 poběží takřka na všem, systém 7.6.1 je určen pro 68030, 68040 a PPC, MacOS 8.1 pro 68040 a PPC, MacOS 8.5 a vyšší jsou jen pro PPC.
- Zjistěte si, jaká nejnižší možná verze systému bude stačit programům, které budete chtít spouštět (*chcete-li provozovat KDX server nebo klienta, musíte použít Mac OS 9.1 nebo 9.2, většinou ostatních běžnějších programů ale bude stačit systém 8.x, webový či FTP server lze bez potíží provozovat i se systémem 7.x, stejně tak BBS*).

- U Mac OS X je, při dostatečném výkonu počítače, lepší použít naopak vyšší verzi (*nejlépe minimálně 10.3.9*), protože je lépe odladěná a běhá kupodivu rychleji než verze starší, navíc toho i více nabízí (*kromě lepších nástrojů pro správu nebo rychlého přepínání uživatelů bez nutnosti odhlašování je to třeba i fakt, že X11 utilita v Mac OS X je přítomna až od verze 10.3*).

Kromě počítačů s více síťovými kartami a vhodným software lze jako router použít i hardwarové zařízení – krabičku, která tento počítač zastupuje, ovládanou přes webové rozhraní. Lze použít běžné výrobky používané u PCí, firma Apple vyrábí vlastní takzvané AirPort Base Station.

Base Station je podobný router, ovládaný přes webové rozhraní (*obsahuje software Karl's router, které vedle ShareWay IPNetRouter patří k nejlepším*), kromě Ethernetových přípojek obsahuje i zabudovaný telefonní modem a WiFi vysílač/přijímač, počítače tedy můžete "sesítovat" bez tahání kabeláže (*a lze takto routovat i notebooky vybavené AirPort kartou*).

AirPort Extreme se liší především vyšší rychlostí použitého WiFi spojení.

Promyslete si, zda přidělíte počítačům ve vnitřní části sítě IP ručně (pro vnitřní sítě se používají IP adresy z oboru 10.x.x.x nebo 192.168.x.x) nebo ji necháte přidělovat DHCP serverem.

Ruční nastavení předpokládá nastavení IP adresy, masky podsítě, gatewaye a DNS na každém počítači zvlášť.

Přidělování pomocí DHCP vyžaduje pouze nastavení adresy DHCP serveru. Na něm se potřebné údaje nastaví pouze jednou a on podle nich jednotlivé počítače automaticky konfiguruje.

DHCP server je často zabudován i v hardwarových routerech.

Ve většině případů i pro klasický MacOS existují potřebná softwarová řešení a lze se heterogenitě sítě (*současné použití Macintoshů spolu s UNiXovými stroji nebo PeCemi s Windows*) vyhnout, jak ukazuje třeba síťové řešení v samotné firmě Apple, kde si dlouhou dobu vystačili jenom s Macintoshi a standardním operačním systémem s pomocnými programy.

Pro celou síť, roztahanou po půlce planety, čítající patnáct tisíc počítačů, jim jako Domain Name Server stačil jediný stroj s instalovaným MacDNS – a ten obhospodařoval seznam jmen a adres všech patnácti tisíc počítačů, potřebné přesměrovávání, sdílení zátěže a další funkce včetně emulace rekurzivního odkazování.

Od té doby se sice firemní síť Applu dále vyvíjela a dočasně se v ní objevily i PowerPC servery od IBM s instalovaným AIX, ovšem díky výrobě X Serve, díky UNiXové podstatě Mac OS X a díky tomu, že Steve Jobs je předsedou správní rady nejenom Applu, ale i filmové společnosti Pixar, do jejíhož strojového parku počítače od Applu expandují, lze očekávat, že se Macy opět ujmou vlády nejenom ve firemní síti Applu.

Popřemýšlejte, zda nebude síť heterogenní, zda v ní kromě Applů (které mezi sebou mohou sdílet disky přes AppleShare) nebude ještě nějaký UNiXový stroj (*Sun, Silicon, DEC, ..., kvůli kterému se vyplatí zavést NFS či FTP*), případně PeC (*se kterou vás propojí DAVE nebo Samba na OS X*).

Určete si, co bude pro síť nativním prostředím a jak bude využíváno. UNiX sám o sobě je nudný, teprve v TCP/IP síti je s ním ta správná zábava. S Apply je to podobné, jedna stolní stanice se příliš neliší od jiných počítačů, jako je PeC nebo Amiga či Atari ST. AppleShare a sdílení disků na serverech ovšem znamená velký přínos.

Vaše sekretářka má po zapnutí svého počítače na ploše vzdálený disk, který je ve skutečnosti adresář na vašem počítači nebo serveru, kam jí ukládáte dokumenty k vyřízení nebo seznam úkolů – dostane se k nim i bez elektronické pošty, úkoly jí tam může ukládat i váš šéf, který má zároveň kontrolu o tom, jak ji úkolujete vy a jestli po ní náhodou nechcete vyřídit nějakou věc oba.

Do jiného nasdíleného adresáře může někdo ukládat drobná provozní sdělení, která se tím okamžikem objeví mezi aktualitami na firemním webu.

Je to všechno jednodušší, než kdyby všichni ti uživatelé museli spouštět FTP klienta, někam se nalogovat, zadávat heslo, kopírovat soubory na server a tak dále. Takhle je jen přesunou z jednoho okna do druhého, z místního adresáře do vzdáleného.

Možností, jak samotné AppleShare využít, je hodně. Když k tomu přidáte TCP/IP komunikaci s UNiXovými stroji, nabízejí se možnosti další, ale je potřeba k tomu uživatelům nabídnout co nejjednodušší prostředky.

Pokud shromáždíte několik Apple stanic kolem UNiXového superserveru, který z nějakého důvodu nebude podporovat AppleTalk, jak na něj budete data dostávat? A jak je z něj zase stahovat?

FTP, které se nabízí, znamená komplikace:

Složitou práci navíc pro uživatele a instalaci third-party software, nějakého FTP klienta.

Přes FTP často nevidíte ikony s typem souboru nebo náhledem obrázku, což je někdy ne zrovna příjemné.

Na druhou stranu, pokud zpracováváte výsledky měření magnetické rezonance, která je řízena UNiXovou stanicí a program na zpracování výpočtů běží na UNiXovém serveru, je stažení výsledků ze serveru na váš Macintosh už jen rutina, která se dá navíc třeba pomocí AppleScriptu automatizovat (*pokud je váš FTP klient scriptovatelný*).

Podobně lze scriptovat i na samotné centrální UNiXové stanici (*od toho tam je UNiX, aby se na tom dalo programovat, a ne Windows od Microsoftu, kde můžete akorát tak klikat*). Může vám například posílat vypočtené výsledky e-mailem přímo jako soubor pro Excel.

Nezapomínejte, že nastavená přístupová práva v MacOS platí jen pro AppleShare. Zajistěte, aby uživatelům nebyly k dispozici prostředky, které by jim mohly dát vládu nad počítačem.

Při nastavování práv v UNiXu nezapomínejte, že jedním z rozdílů mezi BSD a Systémem V je i to, zda může uživatel patřit do jedné či více skupin.

BSD podporuje členství ve více skupinách.

Vyplatí se všimnout si detailů (*a těmi počítače Apple opravdu oplývají, většinou to jsou samé praktické drobnosti*).

Servery (*jako Quadra 950*) mají možnost zamknout myš a klávesnici, což počítač chrání nejen před sabotérem, ale i před blbou náhodou, kdy někdo o klávesnici nebo myš v serverovně omylem zavádí.

Podobně vás asi bude zajímat, zda se stroj uchladí sám, nebo v něm ventilátory hučí jako ve vysavači, takový rámus se v pokojíčku nesnese, zatímco v oddělené serverovně, na půdě či ve světlíku to už jde.

Dalším detailem je to, že do počítačů, které mají několik PCI slotů, lze sehnat další síťové PCI karty v běžných PC bazarech, a využít je tak pro routerování (*sehnat NuBus nebo PDS karty je naopak skoro nemožné, máte však u nich zaručenu kompatibilitu, což se o kartách ze světa PeCí říci nedá a budou fungovat jen některé*).

Pokud je váš server stolní počítač s odděleným monitorem, zřejmě ho necháte stát někde v koutě s vypnutým monitorem, který budete zapínat jen kvůli administrátorským zásahům. Pořád jde ale o počítač rozdělený do dvou kusů, které v prostoru překáží.

Použitím třeba i staršího iMacu (*dají se koupit za cca 5 000 korun*) vznikne snadno přenosná jednotka (*dokonce s rukojetí, i to je praktický detail*), vybavená Ethernetem a modemem, případně AirPortem.

USB klávesnici a myš lze odpojovat a přepojovat i za chodu, takže se lze vyhnout náhodnému stisku nějaké klávesy a nežádoucí akci podobně, jako u zamykatelných serverů.

Po odpojení klávesnice a uspání obrazovky se z iMacu stane malá věc, která si tiše běží někde v koutku a krom šumu nezastaveného harddisku moc neotravuje, v případě lidského zásahu je ale rychle připravená (*jen zasunete myš do USB a pohnete s ní, obrazovka v počítači se sama probudí, nemusíte ani přinášet monitor ze sklepa*).

Pokud iMacu nastavíte automatické přepínání monitoru do úsporného módu, šetříte nejen luminofor, ale eliminujete i největší zdroj tepla.

Někomu přijde možná zvláštní, že většina Maců nemá žádné chlazení, když ze světa PeCí jsme zvyklí, že pouhé větráky často nestačí a je potřeba doplnit chlazení vodou nebo silikonovým olejem, ale Macy prostě tolik nehicují.

Usínání harddisku je lepší v sítích s hustším provozem nastavit na "nikdy", sice se pořád točí, ale zaručí vždy promptní odezvu. Pokud naopak síť většinu času běží naprázdno, doporučuje se šetřit harddisk a nechávat ho uspávat, ale rozjezdy a brzdění ho podle některých údajů mohou ničit více než stále se točící ložiska.

Použit jako server slabší stroj, když jako klient je připojená silnější mašina, se zdá jako logický nesmysl, jde ale o to, na co ten který stroj upotřebí svou energii.

Pokud u silného stroje máte scanner, velký monitor, děláte na něm DTP a digitální fotografii, je jasné, že zpracováváte obrovská data a jasné je i to, že na zpracování jednoho efektu v PhotoShopu chcete čekat minutu místo čtvrthodinky. Pak se nelze rychlému procesoru a velké videopaměti divit.

Pokud server slouží jenom k tomu, že na něj výsledky své práce ukládáte a občas si je odtamtud přes FTP někdo vyzvedne, pak u něj víc než rychlý procesor a 3D grafický akcelerátor oceníte spíše velkou diskovou kapacitu.

Nutné je zajistit bezpečnost dat. Je proto dobré myslet na vytváření záloh a nejlépe používat RAID disky s kontrolními součty, případně RAID software, který se dodával k Applovským serverům.

I americké univerzity používaly jako server, mám-li se zmínit o konkrétním stroji, Macintosh SE/30 připojený LocalTalkem, a to současně pro Gopher, FTP i AppleShare.

Stroj, který byl špička a postačoval, bude postačovat i dál, pokud po něm nechcete něco, co neumí (*dotyčný SE/30 by měl třeba s přehráním MP3 velké potíže*).

V místní síti vám takhle může fungovat starší WWW server, a dokud hostuje jen WWW stránky a běžné dokumenty, nikomu to ani nepřijde, projeví se až teprve stahování větších souborů, ovšem za předpokladu, že nepředpokládáte příliš silný provoz (*nutnost vyřídít několik připojení najednou*), nevádí ani jeho připojení na Internet.

V rámci místní sítě bývá přenos dat obecně rychlejší a lepší, než mezi sítěmi, takže v místní síti se zdá být delší odezva serveru více nápadná, než na internetu.

Máte-li například ADSL připojení k internetu 512 kbps a myslíte si, že server ve vaší LocalTalkové síti (*téměř 1 Mbps*) jede moc pomalu, pak asi nejste duševně úplně v pořádku.

I tehdy, předpokládáte-li silný provoz a časté požadavky uživatelů či nutnost současného vyřízení několika požadavků, stále nejsou slabší stroje mimo hru. Máte-li jich víc, pak mohou v souhrnu představovat vyšší výkon, než by poskytla mašina o třídu lepší.

Můžete-li pak třeba vhodným nastavením DNS rozdělit zátěž symetricky mezi ně, získáte krásný víceprocesorový cluster (*to už je pak spíš superpočítač, než jen pouhá síť*).

Myslíte-li si, že udržovat na discích takto propojených počítačů několikrát zrcadlo třeba webových stránek není nic snadného, tak i na tohle existují utility, které zajistí synchronizaci samy po síti. Vedle Synchronizace souborů, která je přímo součástí OS, je to třeba Simple Backup či velmi povedený Assimilator.

Rozdělování výpočetní zátěže je možné přes Propojení programů (*Program Linking*) dostupné v ovládacím panelu Sdílení souborů (*File Sharing*), dnes se nazývá Apple Remote Events - jedná se o vzdálené volání událostí AppleScriptu.

Umožňuje jednomu programu (*třeba textovému editoru*) získat data, která připraví jiný program (*třeba databáze*) na jiném počítači, a šetří tak procesorový čas i diskovou kapacitu.

Programy ale musí Apple Remote Events podporovat (*vzdálený program musí být skriptovatelný*) a program na vzdáleném počítači musí být spuštěný.

Pokud se vám ale podaří AppleScript a Remote Events ovládnout, můžete rozkládat výpočetní zátěž mezi více serverů. Pozor ale na bezpečnostní rizika!!! (*I Finder je skriptovatelný, nepovolujte tedy Program Linking nedůvěryhodným uživatelům, jinak někdo převezme vládu nad vaším počítačem*).

Myslíte-li to se serverováním vážně, nerozkládejte diskovou kapacitu sdílením mezi několik počítačů – přenosy mezi nimi zdržují provoz.

Raději se sežeňte velký disk nebo několik disků, případně diskové pole, a připojte ho třeba i ke staršímu stroji.

Vyplatí se dát do takového počítače co největší paměť, v dokumentaci na internetu nebo v programu Mactracker snadno zjistíte, kolik je pro daný typ maximum a jaký druh pamětí se do něj dává.

Pozor také na formát disku, systémy 7.x umí jenom formát HFS, rozšířený formát HFS+ podporuje Mac OS až od verze 8.

HFS se nejlépe hodí u disků zhruba do 1 nebo 2 GB, větší kapacity sice umí, ale pak neúměrně narůstá velikost clusterů a tím se z celkové kapacity disku zbytečně mnoho ukrajuje. Rovněž počet souborů na disku je omezen na 65535.

HFS+ umí zpracovat víc než 65536 clusterů, takže nezvětšuje jejich velikost, větší počet clusterů a větší disková mapa kladou ovšem vyšší nároky na paměť a rychlost procesoru. Počet souborů rovněž na 65535 není omezen.

Velkou výhodou může být to, že k Macintoshi lze v panelu Přenos souborů (*File Exchange*) připojit i SCSI disky z PeCe.

Používat disky v PC formátu dlouhodobě ovšem nikomu neradím, neustálé konvertování zbytečně zdržuje.

Hodí se ovšem dočasně, pokud musíte Macem nahradit PC server, který nečekaně kleknul, a zpřístupnit aspoň nějakou formou jeho data, nebo tehdy, chcete-li si data z PC disku zkopírovat na HFS+ oddíl.

Příklady sítí

Podíváme se nejdříve na příklad s Gopher serverem SE/30 na katedře chemie a biochemie jedné americké univerzity. Byl už jednou zmíněn, najdete ho i v dokumentaci k FTPd (NetPresenz).

Univerzita je americká, takže všichni, i sekretářky, mají Macintoshe, a vše je propojené LocalTalkem. Mezi počítači se našla jedna SE/30, určená na vyhození (*SE/30 je upravený Macintosh IIx, nacpaný do krabičky pro Macintosh SE; je to relativně silný stroj v malé přenosné krabičce se zabudovaným monitorkem*).

Osoba, za provoz Gopher serveru na katedře zodpovědná, si může SE/30 postavit v pracovně vedle svého vlastního počítače (*aby byl na očích a šlo provádět případné administrátorské zásahy bez pobíhání do sklepa a zápatky*) a kabelem ho připojit.

Stačí mít v systému MacTCP nebo OpenTransport, nainstalovat nejlépe NetPresenz (*využijeme-li FTP, jinak by stačil Gopher Surfer*), nastavit sdílení adresáře pro Gopher a FTP (*anonymní uživatelé jen pro čtení, autorizované osoby, jako sekretářky oddělení a provozovatel serveru, i pro zápis*), nahrát obsah Gopheru do adresářů a pak už jen nahlásit správci nameserveru (*DNS*), na kterém počítači Gopher a FTP běží, aby mu mohla být přidělena nějaká rozumná URL.

Vlastně ještě nastavit na počítačích sekretářek trvalé namountování Gopher adresáře, aby mohly dokumenty, určené ke zveřejnění, zkopírovat na Gopher pouhým přesunutím na ikonu na ploše, a nemusely lovit v Chooseru a připojovat se ručně.

Vzhledem k tomu, že na zpola úředním, zpola pracovním serveru nějaké bohem zapomenuté katedry nebude asi příliš velký cvrkot, soubory budou spíše menších objemů a Gopher nebyl ani tehdy příliš využívanou službou, lze očekávat, že dotyčná SE/30 nebude ani plně vytížena (*většinu času stráví čekáním, čas od času pak odešle nějaký nevelký soubor*).

Myslím, že je to nádherná ukáзка využití solitérního serveru.

Zkusíme využít několik počítačů tak, že každý bude využit pro serverování jiné službě. Předpokládejme, že máte k dispozici jedinou IP adresu. Ta v tomto případě úplně stačí.

Velmi jednoduché, ale ne čisté řešení využije z jednotlivých počítačů jejich diskovou kapacitu, ale skutečný server (*s příslušnou IP adresou*) bude jen jeden z nich.

Například harddisk jednoho stroje dedikujeme pro FTP, harddisk druhého pro WWW. Nemusíme na nich ani zapínat TCP/IP, stačí připojení přes AppleTalk.

Na třetím stroji, s přidělenou IP, si jejich disky přes AppleShare nasdílíme, spustíme třeba NetPresenz a jako kořenové adresáře služeb FTP a WWW určíme sdílené disky příslušných počítačů. Stačí mít jen správně nastavená práva.

Takové řešení ovšem může hlavní počítač dost zatížit a procesory podřízených počítačů mu v ničem neulehčí. Snadno tento způsob nahradíme tak, že disky, určené pro uložení dat obou služeb, prostě přímo připojíme k hlavnímu počítači (*ať už jako interní, má-li dostatek pozic, nebo jako externí*).

A je z toho zase solitérní server.

My jsme ale chtěli, s jedinou IP adresou, provozovat ka každém z několika počítačů server pro jinou službu.

Při použití programu IPNetRouter na hlavním počítači lze použít IP maškarádu (*všechny počítače se "schovají" za společnou IP adresu*) a port mapping.

IPNetRouter, v případě, že pouze jeden počítač má Ethernetovou kartu, zajistí i přesměrování TCP/IP z Ethernetu do LocalTalku.

Port mapping se nastavuje přímo v IPNetRouteru, a to tak, aby internetové pakety, doručené "routeru", přeposlal správnému počítači na základě toho, pro jaký port (*a tudíž pro jakou službu*) jsou data určena. Takže data, která přijdou na port 80 (*http*) se nechají přeposlat webovému serveru, data z portu 23 (*Telnet*) zase počítači, na kterém běží například BBS.

Tím je docíleno toho, že různé procesory různých počítačů zpracovávají dotazy různých služeb a systému tím ulehčují.

IPNetRouter pracuje ovšem s IP adresami a neumí rozdělovat zátěž jedné služby mezi několik různých počítačů. Jediná společná IP totiž představuje jediný počítač, a jednotlivé stroje jsou zvenčí neviditelné, a kromě portmappingu (*který stále ještě předstírá jediný počítač*) se na ně dostaneme jen tím, že jim odpovíme, jinak vůbec.

Tedy ještě poznámka k tomu, jak je IP maškaráda realizována – podobně, jako port mapping. Zjednodušeně řečeno, gateway, maškarádu realizující, dostane od jednoho z vašich strojů požadavek na nějakou informaci (*s údajem, z které IP pochází a na který port se má poslat odpověď*). Přepośle ho příjemci, ale tak, jako kdyby přicházel od ní (*z její IP*), a odpověď si vyžádá na nějaký zvláštní port. Tento port si sama namapuje tak, aby odpověď, která na něj přijde, mohla být přeposlána na IP a port, kam je správně určena.

Zkusme teď předpokládat opak, tedy to, že chcete na několika počítačích serverovat jediné službě, například webu, u kterého předpokládáte vysokou návštěvnost.

Protože je to otázka složitější, předpokládejme nejprve, že máte k dispozici IP adres několik.

Srovnajte počítače tak, aby zabíraly málo místa a propojte je.

(Desktopové počítače zřejmě postavíte na sebe, úplně úžasně se takhle do věže stavějí ploché "pizzaboxy" počítačů řady LC - aby byly zcela vodorovné, stačí zadní nožičky podložit standardní krabičkou od sirek. Towers budete stavět především vedle sebe a částečně i na sebe. Je vhodné, aby všechny stroje byly stejného druhu).

K celé sestavě vám bude stačit jediná klávesnice, jediná myš a jediný monitor, vše se dá přepichovat za chodu (*ale opatrně, zkratem lze počítač nebo periférie zničit*).

K tomu jedna poznámka – nezapínejte Macintoshe bez připojeného monitoru, nezaktivuje pak videokartu.

Je tomu tak proto, aby bylo možné mít v počítači více videokaret, a počítač si sám zaktivuje jenom ty, ke kterým je monitor připojen.

Po naběhnutí obrazu už můžete monitor odpojit a připojit ho k jinému počítači, který chcete zapnout nebo zkontrolovat jeho činnost.

Na jednom stroji vám běží DNS server, na ostatních identické kopie vašeho webu, a doménu už asi máte taky zaregistrovanou (*dotazy na vaši doménu si necháte ze své nadřídzené domény posílat na svou DNS*).

DNS nastavíte tak, že odpovídající domény (doména.cz a www.doména.cz) přiřadíte počítačům s webem, všechny si je označíte a nastavíte sdílení zátěže (*Share Load*). Kdykoliv na DNS přijde dotaz na webovou doménu, odešle IP adresu jednoho ze zvolených počítačů (*MacDNS nevybírá adresy náhodně, ale cyklicky*) a tím se zátěž mezi ně v podstatě symetricky rozdělí.

Použití vlastní DNS je v tomto případě nutnost, cizí DNS většinou sdružování IP adres pro sdílení zátěže neumožňují.

Nevýhodou je redundantní výskyt několika kopií webu, které se musí mezi sebou synchronizovat, však se také tato metoda jmenuje RAIC (*Redundant Array of Independent Computers, redundantní pole nezávislých počítačů*).

Rozhodnete-li se pak provozovat třeba ještě ftp, můžete (*nebo nemusíte*) těm samým počítačům přiřadit ještě doménu ftp.doména.cz, ale měli byste na nich spustit FTP server.

Vzhledem k tomu, že na ten vám uživatelé budou asi uploadovat, máte několik možností:

- Na každém počítači mít část upload adresáře. A pak synchronizovat, synchronizovat a synchronizovat.
- Jedno řešení využívající vymoženosti AppleShare - dedikovat jeden počítač (*samostatný disk*) pro upload. Na ostatních počítačích je pak místo upload adresáře jen odkaz na uploadový počítač. Ten ani nemusí být přístupný z internetu, uživateli zvenku se přesto bude zdát, že upload adresář je umístěn normálně na FTP serveru. Cokoliv totiž na uploadový počítač uploadnete přes jeden server, automaticky se objeví i "na disku" na těch ostatních, které mezi sebou sdílí zátěž. (*Toto řešení předpokládá, že upload není zdaleka tak frekventovaný, jako download. Pro praxi je to předpoklad pravdivý – nestaneme-li se obětí DoS attacku nebo floodu.*)

V tomto okamžiku nám tedy ty samé počítače poskytují WWW a FTP server.

Co ale dělat, když se z nějakého důvodu rozhodneme, že je to pro ně příliš velká zátěž?

Dejme tomu, že máme k dispozici ještě další počítače, které můžeme do systému přidat. A rozhodneme se provozovat WWW na polovině z nich, FTP na druhé polovině.

Máme-li dost IP adres, tak ftp doménu můžeme přisoudit jedné části počítačů, www doménu (*a obecnou doménu, protože lidé někdy subdoménu www vynechávají*) druhé skupině.

To by ale znamenalo, že nemůžeme přistupovat k FTP jinak, než přes ftp subdoménu, což je hloupé, neboť lidé raději přistupují přes obecnou doménu.

Jakmile ale zjistíme, že IP adres dostatek nemáme, řešení přijde samo.

Sdílet zátěž mezi různými službami přeci umíme stejně dobře, jako mezi jednou službou.

Vyrobíme tedy přes port mapping jakési maškarádové dvoupočítače.

Takový dvoupočítač se skládá ze dvou počítačů, na jednom běží FTP, na druhém WWW server, gateway jsou oba schované za jedinou IP adresu a přes port mapping se dělí o poskytování příslušných služeb, to už přeci známe.

DNS potom všechny domény (doména.cz, www.doména.cz i případně ftp.doména.cz) přesměrovává na IP adresy gatewayí (*nemusí jít o více počítačů, může to být i jeden s několika síťovými kartami*), mezi které rozděljuje zátěž směřovanou na doménu, a gatewaye se pak přes port mapping starají o rozložení zátěže směřované na služby (*porty*).

Představme si, že máte k dispozici datovou linku s několika IP adresami (*určenými pro servery a router*), kromě serverů ovšem chcete do sítě zapojit i pracovní stanice, o nichž předpokládáte, že je potřeba jim zajistit přístup na internet.

Základem řešení je opět router, buď samostatný počítač, nebo přes Web ovládané hardwarové zařízení (*vhodná je Apple AirPort Base Station, cenový rozdíl oproti běžným bezdrátovým routerům je malý a možnosti nabízí velmi široké*).

Router má svou IP adresu, za ním je pak zapojená případná DNS (*s veřejnou adresou*), servery (*s veřejnou adresou, případně se službami rozloženými přes port mapping na stroje s adresami vnitřní sítě – tím se šetří veřejné IP adresy*) a pracovní stanice (*s IP adresami vnitřní sítě, jsou tak chráněny proti útoku zvenčí; routování od těchto počítačů do internetu může být povoleno nebo pro některé z nich znemožněno*).

Důležité je zajistit hlavně to, aby byla zajištěna komunikace počítačů ve vnitřní síti mezi sebou, bez ohledu na to, zda mají nebo nemají povolen přístup do veřejného segmentu.

Software pro MacOS classic

Co se týče pro síť potřebného softwarového vybavení, často je překvapivě málo náročné a běhá i na Systému 7.x nebo Systému 8.

Integrovaná serverová řešení

Daemon

Daemon poskytuje několik služeb, známých z UNiXu: Finger, Whois, Ident, Daytime, Time a NTP. Část z nich poskytuje zájemcům podrobnější údaje o vašem počítači a jeho uživateli (Finger, Whois). Rozsah a forma informací je pro každého uživatele definovatelná, nemusíte se tedy bát, že na vás práskne něco, co nechcete. Děje se tak pomocí „plan“ souborů, což jsou obyčejné textové soubory, ve kterých vyjvíte případným zájemcům svoje spády a můžete je obohatit o informace o svém stroji, o tom, jak dlouho ho máte zapnutý, a podobně. Způsob, jakým se tak děje, je popsán v dokumentaci a navíc jsou přiloženy i ukázkové soubory s vysvětleními.

Druhá část informuje zájemce o vašem systémovém čase – ideálně by se mělo jednat o čas aktuální. Nejste-li si jisti správností nastavení hodin ve svém počítači, případně máte zničenou baterii zálohující hodinový obvod, můžete si některým NTP klientem (viz dále) seřadit čas podle jiného NTP serveru. Ve světě je dokonce zvykem sdružovat NTP servery do poolů – při požadavku na přesný čas DNS poolu vybere náhodně jeden z NTP serverů, na který se pošle požadavek na přesný čas. Nejste tak závislí na tom, je-li zrovna váš oblíbený NTP server zrovna dostupný. Pokud chcete NTP službu poskytovat někomu, kdo o to stojí, snažte se, aby byla rovněž dostupná kdykoliv.

Daemon není náročný, běží na pozadí a takřka o něm nevíte. Stačí mu 68k procesor a Systém 7.

NetPrezenc

NetPrezenc je pokračovatelem programu FTPd (*jméno pocházející od FTP daemona na UNiXu*). Prosim vás ale, abyste FTPd nepoužívali, protože obsahuje několik bezpečnostních děr, které právě NetPrezenc odstraňuje.

NetPrezenc poskytuje tři služby – FTP server, Gopher server a WWW server, který nabízí dokonce podporu CGI scriptů.

Nemusí běžet všechny tyto služby, aktuální sestavu si nastavíte pomocí Setup programku. Ten vám umožní nadefinovat sdílené oblasti disků, uživatele a přístupová práva. Práva jsou odvozena od nastavení AppleShare, pro provoz WWW tedy musíte pro ten adresář, který WWW stránky obsahuje, mít povolen přístup anonymních uživatelů, a vůbec se vyplatí práva AppleShare synchronizovat s nastavením NetPrezenc.

Co se CGI týče, je to potenciálně nebezpečná věc, skripty musí být umístěny mimo sdílenou oblast disku, zcela nepřístupné běžným uživatelům. To je ale zcela obecná bezpečnostní zásada platící pro CGI, nikoliv specifická vlastnost NetPrezenc. Dále je možné kromě index souborů (jak HTML, tak scriptů) používat i missing soubory (včetně scriptů), které mohou jednak zvýšit bezpečnost site, druhak zvýšit pohodlí navigace.

S tím, jak NetPrezenc ctí práva AppleShare, může mít každý uživatel jiná omezení a vy máte možnost důvěryhodnému uživateli umožnit přístup tam, kam by se jiný nedostal. Při správném používání jde o server značně bezpečný. NetPrezenc rovněž ctí aliasy a může jejich pomocí čerpat obsah nejen jiných disků, ale i jiných počítačů v síti.

I FTP server je velice podařený a nabízí množství funkcí specifických pro Macintosh, jako přenos MacBinary, vzdálenou změnu hesla, indexování, vzdálené vypnutí...

Gopher se sice v dnešním světě takřka nepoužívá, jistě se ale dají najít situace, kdy se jeho použití hodí. Samotný program NetPrezenc může běžet nepozorovaně na pozadí, nebo může zobrazovat log (v případě, že není zvolen jako aktivní aplikace, sám se skryje). Práce s ním je velmi příjemná a při své jednoduchosti nabízí hodně možností – přesně to, co by Macintosh měl nabízet.

Jeho další výhodou je rychlost, v tomto směru je to asi nejlepší WWW a FTP server, rychlostí předčí i jinak výborný MachHTTP. Neumí ovšem sám od sebe virtuální domény.

Program běhá i na 68k procesorech a stačí mu Systém 7.

WebTen

WebTen je komerční integrovaný balík, zahrnující webový server Apache pro Macintosh, skriptovací jazyk PHP, rozhraní pro webmail a další služby.

WebTen je jedinou možností, jak pod Mac OS (*nepočítáme-li OS X*) zprovoznit PHP, které dnes mnozí uživatelé potřebují. To je zde bohužel koncipováno přímo jako modul pro Apache, takže nejde použít s jinými webservery. PHP je dostupné ve verzi 3 a existuje i upgrade na verzi 4.

Zajímavé na tomto balíku je, že administrátorská správa se provádí přes WWW, je tedy možné spravovat server i vzdáleně, a to relativně pohodlně oproti editaci konfiguračních souborů pro Apache třeba pod Linuxem. Použití právě Apache serveru je velkou výhodou, jde o mimořádně výkonné řešení s rychlou odezvou, a především dobře prověřené i na jiných platformách (UNiX, Linux, Windows).

Další plus představují integrované služby, kterých je opravdu hodně. Log soubor, který produkuje, je navíc standardní a analyzovatelný dalšími nástroji jako třeba AnaLog.

WebTen vyžaduje PowerPC procesor a dostatečně výkonný počítač.

Bez platné licence poskytuje třicetidenní plně funkční demo, ale co jsem zkoušel, licence jsou nejspíše časově omezené.

Další webové servery

EasyServe

Pokud vás popis funkcí a ovládání NetPresenz vyděsil, bude EasyServe pro vás to pravé.

Jde o jednoduchý server, který prostě spustíte s tím, že v adresáři *doc*, uloženém v adresáři s programem, musíte mít uložené vytvořené (statické) WWW stránky s obrázky a soubory na stažení, nezapomeňte na *index.html*.

Nic jiného server nedělá, neumožňuje použít dynamické WWW stránky (skriptování), zobrazuje ale při běhu log.

I tomuto programu stačí 68k procesor a systém od verze 7, má ovšem některé nedostatky, především není příliš rychlý.

Personal WWW sharing

Jako alternativní webový server lze použít i ten, který je standardní součástí systému 8 a vyšších (najdete ho pod ovládacím panelem **Sdílení WWW**).

Pod systémem 8.1 se podobá spíše EasyServe s tím, že nabízí i zobrazování obsahu disku a stažení souborů (Personal Net Finder), ve vyšších verzích už nabízí i skriptování a další pokročilé možnosti.

Vyhnete se ale systému 8.5, tam Personal WWW sharing obsahuje závažnou bezpečnostní chybu, umožňující velmi snadné napadení vašeho počítače (doporučuji spíše systém 8.1, 8.6, 9.1 nebo 9.2).

Ovládání je tradičně přehledné a jednoduché, vzhledem k tomu, že ovládací panel a příslušný doplněk je součástí konkrétního systému, neměl by být se systémovými požadavky žádný problém.

Tento server je nicméně určen spíše pro stránky osobního charakteru, firma Apple doporučuje, chcete-li na internetu vystavovat větší množství dat, použít některé komerční řešení.

MacHTTP

Jde o volně šiřitelný, OpenSource server vysoké kvality.

Umožňuje široké možnosti nastavování, i když relativně složitě pomocí konfiguračních textových souborů. Umožňuje skriptování, správu subdomén, existuje i verze, upravená tak, aby umožnila ovládání zařízení z webové stránky pomocí X10 Tools. Výkon je nastavitelný, nicméně i bez složitých zásahů do konfigurace běží program uspokojivě. Log z MacHTTP je díky jeho rozšířenosti rovněž možné dále zpracovávat.

Pokud nepotřebujete nutně PHP, patří MacHTTP k tomu lepšímu, co se nabízí, i přes svou složitost.

Program není náročný, běží i na procesorech 68k a Systému 7, pro vyšší výkon se doporučuje Thread Manager (nebo vyšší systém, který ho má už zabudovaný).

Existují i další komerční WWW servery, například **4D WebStar** nebo **Apple IP Share**, předpokládám ale, že pro svou nedostupnost nemají pro českého uživatele velký význam.

Další FTP servery

Kromě NetPresenz můžete jako FTP server používat **VICOM FTP Server**.

Možnostmi se od FTP serveru NetPresenz příliš neliší, i on poskytuje možnost definovat uživatele a rozsah jejich přístupu, není ale závislý na AppleShare, umožňuje vyčlenit určité procento strojového času a tím ovlivnit výkon. Podle mých testů má ale NetPresenz při defaultním nastavení lepší odezvu. Lze spustit i na stojících s procesory 68k.

Relativně zvláštním jevem je skutečnost, že FTP server, a velice dobrý, je zabudován i do telnetového a SSH klienta.

Better telnet a jeho SSH odvozenina **MacSSH** opravdu obsahují zdařilý FTP server. Vzhledem k jeho integraci ke klientovi je ovšem vhodný spíše pro krátkodobé spouštění než dlouhodobý běh na pozadí. MacSSH existuje ve verzích pro 68k a PPC a o obou programech ještě bude řeč.

Scriptování na straně serveru

Na Macintoshi existuje několik druhů scriptů.

Jednak je to klasické CGI, známé i z jiných počítačů.

Jedná se o relativně nebezpečný prvek, protože umožňuje spouštět takřka cokoli a cokoli s počítačem provádět. Je proto nutné ho dobře hlídat a zabezpečovat před nenechavci. Další nevýhodou CGI je to, že při zavolání skriptu se musí naalokovat paměť, nahrát soubor se skriptem a spustit. Po dokončení běhu se výsledek předává webserveru, ukončuje se běh skriptu a paměť se uvolňuje, což spotřebovává systémové prostředky (strojový čas, přístup k disku, paměť), které pak mohou chybět jinde.

Pro Macintosh specifické aCGI využívá Apple Events. Program, zajišťující běh skriptu, je celou dobu spuštěný a umístěný v paměti, webserver pouze vyvolá událost, kterou program zpracuje a vrátí výsledek, přičemž zůstane běžet a čekat na další zavolání, ušetří se tak mimo jiné něco času.

Na OS X dělá něco podobného fCGI, fast-CGI, tedy „rychlé“ CGI.

Zvláštností jsou pak moduly pro Apache, jako třeba PHP pro WebTen.

Skriptování na straně serveru je, ještě jednou opakuji, ošemetná záležitost, protože se vždy jedná o potenciální bránu pro napadení systému. Uživatel nemá mít možnost umisťovat na server libovolné svoje skripty. Na druhou stranu, existující skripty a jejich zdrojový kód jsou ukryty před zraky šťouralů, kteří vždy dostanou WWW stránku v čisté HTML podobě. Kromě standardního browseru není většinou vyžadována zvláštní podpora na straně klienta.

Scriptování *na straně klienta* je jinou věcí, zdrojový kód je doručen až k němu (je tudíž dostupný jeho zkoumáním) a je prováděn příslušným modulem browseru (*nemá mít tedy za běžných okolností přístup k systémovým zdrojům serveru*). Patří sem například JavaScript.

Frontier

Silným, i když na první pohled komplikovaným prostředkem pro CGI skriptování je Frontier pro klasický MacOS.

Jeho součástí jsou i další aplikace, usnadňující skriptování pro Web, jako BarChart pro tvorbu histogramů, jednoduchá databáze uBase, o níž ještě bude řeč, a DocServer, který poskytuje nedostižnou on-line nápovědu k povelům a funkcím Frontieru. Šíře příkazů je sice obrovská, ale jinak je Frontier snadno použitelný.

Frontier pochopitelně nabízí nejen webové skriptování, lze na něm s úspěchem vytvořit řadu úloh i pro lokální použití.

Frontier umožňuje skriptování i na 68k strojích, je použitelný tedy i tam, kde MacASP, o němž bude ještě řeč, spustit nejde.

MacASP

Technologie Active Server Pages od Microsoftu se rozšířila zejména v poslední době.

Její obdoba pro Macintosh, vyvíjená jako volně šiřitelná a OpenSource aplikace, založená na příkazové sadě Visual Basicu, je částečně s řešením Microsoftu kompatibilní, přináší ale další možnosti navíc, především takové, kde využívá specifických vlastností Macintoshe.

MacASP patří na OS 9 mezi aCGI technologie (verze pro OS X je fCGI), běží tedy spolu s webserverem a ten jí poskytuje příkazy, které jsou implementovány přímo do zdrojového kódu HTML. Tento kód se ovšem uživatelům nezobrazuje, ti vidí vždy až výsledný produkt po zpracování pomocí MacASP.

Nabídka příkazů a funkcí je široká a dělá tak z MacASP univerzální nástroj, kterému může konkurovat snad jen PHP, jehož znalost je více v povědomí tvůrců WWW stránek, ale které je v prostředí Macintoshe vázáno na WebTen (*nebo použití systému OS X*).

Dokumentace je bohužel dostupná jen na Webu.

MacASP vyžaduje PowerPC procesor.

AppleScript

Tento skriptovací prostředek, který je součástí přímo systému, umožňuje používat takřka jakékoliv skriptovatelné aplikace pro Macintosh, a to relativně jednoduchým způsobem – posláním zprávy běžící aplikaci. Protože i Finder je skriptovatelný pomocí AppleScriptu, jde o mimořádně silný prostředek, a musí se s ním zacházet opatrně, protože umožňuje převzít kontrolu nad počítačem případnému útočníkovi.

AppleScript ovšem oceníte v případě, že chcete použít jednoduché skriptovatelné aplikace, například MondoMail, umožňující pomocí jednoduchého acgi skriptu odesílat z WWW stránky vzkaz na e-mail, nebo databázi uBase, která je součástí balíku Frontier.

PHP je v současné době nejrozšířenější skriptovací prostředek vytvořený speciálně pro Web (*jeho použití není ale na Web omezeno, chová se jako jakýkoliv jiný skriptovací jazyk a je možné v něm tvořit i skripty běžící lokálně*). Je podobné Basicu, a tedy relativně jednoduché a přístupné i začátečníkům, z čehož jeho oblíbenost zřejmě vychází. Díky jednostrannému zaměření neposkytuje mnoho prostředků nesouvisejících přímo s Webem, například práci s grafikou, a možností definovat rozsah povolených povelů omezuje možnosti napadení serveru. Navíc je kompatibilní napříč platformami zhruba jako Perl. Je přímo součástí systému OS X.

Jeho nevýhodou je, že při použití Mac OS do verze 9 je spojeno s jediným, a to komerčním produktem WebTen, určeným jen pro PowerPC.

Klasické CGI lze provozovat na většině programovacích jazyků.

Nabízí se **MacPerl**, který je sice určen pro PPC, ale s několika omezeními se dá spustit i na počítačích s procesory 68k. Jde o plnohodnotný Perl ve verzi 5.

Perl je výkonný jazyk, velmi oblíbený a nabízející mnoho možností, jak určitou úlohu naprogramovat, navíc má zabudováno množství funkcí pro práci s řetězci, vyhledávání a podobně. Strukturou vzdáleně připomíná Basic, je tedy relativně jednoduché se ho naučit. Díky jeho rozšířenosti a hlavně kompatibilitě s jinými platformami není problém najít odpovídající dokumentaci.

CGI se dá napsat i v **Chipmunk Basicu**. Jde o interpretovaný klasický Basic, dostupný rovněž pro Mac OS X, Windows a Linux, ovšem s množstvím moderních funkcí. Rozhodně něco pro pamětníky éry osmibitů nebo ty, jimž bude vyhovovat svou jednoduchostí a přístupností.

Existuje v mnoha verzích s různými systémovými nároky, starší verze jsou spustitelné i na 68k systémech.

Rovněž pomocí **Pocket Forthu** lze realizovat CGI skripty.

Jde o jazyk v dnešní době poněkud opomíjený, spojuje však výhody nízkourovňového kódování s výhodami vyššího jazyka a ve specifických situacích může být k nezaplacení především díky vysoké rychlosti provádění programu.

PocketPerl pro Macintosh navíc umožňuje, i když zvláštním způsobem, vytvořit samostatnou aplikaci (osamostatnění runtime).

Běží dobře i na velmi starých strojích se Systémem 6.

Programový balík **MacMeth** je ve skutečnosti programovací jazyk Modula 2.

Určený je spíše na simulace procesů a modelování dějů, dá se ale použít i ke skriptování. Jeho potíž je ta, že není ve všeobecném povědomí a snaha naučit se tomuto jazyku je většinou provázena nedostatkem potřebné literatury. Některým programátorům může ale tento objektový jazyk připadat povědomý - většina dnešních objektových rozšíření jazyků (*Delphi*, *Visual Basic*, *C++*) je odvozena od Moduly (výjimkou je *Objective-C*, které je založeno na *SmallTalku*).

Tcl/Tk je interpretovaný crossplatformní jazyk (Tcl) doplněný o toolkit pro tvorbu GUI prvků (Tk). Tk se dá použít i odděleně spolu s jiným programovacím jazykem (například Perl/Tk). Tcl má značně komplikované možnosti zpracování čísel a matematických výrazů, zato je dobře využitelný při zpracování textů a dat – k naprosté většině dat totiž přistupuje jako k textu. Je hojně využíván jako průmyslový standard pro tvorbu utilit a frontendů pro některé složitější programy hlavně v UNIXu, i když je na první pohled poněkud těžkopádný. Jeho výhodou je naopak možnost pracovat na libovolné platformě.

V klasickém Mac OS vyžaduje PowerPC procesor.

Databáze

uBase

Čtete jako „mikrobáze“ – jde o velmi jednoduchou databázi bez vlastního uživatelského rozhraní, ovladatelnou pouze pomocí skriptování.

Dobře se hodí pro správu databází na Webu. Je malá, nenáročná, ovšem pro většinu situací, kdy je potřeba databázi využít, bude postačovat.

Pro provoz postačí stroj s procesorem 68k.

FileMaker je komerční databáze, jedna z nejlepších pro Macintosh (a Windows), která nabízí vlastní webové rozhraní – lze s ní tedy pracovat i vzdáleně. Webové rozhraní mohou využívat i uživatelské aplikace pomocí FileMakeru vytvořené (ve FileMakeru bylo vytvořeno například podvojně účetnictví a obchodní systém UCT - www.uct.cz).

Tyto schopnosti jsou bohužel vázány na relativně recentní verze (5 a výše), které budou vyžadovat procesor PowerPC. Další nevýhodou je komerční povaha tohoto produktu a jeho vysoká cena. Koupí lze ovšem jen doporučit.

Pod Mac OS 9 lze použít rovněž komerční **MacSQL**. To je kompatibilní s relační databází MySQL, hojně používanou na Webu zvláště ve spojení s PHP, ovšem vysokými požadavky na systém a komerční povahou svůj význam samo znehodnocuje.

Na starších systémech pak lze uchodit třeba **Oracle**, neb i ten pro Macintosh existuje, včetně strojů s procesory 68k a Systémem 7. Některé reference hovoří i o možnosti použití **FoxBase**, se kterou ovšem jakožto s komerčním systémem nemám žádné zkušenosti.

OS X pak obsahuje přímo instalaci MySQL a existuje velké množství GUI utilit a frontendů pro jeho správu.

Klientské programy běžných služeb

NTP

Systém 9 (a OS X) obsahují implementaci NTP klienta v ovládacím panelu Datum a čas. Pokud máte na počítači NTP server (Daemon), možnost seřídit si čas podle jiného NTP serveru v síti se hodí.

Pro starší systémy existuje výběr hned dvou možností. První je program **Vremya** se širokými možnostmi a bohatou škálou nastavení, je možné nechat ho spustit skrytě po startu, nechat seřadit čas a samovolně ukončit, nebo nastavit seřizování v pravidelných intervalech. Lze použít na 68k strojích.

Druhou možností je použití ovládacího panelu **Network Time**, jehož možnosti jsou zhruba podobné programu Vremya nebo ovládacímu panelu Datum a čas nových systémů, potrápí vás ovšem, pokud po zapnutí počítače nenajde připojení k nastavenému NTP serveru. I tento panel funguje na 68k strojích.

Pokud chcete přesného času využít a vidět na mapě aktuální rozložení dne a noci na planetě, existuje hezký doplněk **SunClock**, převedený z UNiXu a pracující offline. Pokud k tomu budete chtít znát i aktuální oblačnost, vyhoví vám **Planet Earth** nebo jeho novější verze **Earth Browser** – informace o oblačnosti si stahuje z internetu.

Finger, Whois

Klient služby Finger se jmenuje **Finger**. Umožňuje nejenom využití služby Finger, tedy získávat informace o jednotlivých uživateli na počítači, který tuto službu podporuje, zjišťovat dobu, po kterou s počítačem pracují, jejich zájmy a další informace, ale podporuje i službu Whois, kterou poskytují specializované Whois servery (po světě jich je několik, každý obhospodařuje daný světadíl, například whois.ripe.net pro Evropu). Informace z Whois serverů jsou o mnoho oficiálnější, ale jsou dostupné i tehdy, když vámi zkoumaný server službu Finger či Whois sám neposkytuje.

Služba Finger je užitečná při zjišťování, zda je daný uživatel online (například ve spojení s programem NetBots), dnes už ale není tak používaná jako dříve a tak ji mnoho uživatelů ani nezná. Zvlášť v akademickém a univerzitním prostředí se ale jednalo o užitečnou věc.

Systémové nároky programu Finger jsou tradičně minimální a funguje i na 68k počítačích.

Talk

Podobně jako Finger, i Talk je UNiXový protokol ze starých dob, dnes mnoho lidí neví, že existuje, ani ho neumí používat. Program, který ho realizuje na Macintoshi, se jmenuje **Talk**. Podobně jako na UNiXu, skládá se ze dvou částí, démona **Talkd**, který po spuštění čeká na pozadí a hlídá příchozí „hovory“, a samotného klienta Talk, který ze všeho nejvíc připomíná chat mezi dvěma účastníky. A přesně to Talk opravdu je.

Kvůli rozdílným implementacím protokolu na UNiXu nefunguje verze pro Macintosh s úplně všemi systémy, dokumentace například popisuje, že nefunguje ve spojení s Appllovským A/UX. Mezi dvěma Macintoshi však spojení funguje spolehlivě. Systémové nároky jsou opět minimální a vystačíte si s počítačem s procesorem 68k.

Typický Macintoshácký způsob komunikace přes AppleTalk představuje aplikace **Broadcast**, v heterogenním prostředí (zvlášť při použití TCP/IP) je ale nestabilní, běží dobře ale i na velmi starých systémech (System 6).

Gopher

Služba Gopher je starší než Web, a dá se říct, že je jeho přímým předchůdcem. Gopheru chybí vlastnosti hypertextu, jeho dokumenty se rozdělují na dvě skupiny: vlastní dokumenty (*hlavně textové nebo třeba obrázky*) a menu, která obsahují seznam dokumentů a „slyší díry“, odkazy na jiné Gopher servery.

Pro globální prohledávání Gopher sítě existovala značně pokročilá služba Veronica. Vyplatí se naučit ji ovládat.

Hezký Gopher klient se jmenuje **TurboGopher** a stačí mu System 7.5 (nebo 7.0 doplněný o Thread manager), Gopher protokol ale podporují i některé webové browsery.

Klienty pro FTP jsou starší **Anarchy** (s podporou vyhledávací služby Archie) a novější **Fetch**, rovněž některé webové browsery umí FTP.

Obzvláště stojí za vyzdvihnutí utilita **WhatRoute**, které je součástí systému a kromě služeb Finger, Whois, Ping, Traceroute, Monitor nebo AdressScan zobrazuje například trasu na mapě, statistiku pingu formou grafů, obsahuje i vlastní Telnet server, přes který je možné se k Macintoshi vzdáleně připojit a služby programu WhatRoute použít přes Telnetový terminál i na dálku (pochopitelně lze WhatRoute přeměrovat i na jiný, než Telnetový port, a lze definovat seznam lidí, kterým připojení povolíte nebo zakážete).

Programů podobných WhatRoute ovšem existuje poměrně velké množství. Zajímavou kompilací jsou třeba i **AGNetTools**, které zahrnují Ping, TraceRoute, DNS lookup, Finger, Whois, test přenosové rychlosti, Name scan, Port scan, Ping scan a Service scan.

Jako e-mailové servery lze použít starší **MailShare** nebo novější **Eudora Internet MailServer**. Oběma stačí System 7.0 a oba jsou si velice podobné, ovládají se takřka shodně.

Oblíbené e-mailové klienty pak jsou **Claris e-mailer**, **Eudora Light**, existuje i **Microsoft Outlook** pro Macintosh, v Office 2001 najdete **Microsoft Entourage**, výborně řešený e-mail je i součástí balíku **Netscape Communicator**.

Velice povedený a relativně recentní program pro provozování BBS je **Hermes II**, pracuje s Telnetovým i sériovým či modemovým připojením, takže BBS může být přístupná jak přes TCP/IP (Telnet), tak přes modem (terminál), a to i současně, a jeho nároky na systém jsou opět velice malé. Nástupcem BBS by mohl být systém **KDX**, vyžaduje ale systém 9.1 a navíc server a klient (který sám slouží jako server pro sdílení souborů a komunikaci mezi dvěma počítači) jsou programy placené.

Dobré telnetové klienty se jmenují **DataComet**, **NCSA Telnet**, **Better Telnet**, vznikly vylepšením předchozího, a **MacSSH**, vzniklý doplněním Better Telnetu o zabezpečení SSH. Z množství terminálů stojí za pozornost znovu **DataComet** a **Z-Term**.

Firewall vám poskytne **Socks** nebo **IPNetSentry**, další užitečné programy jsou **MacDNS** coby nameserver (vyžaduje ovšem PowerPC), **VICOM Internet Gateway**, **FreePPP** pro připojení k internetu přes modem, **IPNetRouter**, jehož jméno napovídá, že je určen k provozu routeru, umí ovšem i gateway, DHCP server, přepojování z Ethernetu a PPP na LocalTalk a IP maškarádu. Užitečné jsou i **IPNetTuner** a **IPNetMonitor**. Sdílení sériové zásuvky (u novějších strojů pak zabudovaného modemu) na jiném počítači umožní **SerialShare** ve spolupráci s utilitou **VICOM InterCom**.

X Window servery pro Mac jsou, jak bylo dříve zmíněno, **MacX** a **MI/X**.

Webových browserů existuje velký výběr, textové **Wannabe**, díle **Explorer**, **Netscape**, **iCab**, **Opera** a **Mozilla**, ke stahování celých webů poslouží specializovaný downloader **Lemon**.

Sdílet soubory s PC umožňují programy **DAVE**, **Goliath** a **PC-Mac-Net**, dále **Timbuktu**, které kromě sdílení souborů zabezpečuje i komunikaci a vzdálený přístup k ploše, podobně jako **VNC**, které ovšem nepodporuje sdílení souborů, zato existuje pro více platforem – posílání bitmap odněkud někam je ale dost pomalou metodou vzdáleného řízení počítače (na Macintoshi je lepší použít **Apple Remote Access**).

Ke sdílení souborů mezi více uživateli poslouží i **FileWave** a jako klient peer-to-peer sítě gnutella zase **LimeWire**, který je ale tvořen částečně v Javě a má tedy nehorázné systémové nároky (hlavně když se spouští).

Přístup na IRC (komunikace formou chatu s možností posílat soubory) umožní programy **ShadowIRC** a výborný **IRClE**.

Kromě oficiálního **ICQ**, které má dost náročné požadavky na výkon systému, existuje spolehlivý **Gerry's ICQ**.

Milovníci videokonferencí (a majitelé kamer) mohou využít **CUSeeMe**.

A pokud se vyznáte v AppleScriptu, můžete použít **Script Daemon**, ke kterému se připojíte pomocí Telnetu a on vám přes AppleScriptové příkazy umožní ovládat váš Macintosh (takto lze volat funkce naprosté většiny aplikací včetně samotného Finderu). Použití Script Daemonu je vázáno na znalost jména a hesla majitele počítače, nikdo jiný s ním (naštěstí) nic nesvede.

Nabízí se toho ovšem ještě mnohem víc.

Hacking

Původně jsem to vůbec nechtěl psát, ale už jsem se toho jednou dotkl a navíc, dnes je internet plný hloupých scriptů, které úmyslně (autor to tak schválně napsal) nebo neúmyslně (autor prostě jen nasekal chyby, které působí destruktivně) můžou ohrozit vaše servery, ať vám to přijde hloupé, nebo ne, spoléhat na lidský rozum a slušnost v prostředí, kam má přístup každý blbec, se nevyplácí.

Malá ukázka – server zxm.speccy.cz obsahoval script, který poskytoval jednotlivým dokumentům jednotný vzhled, stejnou hlavičku, stejné logo, stejná menu, jen vlastní obsah se lišil. Jediným vstupním parametrem scriptu bylo umístění neupraveného dokumentu.

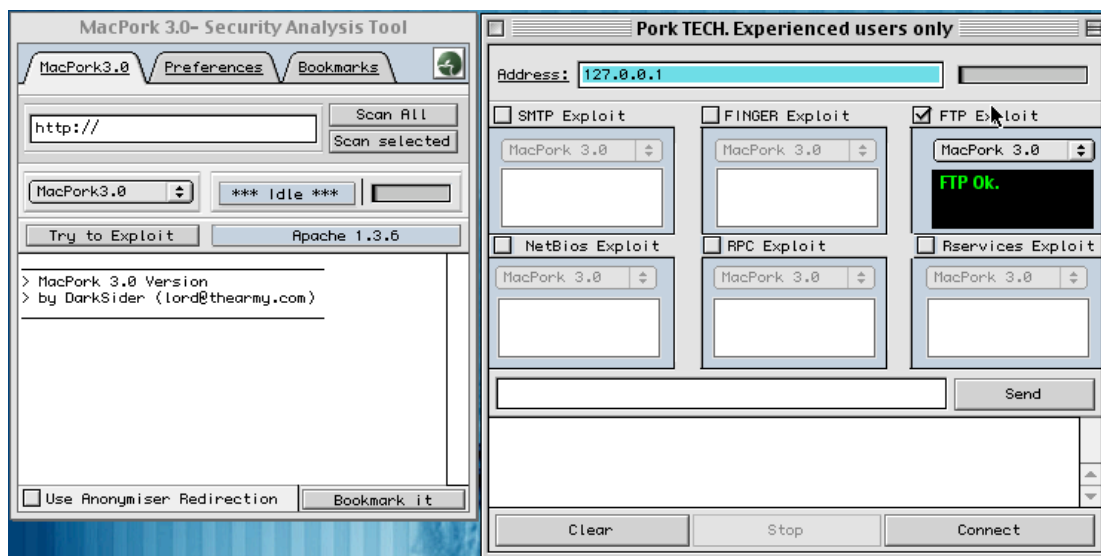
Je to nevinný scriptík, ale když se potká s nějakým blbcem, nebo scriptem nějakého blbce, ten nevinný to většinou odsere – v tomto případě to odnesla nejenom subdoména zxm, ale celá doména speccy. (protože se všemi svými subdoménami je umístěna fyzicky na jediném počítači). Někdo prostě začal bombardovat script parametry a s jeho pomocí scanovat obsah serveru, což server zahlcovalo. A to pravděpodobně vůbec nešlo o nějaký útok, jehož primárním účelem by bylo shození nebo zničení serveru.

Proto dříve, než to za vás (s mnohem horšími důsledky) udělá někdo jiný, otestujte a nastavte bezpečnost své sítě.

- Počátkem všeho je oscanovat si celý rozsah IP adres (Address Scan), který máte přidělen, je sice málo pravděpodobné, že najdete nějaký zapomenutý počítač nebo že se na vaši uvolněnou IP někdo napíchne, ale ověřte si, že se ozývají správné počítače se správnými jmény a že jim to netrvá.
- Ověřte si, že daná služba je dostupná jen na těch počítačích, které ji v daném segmentu sítě mají poskytovat (Service Scan), a to podle dostupnosti portu dané služby.
- Pak jeden po druhém proscanujte jednotlivé počítače, zda mají otevřeny jen ty porty, které nutně potřebují (Port Scan).

K tomu vám poslouží **AGNetTools** nebo **IPNetMonitor**, případně některý z "hackerských" programů, z nich Service Scan jako jediný nabízí **PowerScan**. Zřejmě nejrychlejší portscanner je **PortMasterX**, ten vám ovšem jen ukáže čísla portů a nesdělí už, jaká služba na tom kterém portu sídlí, což starší **PortMaster 3** umí. Program slavné hackerské skupiny UGM (**UGM Port Scanner**) je dost pomalý. Majitelům Mac OS X naopak kromě Mac OS X verze PortMasteru X dobře poslouží **Ordine** a milovníkům UNIXové příkazové řádky pak **CommandLineScanner**.

Velice komplexní nástroj, který prostě musím zmínit, je **MacPork**. Otestuje vám vaše počítače a síť opravdu komplexně, vyhledává díry ve vašem webovém serveru a testuje některé běžnější scripty, testuje počítač na přítomnost trojských koní, hledá chyby, umožňující ovládnutí počítače přes vzdálené přihlašování nebo Telnet, testuje odolnost proti přetečení bufferů, simuluje útoky na mailové servery... Umí toho opravdu hodně, určitě si ho vyzkoušejte.



Chcete-li otestovat svůj SMTP server, zkuste **CAEM 4**, je to výborný program, který umí nejen otestovat úroveň zabezpečení serveru, ale taky otestovat odolnost proti zahlcení velkým množstvím mailů, a umí i další věci.

Overdose je hackerský program, který útočí proti několika bezpečnostním dírám, z nich nejdůležitější je Sdílení WWW v MacOS 8.5, AppleShare IP Mail a ICQ 99a.

Z dalších útočných programů stojí za pozornost **GrouchySmurf** (zneužívá broadcastu k zahlcení), **Tsunami**, a máte-li v síti UNiXový stroj, bude vás zajímat **Session**, v přítomnosti PeCe s Windows zase **MacPuke**.

Základ obrany je tedy v tom, že

- na vašich počítačích běží opravdu jen ty programy a služby, které tam mají běžet, nic víc
- skripty a roboty jsou omezeny na nutné minimum, k cizím scriptům je nutno být nedůvěřivý, protože v nich může být některá ze známých děr
- na discích jsou správně nastavena přístupová práva, tedy anonymní uživatelé nemohou buď vůbec nikam, nebo jen do vyhrazené oblasti, chráněné proti zápisu
- oblastí určené k zápisu (upload), ať už koncipované jako dropboxy (uživatel neví, co v adresáři je, může do něj pouze něco přidat) nebo takové, jejichž obsah je vidět, by měly být na samostatném disku (ať už fyzicky, nebo na samostatné partition), aby v případě nějakého útoku, který má za cíl disk zaplnit, nedošlo k "utlačení" prostoru pro systém, dočasné soubory serverových aplikací, buffery a virtuální paměť na systémové partition
- distribuce služeb mezi několik počítačů znamená i rozptýlení rizika a omezení následků – počítač má otevřeny porty jen pro jednu službu, které může věnovat veškerý strojový čas, je tedy odolnější vůči floodům a útokům hrubou silou, i v případě pádu systému, proti kterému byl útok veden, pak ostatní služby zůstávají v provozu
- využití RAIC rovněž zvyšuje odolnost proti útoku hrubou silou, i v případě úspěchu útoku vůči jednomu ze strojů zůstává služba (alespoň dočasně) uživateli dostupná
- gateway a IP maškaráda (**VICOM Internet Gateway**, **IPNetRouter**) působí jako firewall, je-li počítač zvenčí neviditelný, obtížně se proti němu vede útok
- předpokládáme-li použití klientů kompatibilních se SOCKS protokolem, použití tohoto firewallu výrazně zvýší bezpečnost vnitřní sítě
- síť by měla být monitorována a zvláštní aktivity zalogovány pro pozdější kontrolu administrátorem – aktuální stav celého segmentu si ověříte například utilitou **MacPing** (neplette si ji s utilitou MacTCP Ping, která je součástí systému), zvláště účinné je použití programů **IPNetSentry**, který monitoruje dění na síti, hlásí útoky a před některými i ochrání, ve spojení s **IPNetMonitorem**, který používá k vysledování útočnicka, **IPNetSentry** navíc slouží i jako firewall, umí povolit přístup z určitých adres, přístup na určité služby, umožní naklást několik jednoduchých pastí (monitorovat šedesát nevyužitých portů, monitorovat časté zasílání datagramů, pátrat po textovém řetězci, typickém pro některého červa), a s utilitou **IPNetAuthorize** umožní autorizovaným osobám přístup do vnitřní sítě i z pohyblivé IP adresy
- síť by měla být zapojena a nastavena tak, aby podávala maximální výkon – i to je totiž bezpečnostní faktor, k nastavení parametrů poslouží třeba **IPNetTuner**, stroje se stomegabitovým Ethernetem by měly být zapojeny v páteři, desetimegabitové nejlépe přes jeden z nich jako bránu do pomalejší části sítě, podobně dvoumegabitové a LocalTalkové stroje
- nemělo by se spoléhat na inteligenci strojů, byť sebelepších a sebevýkonnějších či sebekrásnějších, protože ta je jen ve sci-fi pohádkách, všechno by měl zkontrolovat a prověřit nějaký lépe uvažující člověk, přičemž na monitorování a řízení sítě by měl mít k dispozici samostatný počítač

Příloha 1:
Seznam nejdůležitějších TCP portů

20 ftp-data - File Transfer [Default Data]
21 ftp - File Transfer [Control]
23 telnet
24 any private mail system
25 smtp - Simple Mail Transfer
27 nsw-fe - NSW User System FE
29 msg-icp
31 msg-auth - MSG Authentication
33 dsp - Display Support Protocol
35 any private printer server
37 time
38 rap - Route Access Protocol
39 rlp - Resource Location Protocol
41 graphics
42 nameserver - Host Name Server
43 nickname - Who Is
44 mpm-flags - MPM FLAGS Protocol
45 mpm - Message Processing Module [recv]
46 mpm - Message Processing Module [default send]
47 ni-ftp
48 auditd - Digital Audit Daemon
49 login - Login Host Protocol
50 re-mail-ck - Remote Mail Checking Protocol
51 la-maint - IMP Logical Address Maintenance
52 xns-time - XNS Time Protocol
53 domain - Domain Name Server
54 xns-ch - XNS Clearinghouse
55 isi-gl - ISI Graphics Language
56 xns-auth - XNS Authentication
57 any private terminal access
58 xns-mail - XNS Mail
59 any private file service
61 ni-mail
62 acas - ACA Services
64 covia - Communications Integrator (CI)
65 tacacs-ds - TACACS-Database Service
67 bootps - Bootstrap Protocol Server
68 bootpc - Bootstrap Protocol Client
69 tftp - Trivial File Transfer
70 gopher
71 netrjs-1 Remote Job Service
72 netrjs-2 Remote Job Service
73 netrjs-3 Remote Job Service
74 netrjs-4 Remote Job Service
75 any private dial out service
76 deos - Distributed External Object Store
77 any private RJE service
78 vettp
79 finger
80 www-http - World Wide Web HTTP
81 host2-ns - HOSTS2 Name Server

- 82 xfer - XFER Utility
- 83 mit-ml-dev
- 84 ctf - Common Trace Facility
- 85 mit-ml-dev
- 86 mfcobol - Micro Focus Cobol
- 87 any private terminal link
- 88 kerberos
- 89 su-mit-tg - SU/MIT Telnet Gateway
- 90 dnsix - DNSIX Security Attribute Token Map
- 91 mit-dov - MIT Dover Spooler
- 92 npp - Network Printing Protocol
- 93 dcp - Device Control Protocol
- 94 objcall - Tivoli Object Dispatcher
- 95 supdup
- 96 dixie - DIXIE Protocol Specification
- 97 swift-rvf - Swift Remote Virtual File Protocol
- 98 tacnews
- 99 metagram - Metagram Relay
- 100 newacct - [unauthorized use]
- 101 hostname - NIC Host Name Server
- 102 iso-tsap
- 103 gppitnp - Genesis Point-To-Point Trans Net
- 104 acr-nema - ACR-NEMA Digital Imag. & Comm. 300
- 105 csnet-ns - Mailbox Name Nameserver
- 106 3com-tsmux
- 107 rtelnet - Remote Telnet Service
- 108 snagas - SNA Gateway Access Server
- 109 pop2 - Post Office Protocol - Version 2
- 110 pop3 - Post Office Protocol - Version 3
- 111 sunrpc - SUN Remote Procedure Call
- 112 mcidas - McIDAS Data Transmission Protocol
- 113 auth - Authentication Service
- 114 audionews - Audio News Multicast
- 115 sftp - Simple File Transfer Protocol
- 116 ansanotify - ANSA REX Notify
- 117 uucp-path - UUCP Path Service
- 118 sqlserv - SQL Services
- 119 nntp - Network News Transfer Protocol
- 120 cfdpckt
- 121 erpc - Encore Expedited Remote Pro.Call
- 122 smakynet
- 123 ntp - Network Time Protocol
- 124 ansatrader - ANSA REX Trader
- 125 locus-map - Locus PC-Interface Net Map Ser
- 126 unitary - Unisys Unitary Login
- 127 locus-con - Locus PC-Interface Conn Server
- 128 gss-xlicen - GSS X License Verification
- 129 pwdgen - Password Generator Protocol
- 130 cisco-fna - cisco FNATIVE
- 131 cisco-tna - cisco TNATIVE
- 132 cisco-sys - cisco SYSMOINT
- 133 statsrv - Statistics Service
- 135 loc-srv - Location Service
- 136 profile - PROFILE Naming System

137 netbios-ns - NETBIOS Name Service
138 netbios-dgm - NETBIOS Datagram Service
139 netbios-ssn - NETBIOS Session Service
140 emfis-data - EMFIS Data Service
141 emfis-cntl - EMFIS Control Service
142 bl-idm - Britton-Lee IDM
143 imap2 - Interim Mail Access Protocol v2
144 news
145 uaac
146 iso-tp0
147 iso-ip
148 cronus - CRONUS-SUPPORT
149 aed-512 - AED 512 Emulation Service
150 sql-net
151 hems
152 bftp - Background File Transfer Program
153 sgmp
154 netsc-prod
155 netsc-dev
156 sqlsrv - SQL Service
157 knet-cmp - KNET/VM Command/Message Protocol
158 pmail-srv - PCMail Server
159 nss-routing
160 sgmp-traps
161 snmp - Simple Network Management Protocol
162 snmptrap - Simple Network Management Protocol
Trap
163 cmip-man - CMIP/TCP Manager
164 cmip-agent - CMIP/TCP Agent
165 xns-courier - Xerox
166 s-net - Sirius Systems
167 namp
168 rsvd
169 send
170 print-srv - Network PostScript
171 multiplex - Network Innovations Multiplex
172 cl/1 - Network Innovations CL/1
173 xyplex-mux - Xyplex
174 mailq
175 vmnet
176 genrad-mux
177 xdmcp - X Display Manager Control Protocol
178 nextstep - NextStep Window Server
179 bgp - Border Gateway Protocol
180 ris - Intergraph
181 unify
182 audit - Unisys Audit SITP
183 ocbinder
184 ocserver
185 remote-kis
186 kis - KIS Protocol
187 aci - Application Communication Interface
188 mumps - Plus Five's MUMPS
189 qft - Queued File Transport

190 gacp - Gateway Access Protocol
191 prospero - Prospero Directory Service
192 osu-nms - OSU Network Monitoring System
193 srmp - Spider Remote Monitoring Protocol
194 irc - Internet Relay Chat
195 dn6-nlm-aud - DNSIX Network Level Module
Audit
196 dn6-nlm-red - DNSIX Session Mgt Module Audit
Redir
197 dls - Directory Location Service
198 dls-mon - Directory Location Service Monitor
199 smux
200 src - IBM System Resource Controller
201 at-rtmp - AppleTalk Routing Maintenance
202 at-nbp - AppleTalk Name Binding
203 at-3 - AppleTalk Unused
204 at-echo - AppleTalk Echo
205 at-5 - AppleTalk Unused
206 at-zis - AppleTalk Zone Information
207 at-7 - AppleTalk Unused
208 at-8 - AppleTalk Unused
209 tam - Trivial Mail Authentication Protocol
210 z39.50
211 914c/g - Texas Instruments 914C/G Terminal
212 anet - ATEXSSSTR
213 ipx
214 vmpwscs - VM PWSCS
215 softpc - Insignia Solutions
216 atls - Access Technology License Server
217 dbase - dBASE Unix
218 mpp - Netix Message Posting Protocol
219 uarps - Unisys ARPs
220 imap3 - Interactive Mail Access Protocol v3
221 fln-spx - Berkeley rlogind with SPX auth
222 rsh-spx - Berkeley rshd with SPX auth
223 cdc - Certificate Distribution Center
243 sur-meas - Surveet Measurement
245 link
246 dsp3270 - Display Systems Protocol
344 pdap - Prospero Data Access Protocol
345 pawserv - Perf Analysis Workbench
346 zserv - Zebra server
347 fatserv - Fatmen Server
348 csi-sgwp - Cabletron Management Protocol
371 clearcase
372 ulistserv - Unix Listserv
373 legent-1 - Legent Corporation
374 legent-2 - Legent Corporation
375 hassle
376 nip - Amiga Envoy Network Inquiry Proto
377 tnETOS - NEC Corporation
378 dsETOS - NEC Corporation
379 is99c - TIA/EIA/IS-99 modem client
380 is99s - TIA/EIA/IS-99 modem server

381 hp-collector - hp performance data collector
382 hp-managed-node - hp performance data managed node
383 hp-alarm-mgr - hp performance data alarm manager
384 arns - A Remote Network Server System
385 ibm-app - IBM Application
386 asa - ASA Message Router Object Def.
387 aurp - AppleTalk Update-Based Routing Pro.
388 unidata-ldm - Unidata LDM Version 4
389 ldap - Lightweight Directory Access Protocol
390 uis
391 synotics-relay - SynOptics SNMP Relay Port
392 synotics-broker - SynOptics Port Broker
Port
393 dis - Data Interpretation System
394 embl-ndt - EMBL Nucleic Data Transfer
395 NETscout Control Protocol
396 netware-ip - Novell Netware over IP
397 mptn - Multi Protocol Trans. Net.
398 kryptolan
400 work-sol - Worksation Solutions
401 ups - Uninterruptible Power Supply
402 genie - Genie Protocol
403 decap
404 nced
407 timbuku
408 prm-sm - Prospero Resource Manager Sys. Man.
409 prm-nm - Prospero Resource Manager Node Man.
410 decladebug - DECLadebug Remote Debug Protocol
411 rmt - Remote MT Protocol
412 synoptics-trap - Trap Convention Port
413 smsp
414 infoseek
415 bnet
416 silverplatter
417 onmux
418 hyper-g
419 ariel1
420 smpte
421 ariel2
422 ariel3
423 opc-job-start - IBM Operations Planning and Control Start
424 opc-job-track - IBM Operations Planning and Control Track
425 icad-el - ICAD
426 smartsdp
427 svrloc - Server Location
428 ocs_cmu
429 ocs_amu
430 utmpsd
431 utmpcd
432 iasd
433 nnsdp
434 mobileip-agent

435 mobileip-mn
436 dna-cml
437 comscm
438 dsfgw
439 dasp
440 sgcp
441 decvms-sysmgt
442 cvc_hostd
443 https
444 snpp - Simple Network Paging Protocol
445 microsoft-ds
446 ddm-rdb
447 ddm-dfm
448 ddm-byte
449 as-servermap - AS Server Mapper
450 tserver
497 retrospect - Retrospect Backup software
515 printer - spooler
517 talk
518 ntalk
525 timed - timeserver
526 tempo - newdate
548 AppleShare IP Server
1080 wingate
2140 depthroath
3000 firstClass
5500 hotline
5501 hotline
6665 irc
6666 irc
6667 irc
6668 irc
6669 irc
6700 Carracho
7000 IRC
8080 http
12345netbus
27374Sub7
31337BO