UNIVERZITA PALACKÉHO V OLOMOUCI
Přírodovědecká fakulta
Katedra fyzikální chemie

INTERNET A ZDROJE

Tomáš Zelený, Petr Jakubec, Libor Kvítek
Učební texty pro distanční studium

Olomouc, 2013

Obsah

Úvod

Vážený čtenáři,

tento distanční text seznamuje čitatele se základy Internetových technologií. Cílem je, aby po prostudování textu byl schopen samostatně řešit některé základní problémy související s funkčností malé počítačové sítě a obslužných programů pro základní informační služby Internetu. Text je tak zaměřen na základní problematiku výstavby a nastavení malé počítačové sítě, ale i na bližší výklad informačních služeb Internetu. Probrány jsou jak ty nejjednodušší služby, jako je služba přenosu souborů FTP, tak i služby složitější, zejména služba elektronické pošty a především služba WWW (World Wide Web). V rámci služby WWW jsou navíc probrány základy tvorby hypertextových dokumentů publikovatelných na Internetu za pomocí typických prvků jazyka HTML.

Cílová skupina:

Tento učební text je primárně určen studentům druhého ročníku bakalářského studijního programu oboru Aplikovaná chemie na Přírodovědecké fakultě Univerzity Palackého v Olomouci jako studijní opora k předmětu Internet a zdroje. Použitelný je však i pro další studenty neinformatických oborů, kteří chtějí zlepšit své znalosti o Internetových technologiích a zdokonalit svou práci s nimi.

Autoři

Část I

Počítačové sítě – hardware a nastavení

Každý pokročilý uživatel počítačových technologií a Internetu je jednoho dne postaven před problém zvládnutí základní hardwarové a softwarové instalace prostředků a služeb, které mu umožní dokonalejší využití prvků počítačových technologií skrytých před prostým uživatelem, který pouze dané technologie používá, ale neovládá. Pojďme se tedy podívat, jaké základní technické požadavky je třeba splnit při výstavbě malé počítačové sítě.

Kapitola 1

Hardwarové prostředky výstavby počítačových sítí

Hardware - fyzické součásti počítačů a počítačových sítí - budí u počítačových laiků velký respekt a obavu ze zásahu, který z funkčního počítače udělá nepotřebnou hromádku kovu a plastu. Naštěstí rychlý technologický vývoj nejen počítačového hardwaru, ale i základních softwarových prostředků pro jeho nastavení a diagnostiku umožňuje poměrně bezpečné experimentování se součástmi počítače a počítačových sítí i člověku bez titulu elektroinženýra.

1.1 Základní dělení sítí podle schématu jejich výstavby

A) podle rozlehlosti - již zmíněné typy LAN, MAN a WAN (kapitola 4.1.1).
B) podle topologie

Sběrnice (BUS) - počítače navzájem propojeny koax. kabelem (sběrnicí) za sebou (obrázek 2a), což přináší mnoho nevýhod (přerušení v jediném místě vyřadí celou síť, omezený počet uzlů a vzdálenost mezi nimi, použití jen pro pomalé sítě) a jedinou výhodu - nízké pořizovací náklady. Pro uvedené nevýhody se prakticky již nepoužívá.

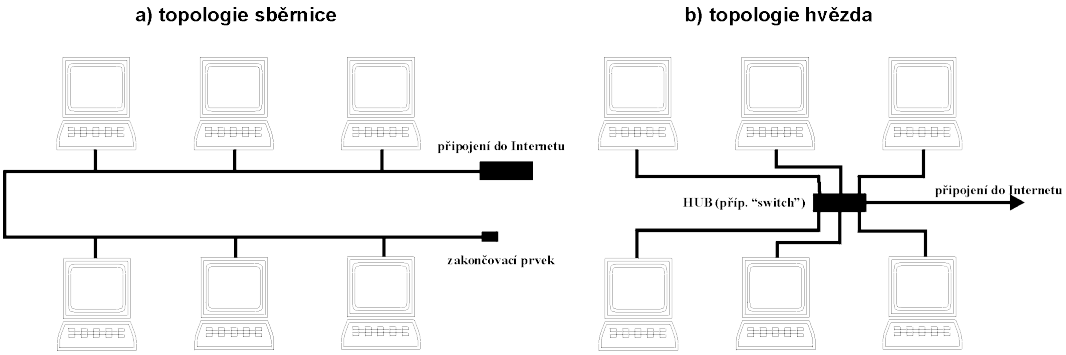
Hvězda (Star) - každý počítač připojen samostatným kabelem k aktivnímu prvku, to je např. rozbočovač (HUB) nebo výhodněji přepínač (obrázek 2b); propojení provedeno kroucenou dvojlinkou. Jediná nevýhoda oproti předchozímu řešení - vyšší pořizovací cena - je vyvážena mnohými výhodami - při poruše jednoho vedení ostatní dále funkční, propojením rozbočovačů do kaskády lze vytvořit i rozlehlejší síť a hlavně je použitelná i pro rychlejší sítě typu typu Ethernet, Token Ring, FDDI, ATM a proto je v současnosti nejpoužívanějším zapojením pro lokální sítě.

Kruh (Ring) - počítače propojeny do uzavřené smyčky, málo používaný typ zapojení.

Strom (Tree) - propojení lokálních sítí do sítí většího rozsahu.

C) podle architektury
Klient-server - jeden z počítačů řídí funkce sítě (server) ostatní využívají jeho prostředků a služeb (pracovní stanice); vhodný pro střední a velké sítě

Peer-to-Peer - neexistuje zde nadřazený počítač, vhodný pro malé sítě



Obrázek 1.1: Topologie sítí.

1.2 Sítě typu Ethernet

„Klasický“ Ethernet (max. přenosová rychlost 10 Mbit/s)

10Base-2 - tento typ sítě používá tenký koaxiál černé barvy o impedanci 50 ? (Thin Ethernet). Délka segmentu je max. 185 m a lze připojit max. 25 počítačů. Vedení musí být na obou koncích zakončeno terminátory (odpory 50 ?). Počítače propojeny přímo přes BNC konektory na síťové kartě. Dnes již zřídka používaná varianta stavby sítí. 10Base-T - počítače jsou připojeny kroucenou dvojlinkou (Twisted Pair = TP) s konektorem RJ45 (obdobný telefonnímu) přímo k rozbočovači (max. 100 m). Podle typu rozbočovače lze připojit do jednoho segmentu sítě až 24 počítačů, resp. přes kaskádu až 4 rozbočovačů tento počet znásobit.

Fast Ethernet (max. přenosová rychlost 100 Mbit/s)

100Base-TX je obdobou 10Base-T, ovšem hardware plně podporuje vyšší přenosovou rychlost. Dnes nejpoužívanější pro výstavbu LAN.

100Base-FX používá mnohavidový optický kabel, přičemž délka jednoho segmentu může dosahovat až 2 km bez zesílení..

Gigabit Ethernet (max. přenosová rychlost 1000 Mbit/s)

1000Base-SX používá mnohavidové optické kabely. Max. délka segmentu podle použitého optického vlákna 275 až 550 m.

1000Base-LX lze používat i jednovidový optický kabel, max. délka segmentu je pak až 5 km.

1000Base-CX používá stíněné kabely, max. délka segmentu je pouze 25 m.

1.3 Používané typy síťových karet

Síťové karty plní funkci síťového rozhranní (NIC = Network Interface Adapter). Dělí se podle použitého typu sběrnice (ISA, PCI, USB PCMCIA), podle typu konektorů pro připojení do sítě (BNC, RJ45, Combo) a podle přenosové rychlosti (10 nebo 100 Mb/s).

Průvodce studiem

Protože tento text poskytuje pouze základní informace o Internetových technologiích, nemůžeme se zde podrobněji věnovat problematice výstavby počítačových sítí. Mimo zde uvedené nejzákladnější možnosti existují další typy sítí, ať již z hlediska topologie, tak i z hlediska technologie jejich prvků. Podrobnější informace lze získat v doporučené literatuře, např. v knize Širokopásmový Internet z nakladatelství Computer Press.

1.4 Další stavební prvky malých počítačových sítí

Rozbočovač (Hub) - signál po zesílení rozešle všem dalším připojeným počítačům. Portů (přípojných míst) mívá obvykle 5, 8, 12, 16 nebo 24; jeden z těchto portů má obvykle překřížené zapojení a slouží ke kaskádovému zapojení dalšího rozbočovače (max. 4).

Přepínač (Switch) - je to vlastně multiportový most, který umožňuje komunikaci mezi různými dvojicemi portů (segmenty sítě). Často se používá ve funkci rozbočovače.

Opakovač (Repeater) - zesilovač sloužící k prodloužení kabeláže.

Převodník (Converter) - převádí signál mezi různými typy kabelů (obvykle signál nezesiluje).

1.5 Bezdrátové sítě

Prakticky všechny bezdrátové sítě využívají k přenosu informace elektromagnetického vlnění **Bezdrátové sítě lze nejjednodušeji třídit dle jejich dosahu:**

- Dosah několik metrů - Bluetooth (BT), Infračervené spojení (IRDA) nebo nově i Near Field Communication (NFC).
- Dosah v řádu metrů až kilometrů - Wi-Fi, WiMax.
- Dosah v řádu kilometrů - Mobilní sítě (GSM, PCS, D-AMPS), pokrytí satelitním signálem.

1.5.1 WiFi

WiFi (rovněž WLAN[1]) jsou bezdrátové sítě založené na standardech IEEE 802.11.[2] Nyní se používají v řadě přenosných zařízení jako jsou chytré mobilní telefony, tablety, notebooky apod. Zařízení se připojují k tzv. přístupovému bodu (access point; hot spot), což je blízké filozofii připojení klient–server. Druhý způsob propojení dvou zařízení, které v síti vystupují jako rovnocenné je založen na peer-to-peer přístupu nazývaném u WiFi sítí Ad-hoc (méně častý). V budovách je dosah WiFi přibližně 20 m, ve volných prostorech je dosah větší. WiFi pracuje v bezlicenčním pásmu ISM (2.6 GHz).

1.5.1.1 Zabezpečení

WiFi síť je možné zabezpečit mnoha různými způsoby:

Schování SSID Každá síť vysílá svoje SSID jako broadcast, které ji rozlišuje od jiných WiFi sítí. Pokud je vysílání SSID zakázáno, pak se připojí jen ten, kdo jej zná. Na routeru nastavíme volbu Hide SSID na YES.

[1] WLAN — Wireless Local Area Network.
[2] IEEE — Institute of Electrical and Electronics Engineers.

MAC filtering Každá síťová karta má svoje unikátní číslo, nazývající se MAC adresa (Media Access Control). Do routeru zadáme MAC adresy všech zařízení, které chceme připojovat a ostatní zakážeme. Pokud k nám nechodí často návštěvy, které by se připojovaly k internetu, je to dobrá volba.

Šifrování

- WEP (Wired Equivalent Privacy) – šifrovací protokol s tajným klíčem o velikosti 40 nebo 104 bitů kombinovaným s 24 bitovým inicializačním vektorem (IV), pro ověření správnosti používá metodu CRC-32 kontrolního součtu. 64 bitový WEP je kombinace 40 bitového klíče a 24 bitového IV, 128 bitový WEP je 104 bitový klíč a 24 bitový IV. WEP je díky zranitelnosti šifrovacího algoritmu RC4, délce klíče a kolizím IV lehce překonatelnou ochranou a jeho použití se nedoporučuje ani v domácnosti.
- WPA (Wi-Fi Protected Access) – stejně jako u WEP je použit šifrovací algoritmus RC4, ale s 128 bitovým klíčem a 48 bitovým inicializačním vektorem (IV). Zásadní vylepšení však spočívá v dynamicky se měnícím klíči – TKIP (Temporal Key Integrity Protocol). Je vylepšena také kontrola integrity (správnosti) dat - díky použití metody označující se jako MIC (Message-Integrity Check). WPA nabízí více možností, jak síť zabezpečit a to buď pomocí autentizačního serveru (RADIUS), který zasílá každému uživateli jiný klíč (podnikové řešení) nebo pomocí PSK (Pre-Shared Key), kdy každý uživatel má stejný přístupový klíč (malé podnikové sítě nebo domácnosti).
- WPA2 – je použit protokol CCMP (Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol) se silným šifrováním AES (Advanced Encryption Standard), MAC (Message Authentication Code) dynamicky mění 128 bitový klíč, MIC pro kontrolu integrity a ochranu proti útokům snažící se zopakovat předchozí odposlouchanou komunikaci (replay). Existují i další metody zabezpečení, jako EAP ověřování pod WPA/WPA2 Enterprise, určené pro silné zabezpečení podnikových bezdrátových sítí.

1.5.2 Mobilní sítě

Mobilní sítě (u nás především GSM) se k připojení k internetu začaly používat teprve relativně nedávno.

První použitelnou technologií pro prohlížení upravených webových stránek byla služba WAP (Wireless Application Protocol) v roce 1998. Webové stránky se speciálně pro WAP buď přímo vytvářely, nebo pomocí speciálního proxy serveru (WAP gateway) se převáděly běžné webové stránky pro WAP prohlížeč v mobilním telefonu.

1.5.3 Satelitní sítě

Také prostřednictvím satelitního připojení lze přenášet data. V České republice je několik málo poskytovatelů připojení k Internetu prostřednictvím satelitního připojení (GiTySAT). Připojení je poměrně drahé, ale lze jej používat kdekoliv kde není jiný poskytovatel (mobilní sítě).

Shrnutí

Počítačové sítě lze třídit podle mnoha kritérií, nejběžnější je třídění podle jejich rozlehlosti, topologie a architektury. Základními stavebními prvky počítačových sítí jsou mimo propojovacích kabelů síťové karty, rozbočovače a přepínače. Nejběžnějším standardem malých počítačových sítí je síť typu Ethernet, jehož jednotlivé podtypy se liší přenosovou rychlostí.

Pojmy k zapamatování

- topologie sítí - sběrnice, hvězda, kruh, strom
- architektura sítí - klient-server, peer-to-peer
- Ethernet - klasický, Fast Ethernet, Gigabit Ethernet
- síťová karta, rozbočovač, přepínač

Kontrolní otázky

1. Popiš systém zapojení počítačů v LAN podle topologie typu sběrnice a hvězda.
2. Jaký je rozdíl mezi architekturou klient-server a peer-to-peer?
3. Jaký účel plní síťová karta?
4. Jaký je rozdíl mezi přepínačem a rozbočovačem?

Kapitola 2

Instalace síťového softwaru a jeho konfigurace v OS MS Windows

Mimo nutný hardware je třeba pro zprovoznění připojení počítače do sítě nainstalovat nutný software:

- Klient - síťový klient provádí přihlášení počítače do sítě a zajišťuje podmínky pro komunikaci mezi počítači v síti.
- Adaptér - ovladač síťové karty (zabezpečuje součinnost síťové karty s OS).
- Protokol - komunikační jazyk mezi počítači v síti (je možné instalovat více protokolů současně).
- Služba - síťové služby (např. sdílení souborů či tiskáren).

OS MS Windows podporují plně technologii „plug and play“, takže po fyzické instalaci síťové karty a zapnutí počítače detekují její přítomnost a pokud mají daný typ v databázi, nainstalují i příslušný ovladač. Pokud máme ale ovladač k dispozici od výrobce, je lepší instalovat tento ovladač (obzvláště, je-li novějšího data). O správnosti instalace a nainstalovaných součástech lze získat informace ve složce Ovládací panely pod ikonou Síťová a telefonická připojení - Připojení místní sítě. Přesvědčíme se hlavně zda je mimo ovladače síťové karty nainstalován protokol TCP/IP, nezbytný pro používání sítě Internet. Ten je ovšem nutné nainstalovat před prvním použitím sítě při instalaci OS, resp. samostatně spuštěním Průvodce vytvoření připojení.

2.1 Vytvoření nového připojení k místní síti LAN

Po stisku tlačítka Start na hlavní liště vybereme složku Ovládací panely a v ní pak složku Síťová a telefonická připojení. Její součástí je mimo jiné Průvodce vytvoření připojení, pro jednoduché nastavení parametrů nově zavedeného připojení k síti.

V prvém konfiguračním okně se průvodce ptá, zda je počítač připojen k síti - to se mu oznámí zatržením políčka s názvem Tento počítač je součástí podnikové sítě a je používán k připojení dalších počítačů v práci. V dalším okně se rozliší architektura sítě - dělení na pracovní skupiny či domény. Volba Společnost používá síť bez domény vede rychle ke konci

pouhým zadáním jména pracovní skupiny. Nastavení pro případ odpovědi Společnost používá síť s doménou je již složitější. V následujících oknech je totiž třeba zadat Uživatelské jméno (název účtu v rámci dané domény - nemusí zatím existovat, jde vytvořit později), Heslo a název existující Domény, do které se budeme přihlašovat. Pokud po zadání nenalezne průvodce daný účet na zadaném doménovém serveru, lze v dalším okně vyhledat existující účet počítače na jiném doménovém serveru po zadání Název počítače a Doména počítače, kde tento počítač je skutečně zaregistrovaný (domény účtu uživatele a počítače se nemusí shodovat). Dále se konfigurace vyvíjí podle toho, zda zadaný účet uživatele již byl na lokálním počítači nadefinován nebo ne. Pokud ano, konfigurace končí, pokud ne, pokračuje se vytvořením účtu uživatele na našem lokálním počítači. V položce Přidat následujícího uživatele je třeba vyplnit Uživatelské jméno a Doména uživatele vše shodné s vytvářeným účtem uživatele v dané doméně. Ovšem účet uživatele na daném lokálním počítači není třeba vytvářet, pak se zaškrtne políčko Dalšího uživatele již nepřidávat. Další okno pak umožní pro vytvořený účet na lokálním počítači nastavit přístupová práva ve třech stupních - Uživatel se standardním oprávněním, Uživatel s omezeným oprávněním a Jiná (individuálně nastavitelná přístupová práva). Tím konfigurace identifikace v síti končí. Nutno podotknout, že uvedené operace musí být prováděny z účtu s oprávněním typu Administrator a provedené změny vejdou v platnost až po restartu počítače.

Průvodce studiem

Všechny probírané postupy si současně vyzkoušejte ve vašem počítači, protože orientace v jednotlivých položkách nastavení připojení počítače k lokální síti a k Internetu je v některých místech Průvodce nastavení připojení nepřehledná. Ovšem nesmíte být přihlášeni jako uživatelé s omezeným oprávněním (najdete v Ovládacích panelech ve složce Uživatelské účty), pak nelze do nastavení síťového připojení ani nahlížet, natož něco nastavovat. Nemusíte mít obavy z narušení nastavení síťových připojení, pokud skutečně vytvoříte nové připojení - to lze okamžitě zrušit. Ovšem pokud takovou činnost děláte poprvé, odpojte raději počítač od sítě, nebo alespoň minimálně od Internetu.Podrobný postup pro začínající uživatele opět poskytuje doporučená literatura, např. kniha z nakladatelství Computer Press Připojujeme se k Internetu od L. Dostálka, či další kniha ze stejného nakladatelstvís názvem Stavíme si malou síť ve Windows XP a 2000 od A. Kostrhouna.

2.2 Konfigurace jednotlivých síťových komponent

K jednotlivým konfiguračním položkám se lze dostat opět přes složku Síťová připojení, kde vybereme nainstalované připojení k místní síti, u nějž tlačítkem Vlastnosti vyvoláme přehled všech nainstalovaných síťových komponent včetně možnosti změn jejich nastavení.

- Konfigurace síťového adaptéru - v tomto případě prakticky nelze nic konfigurovat. Stačí se přesvědčit zda nainstalovaný typ adaptéru odpovídá instalované síťové kartě případně je nainstalován nejaktuálnější ovladač této karty.
- Konfigurace protokolu TCP/IP - na záložce Adresa IP je třeba zaškrtnout políčko Získat adresu IP ze serveru DHCP, pokud je počítač připojen do sítě, kde existuje DHCP server. Pokud tomu tak není, je třeba zadat IP adresu ručně a to např. adresu třídy C tak, aby nekolidovala s adresou jiného počítače v naší síti (např. 192.192.1.1). Do pole Maska podsítě pak zadáme typickou masku pro IP adresu třídy C, tedy 255.255.255.0.
- Dále postačuje nastavení adresy serveru DNS resp. WINS, které se získají buď automaticky nebo musíme znát jejich skutečnou IP adresu (u LAN nepřipojené do Internetu není třeba).

- Další konfigurační možnosti skryté pod tlačítkem Upřesnit není třeba vyvolávat, protože až na výjimečné případy vyhovuje jejich automatické nastavení.
- Konfigurace Klient sítě Microsoft - tato služba se nastavuje za pomoci Průvodce instalací sítě, kde je se nastaví pouze správné jméno pracovní skupiny.
- Konfigurace služby Sdílení souborů a tiskáren v sítích Microsoft - přímo u složek sdílených prostředků v položce Sdílení lze nastavit způsob sdílení - v případě HDD buď jen čtení nebo úplný přístup. Samotné sdílení je pak umožněno pouze definovaným uživatelům. Podstatně bezpečnější je ovšem umožnit pouze sdílení složky Sdílené dokumenty, kam umístíme ty dokumenty, které chceme sdílet s ostatními v LAN.

2.3 Základní utility pro kontrolu funkčnosti sítě

Utilita IPconfig podává informace o aktuálním nastavení parametrů TCP/IP protokolu, zejména IP adresy (důležité v případě jejího dynamického přidělování DHCP serverem). Program pracuje opět v textovém režimu a výpis použitelných parametrů lze získat po zadání příkazu `ipconfig /?`.

Ping je základní utilita pro ladění sítí s protokolem TCP/IP (je jeho součástí). Jedná se o testovací program, který po spuštění vysílá testovací data na zadanou adresu a poté čeká na potvrzení jejich přijetí. Program pracuje v textovém módu, dostupné parametry zobrazí příkaz `ping /?`.

Samotný program se spouští v příkazovém řádku zadáním svého jména s IP adresou kontaktovaného počítače nebo přímo jeho jménem:

```
1  C:\ ping 192.168.1.99
2
3  C:\ ping aix.upol.cz
```

Tracert je utilita přímo obsaženou v protokolu TCP/IP, sloužící obdobně jako Ping k testování funkčnosti sítě. Program rovněž pracuje v textovém módu. Jeho parametry jsou dostupné po spuštění programu bez cílové adresy. Ta se zadává opět v číselné nebo jmenné podobě.

```
1  C:\ tracert 192.168.1.99
2
3  C:\ tracert aix.upol.cz
```

Na rozdíl od utility Ping utilita Tracert umí zobrazit cestu, kterou se vyslaná data pohybují. Tak lze objevit, zda závada v síti je někde na trase nebo až u cílového počítače. Existují samozřejmě dokonalejší možnosti trasování cesty informace po Internetu, ale pro účely testování sítě tato utilita naprosto dostačuje.

Shrnutí

Připojení počítače do Internetu zahrnuje řadu operací souvisejících jak s instalací HW prvků počítače a počítačové sítě, tak i SW prvků, jako je ovladač síťové karty či protokol pro komunikaci v síti a Internetu. I když pro každý OS jsou tyto postupy v detailech specifické, základní požadavky realizace jsou na typu počítače a jeho OS nezávislé.

Pojmy k zapamatování

- připojení k místní síti LAN
- konfigurace připojení
- kontrola funkčnosti připojení - IPConfig, Ping, Tracert

Kontrolní otázky

1. Kde v OS MS Windows najdeme položku pro vytvoření nového připojení do LAN?
2. Jaká je základní podmínka správné konfigurace protokolu TCP/IP?
3. Jaké jednoduché pomůcky nabízí protokol TCP/IP pro kontrolu funkčnosti sítě?

Kapitola 3

Připojení sítě LAN k Internetu

Přístup na Internet poskytují specializované firmy (providers - poskytovatelé, zprostředkovatelé), které na základě smlouvy umožní uživatelům připojení ke svému počítači (uzlu), který je součástí sítě Internet. Tato služba je zpoplatněna, i když v případě připojení soukromých osob je obvykle vlastní poplatek za připojení ukryt v poplatcích majiteli linek (drátových či bezdrátových), s jejichž pomocí se uživatel připojuje k uzlu providera.

Existují v podstatě čtyři způsoby připojení:

- pomocí vytáčené telefonní linky (dial up)
- pomocí pevné linky (klasická kovová, optický kabel, ISDN, DSL)
- bezdrátové připojení (mikrovlny, satelitní spojení)
- pomocí mobilního telefonu

Donedávna nejrozšířenější typ připojení využívá klasickou telefonní linku a modem, který. převádí počítačový signál do podoby přenositelné telefonem. Toto připojení přestává stačit svou nízkou přenosovou rychlostí (max. 56 kbps), klesající při přetížení linky více uživateli až na jednotky kbps. Cenově díky speciálním tarifům a faktu, že uživatel je připojen pouze po nezbytně nutnou dobu, vychází prozatím tato volba nejvýhodněji, ovšem poměr cena/výkon již dávno zaostal za většinou dále diskutovaných typů připojení.

Druhá možnost, tj. připojení pomocí pevné linky, znamená, že počítač je pomocí vhodné linky přímo připojen k uzlu providera. Pevnou linku si lze pronajmout od telefonního operátora nebo od firmy, která takové linky vlastní (např. CESNET, provozovatelé kabelové televize apod.). Základní výhodou tohoto způsobu je přístup k připojení po 24 hodin denně, vysoká rychlost přenosu, minimální poruchovost. Tyto výhody jsou obvykle vyváženy vyšší provozní cenou.

Další možnost, bezdrátové připojení, v současnosti známé pod zkratkou Wi-Fi, které má přes své přednosti i nevýhody související s pokrytím území ČR signálem, kolísavou a poměrně nízká rychlostí přenosu, závislou na počasí, síť je navíc náchylná k poruchám a odposlechu. Proto je dnes spíše alternativou tam, kde není dostupná vhodná pevná linka, případně je využíváno pro snadnou výstavbu LAN. Bezdrátová síť se navíc stává jistým standardem připojení k Internetu pro přenosné počítače.

Poslední možnost, tj. připojení pomocí mobilního telefonu je relativně nová, ale pomalu a jistě začíná být konkurenceschopná i v ČR se zprovozněním mobilních sítí třetí generace. V České republice je základní služba poskytována mobilními operátory od roku 2000, v roce

2005 byl spuštěn zkušební provoz vysokorychlostního Internetu, který již zdatně konkuruje přenosovým možnostem připojení typu ISDN. Nové metody pro rychlý přenos dat GPRS nebo HSCSD, případně nejnovější EDGE, umožňují dosažení max. přenosové rychlosti řádu stovek kbps. Cenově se rovněž tato služba přibližuje službám připojení přes pevné telefonní linky, takže vzhledem k rozvíjející se mobilnosti počítačů lze očekávat i další prudký rozvoj využívání mobilního připojení k Internetu.

3.1 Připojení pevnou linkou

Při požadavku na maximální přenosové rychlosti jsou využívána optická vlákna s rozhraním technologie FDDI či ATM, umožňující dosažení přenosových rychlostí až řádu Gbps. V současné době výše uvedené standardy stále častěji nahrazuje univerzálnější Gigabit Ethernet. Klasické kovové kabely využívají technologii T1/T3. Linky T1 dosahují přenosové rychlosti až 1,544 Mbps, T3 dokonce 44,763 Mbps. Oba typy jsou vícekanálové (T1 má 24 kanálů po 64 kbps).

Tyto technologie využívají pro připojení k Internetu větší organizace, neboť náklady na pronájem vysokorychlostních pevných linek jsou značně vysoké a vyplácí se jen při vysokém objemu přenášených dat.

3.2 Připojení telefonní linkou

Připojení do Internetu po klasické telefonní lince vyžaduje zařízení převádějící digitální počítačový signál do analogového formátu vhodného pro přenos telefonními linkami - modem. Ten může být v provedení jako externí nebo interní (jako samostatná počítačová karta či integrován na základní desce). Mezi nejdůležitější charakteristiky modemu patří jeho přenosová rychlost (v kilobitech za s - kb/s resp. kbps - v analogové telefonní síti max. 56 kbps)., možnosti komprese dat a korekce chyb a jeho homologace (osvědčení o tom, zda vyhovuje požadavkům pro připojení do telefonní sítě).

Mimo připojení po klasické analogové lince (vytáčené připojení) je k dispozici i digitálního přenos dat po telefonní lince - technologie ISDN a DSL.

V technologii ISDN (Integrated Services Digital Network) je klasická analogová telefonní linka od telefonní přípojky k digitální ústředně nahrazena rovněž digitální linkou o kapacitě dvou datových kanálů po 64 kbps a jednoho služebního kanálu 16 kbps.

Technologie DSL (Digital Subscriber Line) je významným vylepšením využití telefonních linek pro přenos dat, umožňujícím se stejnými vodiči dosáhnout přenosovou rychlost v řádech Mbps (ovšem na kratší vzdálenosti stovek až tisíců metrů). Nutnou podmínkou je existence příslušného digitálního modemu na obou koncích linky, protože těchto přenosových rychlostí lze na obyčejné telefonní lince dosáhnout pouze využitím signálů s větší šířkou pásma (v megahertzové oblasti). Existuje několik základních standardů – klasický DSL s přenosovou rychlostí 160 kbps, HDSL (High bitrate DSL) disponuje 1,544 Mbps, ADSL (Assymetric DSL) poskytuje 1,5 až 5 Mbps asymetricky – v opačném směru jen 16 až 640 kbps a VDSL (Very high bitrate DSL) dokonce 13 až 52 Mbps opět asymetricky (v opačném směru 1,5 až 2,3 Mbps) při omezené délce vedení na 1350 až 300 m.

V případě využití kabelové televize pro připojení k Internetu je nutný rovněž modem (ovšem odlišný od telefonního modemu). Díky kvalitnějšímu vedení kabelové televize jsou dosahovány podstatně vyšší přenosové rychlosti srovnatelné s klasickými pevnými linkami a rovněž kvalita přenosu (počet chyb a kolísání přenosové rychlosti) je vysoká.

3.3 Bezdrátové připojení

Již roce 1990 začaly první práce na vytvoření standardu pro bezdrátové připojení ale až v roce 1997 byla přijata norma IEEE 802.11 s max. přenosovou rychlostí 2 Mb/s a používaným přenosovým frekvenčním pásmem v oblasti 2,4 GHz (volná frekvence ve všech státech světa). Ovšem krátce na to, v roce 1999, byla tato norma inovována na verzi IEEE 802.11b, pracující ve stejném frekvenčním pásmu, ale s maximální přenosovou rychlostí 11 Mb/s - norma sítě Wi- Fi. Další možnosti zvýšení přenosové rychlosti představuje buď rozšíření přenosového pásma na frekvenci 5 GHz (IEEE 802.11a), nebo použitím jiného typu modulace signálu - lze tak dosáhnou max. přenosové rychlosti až 54 Mb/s (jako IEEE 802.11a). Základní problém bezdrátového připojení představuje omezení vzdálenosti mezi vysílacím a přijímacím bodem - ve volném prostoru je to 300 až 1000 m, v budovách dokonce jen 30 až 100 m, přičemž se zhoršováním kvality signálu prudce klesá přenosová rychlost. Další problém představuje snadné odchycení předávaných informací, nutný je šifrovaný provoz s časově omezeným šifrovacím klíčem. Na mnoha místech ČR jsou již v provozu lokální sítě Wi-Fi standardu, poskytující svým registrovaným uživatelům připojení k Internetu, dokonce i na mnoha místech zdarma (Prostějov - okolí radnice).

Průvodce studiem

Možnosti připojení lokální počítačové sítě resp.domácího počítače k Internetu se rychle vyvíjí díky vývojii nových technologií i vzrůstající konkurenci různých poskytovatelů připojení k Internetu. Proto nelze provést žádné vyhodnocení ekonomicky nejvýhodnějšího způsobu připojení k Internetu s výhledem na dobu delší než přibližně jeden rok. Ovšem obzvláště pro individuálního uživatele Internetu stojí tento ekonomický pohled velmi vysoko při rozhodování, zda svůj počítač k Internetu připojit či ne. Jedno lze však k ekonomice připojení k Internetu říci s jistotou. Klasické vytáčené připojení svým poměrem cena výkon zaostává za ostatními možnostmi připojení. Snad jen uživatel, který se připojuje k Internetu jen na několik minut měsíčně, může uvažovat o tomto způsobu připojení jako o ekonomicky nejvýhodnějším.

Shrnutí

Možnosti připojení LAN do Internetu v současnosti obsahují jak klasické tak i bezdrátové technologie. Ovšem pro dosažení maximální přenosové rychlosti při prakticky nulové chybovosti a dostatečném zabezpečení přenosu stále převládají klasické technologie s kabely.

Pojmy k zapamatování

- připojení pevnou linkou - Ethernet, T1/T3
- připojení telefonní linkou - vytáčené připojení, ISDN, SDL
- bezdrátové připojení - Wi-Fi, GPRS, EDGE

Kontrolní otázky

1. Jaký typ kabelu je používán pro Gigabit Ethernet?
2. Jaký typ kabelu je používán pro Gigabit Ethernet?Jaký je rozdíl mezi klasickým vytáčeným připojením a připojením pomocí ISDN?
3. Jaké jsou základní problémy využití bezdrátových počítačových sítí?

Část II

Internet a jeho služby

Kapitola 4

Základní pojmy o Internetu

Hlubší pochopení Internetu a jeho technologií se neobejde bez základní znalosti historických souvislostí vývoje počítačových resp. síťových technologií. Překotný vývoj v této oblasti totiž rychle předhonil i ty nejsmělejší myšlenky svých tvůrců. Proto se dnes potýkáme s omezeními, jejichž původ leží v historii sice nedávné, ale z hlediska vývoje počítačových technologií již pravěké. A tak rychle upadají v zapomnění technologie, které se ještě před několika málo lety zdály být vrcholem technického vývoje, ač by se zdálo, že lidská fantazie je bezbřehá.

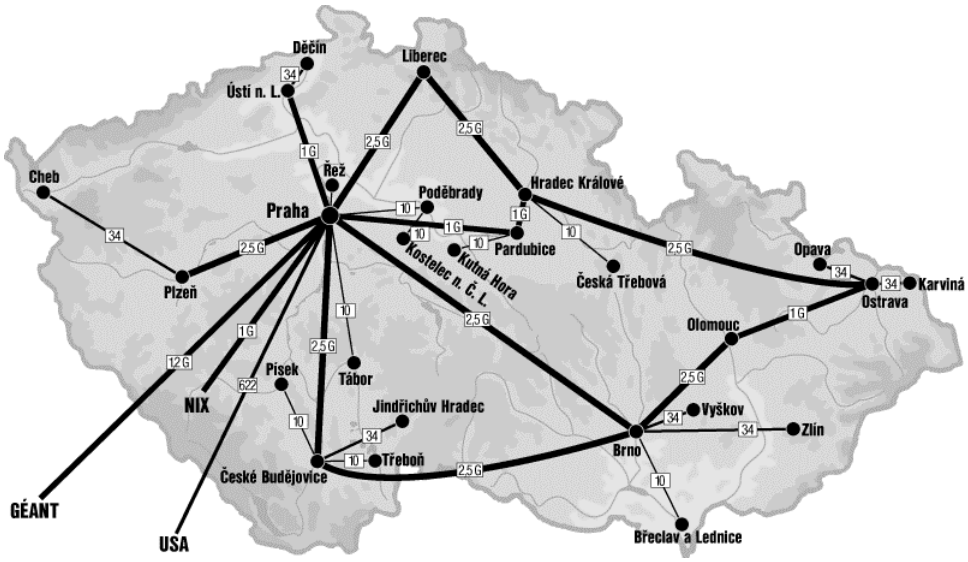
4.1 Internet – historie a současnost

Historicky první prakticky použitelná počítačová síť byla uvedena do provozu v roce 1969 v USA jako vojenský obranný projekt agentury DARPA (Defense Advanced Research Project Agency). Síť nesoucí název ARPANET propojovala čtyři uzly (počítačová místa) a již tato první síť nesla základní výstavbový princip dnešního Internetu - všechny uzly byly rovnocenné. Vojenský projekt prostě vyžadoval funkčnost sítě i v případě vyřazení kteréhokoliv uzlu z provozu. Úspěšnost projektu se odrazila v rychlém růstu sítě - v roce 1971 měl ARPANET 15 vzájemně propojených uzlů, v roce 1972 již 37 a v roce 1984 přes 1 000. Paralelně s vojenskými úkoly začal ARPANET plnit i cíle řekněme čistě komerční - zprvu např. prostou výměnu osobních zpráv, vznikla tedy první elektronická pošta. Vojenský projekt ARPANETu v roce 1981 doplnil v USA projekt univerzitní počítačové sítě BITNET, Evropa následovala tento příklad v roce 1983 univerzitní sítí EARN (European Academie and Research Network) a až v roce 1988 dorazil EUNET (další evropská síť) i do tehdejší ČSSR.

Růst počítačových sítí a hlavně komunikace v jejich rámci vedl k nutnosti zavedení jednotného komunikačního jazyka - protokolu, nezávislého na konstrukci počítačů ani jejich operačním systému. V roce 1974 tak vznikl protokol TCP (Transmission Control Protocol), řešící bezchybné předávání dat po počítačové síti a protokol IP (Internet Protocol), který umožnil bezproblémové směrování přenosu dat. V roce 1982 byly oba spojeny do jednotného protokolu TCP/IP, který se pak postupně stával standardním komunikačním protokolem Internetu. Jeho vznik lze datovat již do následujícího roku, kdy byl zprovozněn první bránový počítač umožňující propojení vzájemně odlišných sítí a současně došlo k odštěpení civilní složky ARPANETu, která se již nadále vyvíjela bez vojenského vlivu na komerčním principu. Rok 1990 je druhým datem uváděným jako datum zrodu Internetu, protože v tomto roce nadace NSF (National Scientific Foundation) vyhlásila program bezplatného připojení vysokých škol v USA k síti NSFNET, jehož součástí byl návrh vytvoření globálního Internetu jako sítě sítí. Tempo růstu Internetu v těchto letech ilustrují závratná

čísla - v roce 1989 bylo ve světě 160 000 uživatelů Internetu, v roce 1995 již kolem 20 milionů a v roce 2000 více než 300 milionů uživatelů. V současnosti (rok 2005) lze odhadovat počet uživatelů blížících se jedné miliardě hlavně díky uvolňování informační politiky a rozvoji sítí v lidnatých asijských zemích, zejména Číně.

Co se týče České republiky, původní česká páteřní síť CESNET (Czech Educational and Scientific Network, společný projekt českých vysokých škol a Akademie věd ČR, byla nahrazena páteřní rozvodem CESNET2 s přenosovou kapacitou až 2,5 Gb/s a počet uživatelů Internetu v ČR je odhadován na přibližně 6.29 milionů lidí (údaj z 13. 6. 2012).



Obrázek 4.1: Cesnet, zjednodušená mapa české sítě.

4.1.1 Struktura Internetu

Internet je systém mnoha propojených počítačových sítí na všech kontinentech naší planety, ale i na vodě a ve vzduchu (lodě a letadla díky bezdrátové komunikaci). Počítačovou sítí nazýváme systém komunikačních linek a počítačů, v němž pracují programy umožňující přenos informace (dat) mezi propojenými počítači. Internet je fyzicky vystavěn z menších počítačových sítí - lokálních (LAN), metropolitních (MAN) a globálních (WAN) počítačových sítí.

Lokální počítačová síť (LAN - Local Area Network) je počítačová síť na úrovni jedné školy, firmy, budovy a používá se k vzájemnému propojení několika počítačových míst tak, že mohou komunikovat každé s každým. Na jednom počítačovém místě může být více počítačů nebo jejich příslušenství (tiskárny, skenery, paměťová zařízení). Důležitou součást lokální počítačové sítě představují servery, které poskytují služby ostatním počítačům sítě (připojení k Internetu, správa databází, správa přístupových práv).

Metropolitní počítačová síť (MAN - Metropolitan Area Network) je počítačová síť na úrovni města nebo oblasti, vznikající propojením lokálních počítačových sítí v této oblasti. Vlastní propojení je obvykle realizováno vysokorychlostními komunikačními linkami (páteřní spoje).

Globální počítačová síť (WAN - Wide Area Network) vzniká propojením sítí MAN obvykle v rámci jednoho státu - národní Internety, u nás je to např. CESNET nebo v rámci evropského kontinentu EUNET.

4.1.2 Přenos informace v Internetu

Přenos informace v Internetu zabezpečují na určité úkoly specializované počítače - brány, směrovače, servery a klientské počítače. Brány (gateways) jsou počítače, které umožňují propojení dvou odlišných počítačových sítí.

Směrovače (routers) jsou počítače, které jsou specializovány na směrování toku dat v Internetu. Směrování znamená hledání cesty, kterou mají být data přenesena od jednoho počítače k druhému, přičemž je minimalizován počet směrovačů mezi zdrojem informace a místem jejího určení.

Servery (servers) jsou počítače obsluhující další počítače příslušné LAN. Jsou mezičlánkem mezi klienty (uživatelskými počítači) a Internetem. Současně zajišťují danou LAN před neautorizovaným přístupem - tzv. firewall. Servery ale plní další žádosti klientů v LAN - správu společných dat (podnikové databáze), úložný prostor pro velké objemy dat, provoz společného specializovaného programového vybavení apod. V jedné LAN může být současně více serverů a každý z nich může zajišťovat jiné služby.

Klientské počítače (clienťs computers) jsou nejčastěji osobní počítače uživatelů informačních služeb Internetu, kteří posílají, žádají, přijímají nebo vytvářejí informace na úrovni lokálních počítačových sítí, někdy též nazývaných Intranet - jeho informace a služby nejsou přístupné všem, ale jen autorizovaným uživatelům dané LAN.

Samotný přenos informace mezi počítači v Internetu probíhá na základě jednotných pravidel definovaných standardními postupy a jazykem - komunikační protokoly. Počítače Internetu si v rámci daného protokolu vzájemně rozumí a stejně interpretují přenášenou informaci. Každá informační služba má v Internetu vlastní protokol. Komunikační protokoly, které se v Internetu používají, jsou sdruženy v jedné množině označované jako protokoly TCP/IP, která zahrnuje kolem 100 protokolů. Jsou to např. protokoly označované jako FTP, Telnet, SMTP, HTTP apod.

Komunikační protokoly jsou dohodnutým systémem pravidel vzájemné komunikace počítačů v Internetu, pracujícím na obdobných principech jako např. poštovní služba - informaci (dopis) je třeba zabalit do obálky a obálku opatřit adresou. Stejně tak při komunikaci v Internetu je informace zabalena do obálky a opatřena adresou, aby mohla být úspěšně dopravena od odesílatele k adresátovi. Informace se přenáší ve formě malých balíčků dat - pakety (packets), na které je daná informace transformována již na počátku přenosu a zpětně dekódována na jeho konci.

Vlastní komunikace mezi počítači v Internetu probíhá ve vrstvách (layers). Každé vrstvě přísluší jen určitá část komunikace, přičemž si jednotlivé vrstvy vyměňují data se svým protějškem ve stejné vrstvě a dostávají pokyny od vrstvy, která je nad nimi. Z hlediska zjednodušeného pohledu probíhá komunikace v Internetu ve čtyřech vrstvách:

- Aplikační (FTP, Telnet, SMTP, HTTP, ...)
- Přenosová (TCP)
- Síťová (IP)
- Linková (komunikační linky, síťové karty a jejich ovladače).

Linková vrstva je vytvořena fyzickými prvky používanými k přenosu dat mezi počítači. Patří sem např. síťová karta, ale i její příslušný ovladač (software) a také komunikační linka spojující počítače.

Síťová vrstva je realizována protokolem IP, který zabezpečuje směrování přenášených dat (ve formě paketů). Přitom každý paket je přepravován samostatně a nezávisle na ostatních. Směrování přenosu je zabezpečeno tak, že počítače v Internetu mají své jedinečné adresy.

Adresy počítačů v Internetu mají dva formáty - číselný (IP adresa) a symbolický (DNS adresa). O struktuře obou adres bude pojednáno v kapitole 5.

Přenosová vrstva je v Internetu realizována protokolem TCP, jehož hlavním úkolem je zabezpečení bezztrátového přenosu paketů dat. Přenos je je neustále kontrolován, v případě zjištění chyby je daný paket odeslán znovu, dokud není potvrzen jeho bezchybný příjem.

Aplikační vrstva je realizována protokolem informační služby používané klientem. Každá z informačních služeb Internetu používá své vlastní protokoly aplikační vrstvy - přenos souborů (FTP), přístup k webovským dokumentům (HTTP) apod.

Shrnutí

Historický vývoj Internetu byl zahájen v šedesátých letech vznikem prvních počítačových sítí. Internet samotný je vystavěn hierarchicky - základní prvek představují LAN, nad nimi stojí sítě MAN, propojené následně do sítí velkého rozsahu WAN. A na vrcholu této hierarchie stojí Internet jako celosvětová síť. Vlastní komunikaci v rámci Internetu zabezpečují komunikační protokoly, ten základní, protokol TCP/IP zabezpečuje přenos dat včetně jejich adresování.

Pojmy k zapamatování

- Počítačová síť.
- Komunikační protokol.
- Rozlehlost sítí - LAN, MAN, WAN, Internet.
- Komunikační vrstvy Internetu.

Kontrolní otázky

1. Vyjmenuj základní prvky počítačových sítí nutných pro přenos informace v Internetu.
2. Vysvětli význam zkratek LAN, MAN, WAN.
3. Vyjmenuj čtyři základní vrstvy zjednodušenéhopřenosového modelu Internetu a popiš jejich základní funkci.

Kapitola 5

Komunikační protokoly

Data se v sítích posílají po částech definované velikosti - pakety, přičemž jejich uspořádání se řídí podle pravidel daných jednotlivými síťovými standardy – komunikačními protokoly.

V sítích s počítači pracujícími pod OS MS Windows se běžně používají tři komunikační protokoly : NetBEUI (NetBIOS Extended User Interface), IPX/SPX (Internetwork Packet eXchange/Sequenced Packet eXchange) a TCP/IP (Transmission Control Protocol/Internet Protocol).

5.1 Komunikační protokol NetBEUI

Tento protokol vyvinula IBM v polovině 80. let 20. stol. z protokolu NetBIOS. V současnosti se používá hlavně pro komunikaci mezi počítači pracujícími pod OS Windows. Nastavuje se jen název počítače pro identifikaci v síti a název pracovní skupiny či domény, kam počítač náleží. Při své jednoduchosti má vysokou komunikační rychlost, ale je „neroutovatelný“ (není směrovatelný) a proto jej nelze použít pro komunikaci ve větších sítích. Proto se obvykle používá s jiným protokolem, který „routovatelný“ je (např. TCP/IP).

5.2 Komunikační protokol IPX/SPX

Byl vyvinut pro potřeby síťového OS Novell NetWare. V OS Windows je nahrazen protokolem NWLink, který je s ním kompatibilní. Při instalaci prakticky není třeba konfigurovat jeho parametry. Na rozdíl od NetBEUI je „routovatelný“.

5.3 Komunikační protokol TCP/IP

Jedná se o celosvětově nejpoužívanější komunikační protokol (či spíše soubor protokolů). Na rozdíl od předchozích protokolů je univerzální (nezávisí na typu OS) a je „routovatelný“. Vzhledem k jeho možnostem je ovšem poněkud komplikovanější jeho konfigurace po instalaci.

Nejdůležitější součásti protokolu TCP/IP jsou:

DHCP (Dynamic Host Resolution Protocol) - zajišťuje dynamické přidělování IP adres (IP adresa je unikátní číslo počítače v síti s protokolem TCP/IP). Tuto službu vykonávají vybrané počítače v síti, na nichž je nainstalována služba DHCP Server.

Jinou možností je statické přidělování IP adres počítačům připojeným do sítě, které se ovšem řídí přesnými pravidly, aby byl splněn požadavek jedinečnosti adresy v síti.

DNS (Dynamic Name Service) - tato služba zajišťuje překlad symbolické na IP adresu.

WINS (Windows Internet Name Service) - pro počítače pracující pod OS MS Windows plní obdobnou funkci jako DNS.

SMTP (Simple Mail Transfer Protocol) - poskytuje službu elektronické pošty (E-mail).

FTP (File Transfer Protocol) - protokol používaný pro přenos souborů mezi vzdálenými počítači využívající službu tzv. FTP Serveru.

Telnet - umožňuje počítač připojit jako terminál k jinému vzdálenému počítači a ovládat jej pomocí textových příkazů.

Ping - utilita, s jejíž pomocí lze testovat spojení mezi počítači. Na zadanou adresu vyšle soubor dat (packet) a čeká na odezvu. Pokud odezva nedorazí je spojení nefunkční.

5.3.1 Protokol IP

Přenos dat Internetem se řídí pravidly definovanými protokolem IP (Internet Protocol), o kterém již byla řeč v předchozích kapitolách v souvislosti s hlavním Internetovým protokolem TCP/IP. Základní problém směrování informace po Internetu - jednotný formát Internetových adres - řeší právě protokol IP, dosud nejčastěji implementovaný ve verzi 4 (IPv4).

Adresování protokolu IP

Protokol IPv4 definuje síťové adresy jako 32bitové číslo (základní informace byly podány již v kapitole **??**). Adresy IP přiděluje úřad IANA (Internet Assigned Numbers Authority, viz http://www.iana.org). Adresy IP se dělí podle významu a použití do čtyř tříd:

Třída adresy	Přípustný tvar IP adresy	Síťová maska	Počet dostupných adres ve třídě
Třída A	1.x.x.x až 126.x.x.x	255.0.0.0	128
Třída B	128.0.x.x až 191.254.x.x	255.255.0.0	16 384
Třída C	192.0.0.x až 223.254.254.x	255.255.255.0	2,1 miliónu
Třída D	224.0.0.x až 239.254.254.254	není	není

Mnohé organizace, které mají přidělenu adresu třídy B, mnohdy nevyužijí samostatné adresy pro 16 000 počítačů, ale potřebují logicky rozdělit svou síť na podskupiny - podsítě. To lze provést předefinováním hodnoty síťové masky tím, že se rozšíří počet bitů tvořících masku. Snižuje se tak sice počet adres, které jsou k dispozici pro počítače této domény, ale zvyšuje se počet samostatných segmentů sítí (podsítí - subnetting).

Přidělování IP adres závisí na rozsahu sítě:

1. Pro lokální sítě nepřipojené k Internetu je hodnota IP adresy volitelná, pouze žádné dva počítače nesmí mít stejnou IP adresu a navíc aby jejich adresy patřily do stejné třídy a podsítě, jinak se vzájemně nebudou „vidět“.
2. Pro lokální sítě připojené k Internetu je nutno hodnotu IP adresy přiřadit tak, aby nedošlo ke konfliktu s jiným počítačem připojeným k Internetu. Protože takový počítač může být lokalizován kdekoliv na světě, existuje centrální správa přidělování IP adres. Tu zabezpečuje Network Information Center (NIC), který (resp. jeho pobočky) přiděluje IP adresu nebo rozsah použitelných IP adres nejprve tzv. poskytovatelům připojení k Internetu – Internet Service Provider (ISP), který pak IP adresy dále poskytuje svým smluvním partnerům.

Datagramy IP

Datagram představuje systém přenosu dat podle protokolu IP. Každý datagram tohoto protokolu se skládá z hlavičky, za kterou následují data. Hlavička má proměnnou délku a její strukturu obsahuje základní údaje pro správný přenos dat a kontrolu jejich celistvosti během přenosu. Struktura hlavičky datagramu mimo jiné určuje maximální velikost paketu (balíčku dat) posílaného po síti na 65 535 bajtů (viz kapitola 7.1 věnovaná elektronické poště).

Porty a čísla portů

Každá aplikace může na Internetu komunikovat jen s jinou vhodnou aplikací. Ovšem adresa IP nestačí pro jednoznačnou identifikaci aplikace běžící na počítači s touto adresou, protože může být spuštěno současně několik aplikací. Aby každá aplikace nemusela mít svou IP adresu, která by ji jednoznačně identifikovala, doplňuje se IP adresa identifikující počítač tzv. číslem portu, který identifkuje konkrétní typ aplikace běžící na tomto počítači. Pro správnou komunikaci po Internetu mezi dvěma aplikacemi jsou tedy třeba IP adresy odesílatele a adresáta informace a čísla portů aplikace odesílatele a aplikace adresáta pracující s posílanými daty. Některým důležitým a známým aplikacím jsou čísla portů pevně přidělena (např. FTP pracuje na portu 21, WWW na portu 80). Tato předem přiřazená čísla portů se používají pouze na serveru; čísla portů na klientech se alokují dynamicky. Čísla portů mají svůj význam i při zajištění bezpečného připojení k Internetu, protože s jejich pomocí často probíhá filtrování firewallů, o kterých budeme hovořit dále v kapitole III o bezpečnosti na Internetu.

Průvodce studiem

Z hlediska bezpečnosti komunikace na Internetu hrají čísla portů, na kterých komunikují jednotlivé informační služby Internetu, velmi významnou roli. Standardní komunikace probíhají vždy na definovaném čísle portu a proto je lze právě přes toto číslo kontrolovat. Nepřátelské útoky se odehrávají právě využitím nestandardní komunikace přes port, vyhrazený jiné službě, než kterou útočník používá. Proto sledování komunikace z hlediska využití komunikačních portů představuje základní opatření při zabezpečení proti útoku do lokální sítě z Internetu (viz pojednání o firewallech v kapitole III o bezpečnosti na Internetu).

5.3.2 Protokol TCP

Protokol IP představuje mechanismus přenosu dat mezi dvěma počítači, který ale neobsahuje kontrolní mechanismy pro jejich bezchybný přenos. O tyto mechanismy se stará právě protokol TCP vytvářející při zahájení komunikace spolehlivý, bezchybný, plně duplexní kanál mezi dvěma počítači. Samotný přenos dat probíhá na základě protokolu IP, TCP přidává mechanismy zabezpečení proti ztrátě či dublování dat při přenosu protokolem IP. Navíc protokol TCP zabezpečuje správné složení jednotlivých datagramů IP na straně příjemce za obnovení původní formy informace odeslané ze zdrojového počítače.

Protokol TCP nejprve očísluje datagramy IP, rozdělí je na menší části (pakety) a pak je posílá dále po určitých kvantech (tzv. šířka okna). Další balík paketů odešle až po přijetí potvrzení, že předchozí data došla. Velikost takového balíku paketů je definována dynamicky podle vlastností daného segmentu sítě, to jsou tzv. plovoucí okna, definující maximální počet paketů, které může odesílatel vyslat, aniž by obdržel nějaké potvrzení o jejich přijetí. Tímto způsobem se přenos podstatně urychlí oproti situaci, kdy se čeká na potvrzení každého paketu. Ani přijímající počítač neodesílá potvrzení ihned po obdržení prvního paketu, čeká na přijetí určitého počtu paketů a pak teprve odešle jedno společné potvrzení za všechny.

5.3.3 Protokol IP verze 6

Protokol IPv4 má mnohé nedostatky, obzvláště kritický je nedostatek IP adres díky jejich 32bitovému formátu a to jak celkově, tak i z hlediska malého počtu realizovatelných adres třídy B, nejvhodnějších pro již zmíněné vytváření podsítí. Další problém představuje přenos velkých objemů dat pro multimédia a rovněž tak nízká úroveň zabezpečení přenosu dat proti odposlechu či absence nástrojů pro pro zajištění autorizace datové komunikace. Tyto problémy řeší nová verze protokolu IP známá jako verze 6 (IPv6), na jejímž vývoji se začalo již v roce 1995 . IP adresa má v této verzi délku 128 bitů, takže poskytuje dostatečný počet použitelných adres i do daleké budoucnosti (2128 = 3,4.1038 adres v IPv6 oproti 232 = 4,3.109 adres v IPv4). Zjednodušení hlavičky datagramu urychluje přenos dat po Internetu, navíc lze definovat data vyžadující speciální zacházení - např. přednostní přenos multimédií u aplikací pracujících v reálném čase (videokonference apod.). Nová verze protokolu definuje rovněž mechanismy pro zajištění autentizace, důvěrnosti a integrity posílaných dat.

Hlavička protokolu IPv6 má na rozdíl od verze IPv4 pevnou délku 40 byte:

Verze	Priorita	Návěstí toku
Délka zátěže	Další hlavička	Limit skoků
Zdrojová IP		
Cílová IP		

- Pole **verze** (Version) se v hlavičce IPv6 skládá ze 4 bitů a je rovno 6; tato hodnota označuje číslo verze protokolu IP.
- Pole **priority** obsahuje čtyři bity a zdroj (odesílatel) v něm může definovat prioritu paketů IP relativně vzhledem k ostatním paketům IP, obecně čím vyšší hodnota, tím vyšší priorita přenosu.
- Pole **návěští toku** (Flow Label) sestává ze 24 bitů a zdroj pomocí něj požaduje po směrovačích speciální zpracování paketu. Toto pole má sloužit pro aplikace se speciálními potřebami, jako jsou například multimédia a aplikace pracující v reálném čase.
- Pole **délky zátěže** (Payload Length) tvoří 16 bitů a obsahuje délku paketu IP, který následuje za touto hlavičkou s pevnou délkou. Do údaje o délce se zahrnuje délka všech rozšířených hlaviček plus délka vlastní datové zátěže.
- Pole **další hlavičky** (Next Header) se skládá z 8 bitů a identifikuje typ hlavičky, která se nachází bezprostředně za hlavičkou IPv6. Tato hlavička vyznačuje data protokolu vyšší vrstvy vložená do datagramu IPv6.
- Další pole o délce 8 bitů definuje **limit počtu přeskoků** (Hop Limit) a znamená zbývající počet přeskoků, které ještě může paket IP absolvovat.
- Poslední dvě pole tvoří **zdrojová IP adresa** a **cílová IP adresa** paketu (obě 128 bit).

Rozšíření hlavičky IPv6

Mezi hlavičkou a vlastní datovou zátěží definuje protokol IPv6 místo, do něhož je možné umístit určitý počet doplňkových hlaviček, takzvaných rozšíření hlavičky IPv6 (Extension Header). Díky tomuto schématu mohou směrovače hlavičku snadno a rychle zpracovat, zejména pokud za ní nenásledují žádná rozšíření. Důležité jsou zejména dvě bezpečnostní rozšíření hlavičky - autentizační hlavičku a zapouzdřenou bezpečnostní hlavičku zátěže (protokol IPSec).

Autentizační hlavička (Authentication Header) potvrzuje nejen, že daný paket IP pochází od toho uzlu, o kterém to tvrdí, ale i to, že se obsah paketu IP nikde na cestě nezměnil (integrita paketu). Nejdůležitějším posláním zapouzdřené bezpečnostní hlavičky zátěže (Encapsulated Security Payload, ESP) je zajištění důvěrnosti (nečitelnosti pro jiného než určeného příjemce) paketu. V závislosti na použitém algoritmu může ESP poskytovat také služby zajištění autentizace a integrity dat. Hlavička využívá různých šifrovacích algoritmů, přičemž šifrována jsou nejen data, ale i část hlavičky ESP.

Shrnutí

Správný přenos dat Internetem zajišťují komunikační protokoly. Hlavním komunikačním protokolem Internetu je protokol TCP/IP, přičemž protokol IP se stará o vlastní přenos dat včetně adresování. Pro adresování využívá číselnou IP adresu, která má ve verzi protokolu IPv4 32bitovou velikost, ve verzi IPv6 již 128bitovou. Protokol TCP se pak stará o správný přenos dat - poskytuje protokolu IP kontrolní mechanismy. Data se přenášejí v balíčcích definované velikosti - paketech, které začínají hlavičkou, obsahující informace nezbytné pro přenos dat.

Pojmy k zapamatování

- protokol IPv4 a IPv6
- IP adresa
- protokol TCP
- hlavička balíčku (paketu) přenášených dat

Kontrolní otázky

1. Jaké jsou zásadní rozdíly mezi verzemi protokolu IPv4 a IPv6?
2. Jaké kontrolní mechanismy pro správnost přenosu dat nabízí protokol TCP?
3. Jaké základní informace obsahuje hlavička balíčku (paketu) přenášených dat?

5.4 Pracovní skupiny a domény

V rámci počítačových sítí jsou jednotlivé počítače rozčleněny do menších skupin - pracovních skupin nebo domén.

Pracovní skupina - umožňuje členění počítačů do skupin bez ohledu na architekturu sítě a umožňuje členům pracovní skupiny využívat prostředky všech připojených počítačů. Problematické je zabezpečení jednotlivých počítačů, protože přístup do skupin není nijak omezen. Jedinou možnost poskytuje pouze ochrana sdíleného prostředku heslem.

Doména - tento typ členění sítě je použitelný pouze v sítích s architekturou klient/server. Přístup do domény je možný pouze přes server (primární řadič domény), což umožňuje vyšší bezpečnost sítě než předchozí typ členění (přístupová práva lze nastavit individuálně). Jako OS pro správu domény je používán OS MS Windows Server. Stále více jsou však pro správu domén využívány unixovské OS, zejména různé verze Linuxu. Z hlediska uživatele počítačových sítí jsou nejdůležitější dva typy domén:

1. Doména Windows - tato doména je spravována počítačem s Windows Server - primární řadič domény (ověřuje oprávnění ostatních počítačů k přístupu do domény, ověřování práv uživatelů apod.).

2. Internetová doména - je určena hierarchií Internetu. Na vrcholu stojí kořenová doména (root domain), ve které pracují kořenové DNS servery (root servers). Pod touto doménou jsou domény nejvyšší úrovně (top levels domains), dělené na dvě kategorie. První představují geografické domény, přiřazené všem státům světa. Tyto používají dvouznakový kód podle normy ISO 3166 (např. CZ pro Českou republiku, JP pro Japonsko, AT pro Rakousko). Druhá kategorie je specifická pro USA, kde se používají organizační domény s tříznakovým kódem (např. COM pro komerční organizace, EDU pro vzdělávací organizace, GOV pro státní organizace, NET pro organizace udržující síť). Jména nižších domén vždy končí kódem té domény nejvyšší úrovně, kam organizačně daná doména patří. Symbolická (DNS) adresa se tak skládá ze jména počítače a jmen jednotlivých domén v jejich hierarchické posloupnosti. Každá doména má svého správce, který přiděluje jména v rámci této domény.

Shrnutí

Komunikační protokoly používané pro přenos informací po síti jsou směrovatelné a nesměrovatelné. Pouze směrovatelné protokoly jako je TCP/IP lze použít pro komunikaci v Internetu. Základem směrování přenosu informace je definice adresy - protokol IP definuje systém adresování počítačů na základě 32 bitového čísla. Mimo číselnou IP adresu lze použít i symbolickou (DNS) adresu založenou na systému Internetových domén.

Pojmy k zapamatování

- komunikační protokoly - NetBEUI, IPX/SPX, TCP/IP
- IP adresa, maska podsítě
- doména
- symbolická (DNS) adresa

Kontrolní otázky

1. Jaký je rozdíl mezi komunikačním protokolem NetBEUI a protokolem TCP/IP?
2. Jaký formát má IP adresa protokolu IPv4?
3. Jakým způsobem probíhá překlad symbolických adres na IP adresy?
4. Jakým způsobem je zabezpečena jedinečnost adres počítačů připojených do Internetu?

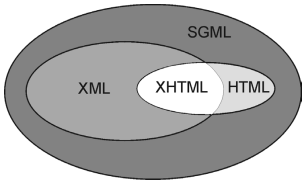
Kapitola 6

Základní protokoly a standardy používané u WWW služeb

World Wide Web neboli WWW představuje soubor protokolů a dalších SW technologií, které jako základ pro prezentaci informace používají hypertext. Vlastní technologii WWW vytvořil v roce 1989 Timothy Berners-Lee, který působil v Evropském centru pro jaderný výzkum CERN, na základě tehdy již rozpracovaných technologií elektronického způsobu prezentace informací. Dnešní vývoj standardů technologie WWW řídí konzorcium World Wide Web Consortium (W3C).

6.1 Hypertext a značkovací jazyky

Hypertext je technologie, s jejíž pomocí lze tvořit dokumenty, vzájemně propojené pomocí takzvaných odkazů (links). tyto odkazy mohou ukazovat na příbuznou informaci uvnitř daného dokumentu, ale i na informace vyskytující se kdekoliv na světě v jiném dokumentu (nemusí být nutně hypertextový). Hypertextové dokumenty jsou vytvářeny pomocí značkovacího jazyka HTML (HyperText Markup Language), jehož úlohu opět v poslední době přebírají obecnější verze značkovacího jazyka XHTML (eXtended HyperText Markup Language) resp. XML (eXtended Markup Language). Všechny tyto verze značkovacích jazyků jsou podmnožinou nejobecnější verze značkovacího jazyka SGML (Standard Generalized Markup Language). Systém značkovacích jazyků ilustruje obrázek 6.1.



Obrázek 6.1: Podmnožiny obecného značkovacího jazyka SGML.

Pro vlastní přenos dat používá WWW již existující protokoly Internetu - jako základ TCP/IP (Transmission Control Protocol/Intemet Protocol) a pro rozšíření přenosu i jiných než textových dat protokol MIME (Multipurpose Internet Mail Extensions). Lokalizace jednotlivých dokumentů na Internetu je realizována speciálně vyvinutým systémem adresování pomocí tzv. URL adresy (Uniform Resource Locator), jejíž specifikace je součástí protokolu pro práci s hypertextovými dokumenty na Internetu - protokol HTTP

(Hypertext Transfer Protocol). pro programování aplikací (server a klient služby WWW) je nutný navíc programovací jazyk pro tvorbu rozhraní - CGI.

6.2 Adresa URL

Adresa URL je vlastně jménem (i s celou cestou) WWW dokumentu (obecně nejen jeho) na Internetu, podobně jako je jméno a cesta určující z hlediska umístění souboru na disku počítače. Protože se dá použít i v jiné službě než WWW, je mimo cesty a jména vlastního dokumentu doplněna i jménem příslušné služby (protokolu). Některé služby, umožňující autorizovaný přístup, mohou v URL adrese obsahovat i jméno uživatele a jeho heslo. Základní schéma stavby URL adresy vypadá takto:

```
<éschma>://<žuivatel>:<heslo>@<hostitel>:<port>/<cesta>/<soubor>
```

kde `<schéma>` je jméno použitého protokolu nebo služby (např. http, ftp) a část za znakem @ tvoří jméno podle daného protokolu. `<uživatel>` je tak uživatelské jméno, pokud je v daném případě nezbytné (protokol Telnet), ¡heslo¿ je heslo uživatele, `<hostitel>` je doménové jméno síťového hostitele (serveru dané služby) v symbolickém zápisu nebo jako číselná IP adresa, (například fch.upol.cz či 158.194.74.30). Protokol HTTP 1.1 umožňuje pro jednu IP adresu nadefinovat více serverů služby WWW - virtuální servery, takže ne vždy je u této služby záměnná symbolická a IP adresa serveru. `<port>` pak definuje číslo portu protokolu IP pro danou službu (obvykle se nezadává a použije se implicitní hodnota definovaná protokolem) a `<cesta>` označuje umístění dokumentu `<soubor>` na serveru. Skutečná adresa URL webové stránky má pak např. tento tvar:

```
http://fch.upol.cz/skripta/intz/obsah.html
```

URL adresu lze použít i pro jiné služby, jak ukazují následující příklady nejběžnějších případů:

Schéma	Popis protokolu či služby
http	protokol HTTP, služba WWW
https	protokol HTTP + šifrování ve standardu SSL
mailto	služba elektronické pošty
FTP	protokol FTP, služba přenosu souborů
file	přístup k lokálnímu souboru

Zápis adresy URL lze v některých případech zjednodušit - pro službu WWW lze vynechat zápis schématu http:// a pokud se chceme dostat na hlavní stránku určité webové prezentace, stačí zapsat pouze doménové jméno serveru pro tuto prezentaci bez udání jména požadovaného dokumentu - zápis fch.upol.cz naviguje na hlavní stránku prezentace na serveru stejného jména (obvykle index.html resp. main.html).

Průvodce studiem

Internetový (webový) prohlížeč je standardně určen pro prohlížení WWW stránek. Proto v adrese těchto stránek není třeba uvádět schéma protokolu HTTP. Ovšem pro jiné informační služby neuvedení schématu služby vede k chabě při pokusu o zobrazení příslušného dokumentu a to již třeba v případě, že vynecháme schéma v případě stránek využívajících zabezpečenou verzi HTTP protokolu - protokol HTTPS. Snadno se o tom přesvědčíme i v Intranetu UP, když při objednávání jídla v menze místo adresy https://menza.upol.cz zadáme pouze http://menza.upol.cz.

6.3 Protokol HTTP

Protokol HTTP zabezpečuje přenos dat mezi serverem a klientem služby WWW. Jedná se jednoduchý a rychlý protokol pracující v modelu požadavek/odpověď a je anonymní. Pro přenos jiných než textových dat používá standard MIME (snadná rozšiřitelnost na různý obsah zpráv).Vlastní datový přenos mezi klientem a serverem je podobný e-mailové komunikaci. Komunikace mezi klienty a servery HTTP probíhá podle protokolu TCP/IP, a to na portu 80, (implicitní hodnota, možno zadat i jinou). Protokol HTTP není závislý na protokolu TCP/IP a dokáže pracovat i s jinými spolehlivými protokoly pro přenos dat po síti.

WWW stránky bývají složeny z více objektů - text, obrázky, zvuk, video, skript. Prohlížeč (klient protokolu HTTP) načte základní text dokumentu HTML v rámci jednoho spojení se serverem (vlákno) a při načítání dalších objektů otevře pro každý nové spojení. Spojení zahajuje klient odesláním požadavku a ukončuje jej server po odeslání odpovědi (spojení tedy není trvalé, i když rozšíření protokolu HTTP 1.1 umožňuje udržet spojení přes několik požadavků). Proto jsou jednotlivé části WWW stránky zobrazovány postupně - nejprve text (načítá se první a je nejmíň náročný na přenos), pak se teprve postupně objevují obrázky a další části stránky v závislosti na rychlosti přenosu.

Protokol HTTP vystačí při přenosu WWW stránek jen s několika jednoduchými příkazy - metodami. Nejdůležitější jsou GET, HEAD a POST - ty vlastně postačují pro celou komunikaci. Příkaz GET načte zdroj ze serveru a odešle jej klientovi. Příkaz HEAD slouží jen k testování existence dané adresy URL, nevrací žádná zobrazitelná data. Příkaz POST pak slouží k zasílání dat z klienta na server (např. při práci s formuláři). Aktuální verzí protokolu HTTP je verze 1.1. Tuto verzi podporují všichni nejdůležitější klienti a webové servery.

6.4 Rozhranní CGI

Rozhraní CGI (Common Gateway Interface) je na platformě nezávislé rozhraní, nad nímž pracuje software spojený se serverem HTTP. Toto rozhranní je vlastně propojovacím mechanismem brány mezi servery jiných protokolů než HTTP a daty jiných tvarů. Jedním z nejpoužívanějších forem rozhraní CGI je databázová brána, která se používá pro webovou reprezentaci dat uložených v databázi. Proces rozhraní CGI bývá často samostatnou aplikací; vykonává jej vždy server HTTP. Aplikaci rozhraní CGI spouští klient HTTP, a to zadáním adresy URL, která na danou aplikaci CGI ukazuje. Server HTTP zavolá určenou aplikaci CGI a její výstup vrátí klientovi HTTP. Standard CGI definuje rozhraní mezi serverem HTTP a aplikacemi CGI, tedy podobu příkazového řádku, parametrů (proměnných prostředí), vstupů a výstupů. Ve spojení s rozhraním CGI se velice často používá softwaru orientovaného na skripty, zejména pak jazyka Perl, takže aplikacím rozhraní CGI se běžně říká skripty CGI.

Rozhraní CGI umožňuje klientům spouštění programů, které posléze běží na serveru. Při psaní aplikací CGI i při jejich provozu je proto nutné učinit jistá bezpečnostní opatření. Klientům HTTP tak nesmí být přístupný žádný nebezpečný software a aplikace rozhraní CGI nesmí obsahovat bezpečnostní díry; všechny tyto kontroly musí zajistit administrátor serveru.

6.5 Standard HTML jazyka

Jazyk HTML (HyperText Markup Language) je zjednodušenou verzí obecného jazyka SGML (Standard Generalized Markup Language), který představuje formální systém pro popis jednotlivých částí dokumentů. Podle standardu MIME se dokumenty vytvořené v jazyku HTML označují jako text/html.

Standardizací jazyka HTML řídí konsorcium W3 (http://www.w3.org/), přičemž první oficiální verze byla označena v roce 1996 jako verze 3.0. Na nátlak velkých SW firem podnikajících v oblasti Internetu (Microsoft, Netscape) vznikla prakticky okamžitě verze s označením 3.2. Ale již v roce 1997 byl navržen a schválen standard HTML 4.01 jako konečná verze vývoje.

Jazyk HTML popisuje dokument a označuje jeho části pomocí značek - tagů (tags). Tyto značky jsou použity pro základní definici struktury HTML dokumentu, vyznačení a formátování důležitých částí v textu (nadpis, seznamy, tabulky), vkládání dalších objektů (zejména obrázků) a hlavně hypertextových odkazů. O syntaxi jazyka HTML bude podrobněji pojednáno v další kapitole 15, věnované základům tvorby statických WWW stránek.

Shrnutí

Informační služba WWW využívá řadu technologií pro tvorbu a prezentaci tzv. hypertextových dokumentů. Základem je jednoduchý transportní protokol HTTP zabezpečující přenos dat mezi klientem a serverem této služby. Pro správnou adresaci dokumentů byl nadefinována adresa URL, spojující adresu počítače v Internetu se službou, kterou používá a jménem dokumentu, který je danou službou využíván. Pro vlastní tvorbu hypertextových dokumentů je pak používán značkovací jazyk HTML, což je podmnožina znaků obecného značkovacího jazyka SGML.

Pojmy k zapamatování

- Hypertextový dokument a značkovací jazyk HTML.
- Protokol HTTP.
- Adresa URL.

Kontrolní otázky

1. Čím se liší hypertextový dokument od normálního textového dokumentu?
2. Jakou strukturu má adresa URL?
3. Jaké znáte značkovací jazyka a který se používá pro tvorbu hypertextových dokumentů?

Kapitola 7

Služby Internetu

Internet tu neexistuje samoúčelně. Jeho hlavním posláním je poskytovat svým uživatelům informace. Tvůrcem těchto informací jsou ale samotní uživatelé Internetu, on samotný je pouze zprostředkovatelem jejich přenosu podle definovaných pravidel.

7.1 Elektronická pošta a její správa

Elektronická pošta, nebo-li e-mail, je jednou z nejpoužívanějších služeb Internetu. Historie elektronické pošty je spojena s prvními počítačovými sítěmi, kdy jejich uživatelé provozovali elektronickou poštu prostřednictvím vybraného serveru v síti v úloze „úložiště zpráv“.Taková metoda elektronické pošty je realizovatelná jen v malých sítích, protože s růstem jejich rozměrů roste problém se směrováním.

7.1.1 Principy a protokoly elektronické pošty

Současný princip elektronické pošty je založen na jednoznačně definované komunikaci klient/server mezi uživatelským agentem elektronické pošty (Mail User Agent), běžícím na klientském počítači, a serverem elektronické pošty (Mail Transfer Agent). Na tento server uživatel odesílá e-mailové zprávy a server je pak směruje dále do sítě k adresátovi. Zpráva na cestě k poštovnímu serveru adresáta obvykle prochází několika agenty MTA, přičemž každý zanechá ve zprávě svůj podpis, potvrzující úspěšný přenos zprávy.

7.1.2 Funkce elektronické pošty

Elektronická pošta v architektuře klient/server může pracovat ve třech odlišných modelech:

- Off-line model - klient se připojuje k serveru jen občas a načte od něj vždy veškerou poštu (ta se ze serveru přitom odstraní). Tento model používá protokol POP (Post Office Protocol). Off-line model může podporovat také protokol IMAP (Internet Message Access Protocol), který ale nejlépe pracuje v on-line nebo v odpojeném modelu.
- On-line model - veškerou práci s poštou řídí klient v rámci aktuálně ustavené relace, fyzicky však vše probíhá na serveru podle protokolu IMAP.

- Odpojený model - tento model je kompromisem mezi off-line a on-line modelem. Klient se připojí k serveru, načte hlavičky zpráv a uživatel na jejich základě vybere poštu, se kterou chce dále pracovat. Tyto zprávy jsou přeneseny na klientský počítač, kde se s nimi dále pracuje a při dalším spojení (relaci) jsou změny přeneseny zpět na server. Hlavním místem pro ukládání zpráv je server, na klientovi se ukládají pouze dočasně. V tomto režimu je používán převážně protokol IMAP.

Každá e-mailová zpráva podobně jako dopis musí nést jedinečnou adresu koncového příjemce zprávy. Jedinečnost adresy se zabezpečuje jejím složením ze dvou částí – ze jména domény, kde je příslušná poštovní schránka uložena, a jména uživatele této schránky. Správce příslušné domény je odpovědný za to, aby nedošlo v jeho doméně k duplikaci jmen a tedy adres poštovních schránek. Možný tvar adresy poštovní schránky, vytvořené na poštovním serveru Univerzity Palackého pro uživatele Jana Nováka by pak mohl být např.:

jenda.novak@aix.upol.cz

Tuto adresu pak používá poštovní klient i server ke směrování e-mailů do příslušné poštovní schránky z počítače umístěného kdekoliv na světě. Standardně se e-mailová zpráva skládá ze dvou hlavních částí - obálky a vlastního obsahu zprávy.

- Obálka obsahuje informace nutné pro správný přenos a doručením zprávy.
- Vlastní obsah zprávy se dělí do dvou částí - hlavičky a těla zprávy.
  - Hlavička obsahuje identifikátor (ID) zprávy a časové údaje, které označují okamžik zpracování zprávy každým agentem MTA, přes který zpráva prochází.
  - Tělo e-mailu obsahuje vlastní zprávu vytvořenou uživatelem služby

7.1.3 Protokol POP

Protokol POP pracuje tedy v režimu offline. Klient se připojí k serveru a dotáže se na novou poštu. Server mu předá veškeré připravené zprávy, které po načtení e-mailový klient dále zpracovává bez účasti serveru. Veškerá komunikace protokolu probíhá standardně na portu 110.

Protokol POP ve verzi POP3 pracuje jako stavový automat, tzn. že se může v daném okamžiku vyskytovat pouze v jednom z předem definovaných stavů. Po splnění určené činnosti se automat přepne do dalšího stavu. Klient nejprve zašle serveru uživatelské jméno a heslo - autorizační stav. Již teď nastává bezpečnostní problém s nezabezpečeným přenosem hesla - rozšíření APOP proto umožňuje šifrované odeslání hesla.

7.1.4 Protokol SMTP

Protokol SMTP (Simple Mail Transport Protocol) je jednoduchý protokol pro přenos elektronické pošty od klienta k serveru a také ze serveru na jiný server. Na rozdíl od protokolu POP je SMTP protokol typu požadavek-odpověď. Příkazy i odpovědi mají tvar prostého ASCII textu. Odesílající uzel SMTP zadá zpravidla ihned po ustavení spojení TCP příkaz HELO, kterým odesílatel oznamuje svoji totožnost. Dále odesílající uzel SMTP zadá příkaz MAIL. Druhý server odpoví zprávou OK, která znamená, že je připraven k příjmu e-mailu. Poté odesílající uzel SMTP zadá příkaz RCPT, v němž oznamuje požadovaného příjemce pošty. E- mailová zpráva se odesílá příkazem SMTP DATA. Protokol SMTP definuje dále příkaz VRFY, který slouží pro ověření existence dané uživatelské poštovní schránky a pro zjištění podrobných informací o uživateli - zneužitelný příkaz. Proto bývá na serverech elektronické pošty blokován podobně jako příkaz TURN, který obrací směr ustaveného spojení.

7.1.5 Protokol IMAP verze 4

Protokol IMAP (Internet Message Access Protocol) pracuje opět jako stavový automat (standardně na portu 143) a umožňuje uživateli selektivně načíst na lokální počítač jednotlivé vybrané zprávy nebo jen jejich části a poté se odpojit. Díky nutné synchronizaci klienta a serveru je protokol IMAP složitější než protokol POP3 a jeho implementace je obtížnější. Příkazy protokolu IMAP se skládají z identifikátoru a jména příkazu s parametry. Server vrací jako odpověď značku, podle níž může klient spojit odpověď s původním příkazem. Klient totiž může vydat několik příkazů po sobě a nemusí čekat na odpověď.

Průvodce studiem

Vzhledem k rostoucím požadavkům na bezpečnost a univerzálnost komunikace po Internetu se pomalu upouští od používání protokolu POP pro přenos pošty mezi serverem a klientem elektronické pošty, který je nahrazován stále častěji použitím univerzálnějšího protokolu IMAP, do nějž lze podstatně snadněji implementovat zejména bezpečnostní rozšíření přenosu elektronických zpráv.

7.1.6 Rozšíření MIME

Podle původního standardu bylo možno pomocí SMTP přenášet pouze čistě textové zprávy (poslední bit každého bajtu musí být vždy 0). Umožnění přenosu i jiného obsahu zpráv (binární data, kde není poslední bit roven 0) přineslo rozšíření MIME (Multipurpose Internet Mail Extensions). MIME definuje oproti původnímu standardu několik typů obsahu pro různá textová a binární data. Každý ze základních typů má definovány další podtypy. Velikost zprávy je stále omezena na 64 KB (požadavek protokolu IP); zprávy větší než 64 KB se tedy musí rozdělit na menší zprávy a v cíli se opět sestaví do původní zprávy. Existuje šest základních typů zpráv rozšíření MIME (používáno při veškeré komunikaci po Internetu, nejen v rámci elektronické pošty):

- Typ Text slouží k přenosu vlastního těla zprávy. Podtyp Plain (prostý text) je implicitní, další možné podtypy jsou například Rich Text Formát (RTF), který podporuje speciální formátování znaků, jako je například tučné písmo a kurzíva, lze používat i jiné zankové sady než ASCII (národní znaky).

- Typ Image znamená, že přenášená data obsahují obrázek. Jako podtypy jsou definovány např. formáty GIF (Graphic Image Formát) a MPEG (Motion Picture Experts Group).

- Typ Audio označuje přenos zvukových dat.

- Typ Application značí přenos dat ve formátu určeném konkrétní aplikací, např. dokument vytvořený v programu Microsoft Word.

- Typ Structured (rovněž Multipart) definuje přenos dat v kombinaci výše uvedených typů.

- Typ Message označuje další možnosti související s formátem zprávy, resp. přílohy zprávy. Aby mohla být přenesena zpráva podle definice rozšíření MIME, musí být předem zakódována do formátu odpovídajícímu přenosu podle původního standardu používajícího 7bitový kód ASCII. Pro tento účel je používáno automatické kódování obsahu zprávy definované v hlavičce zprávy pro její pozdější dekódování u příjemce.

7.1.7 Bezpečnostní rozšíření služby elektronické pošty

Bezpečnost komunikace na Internetu pomocí služby elektronické pošty vyžaduje zabezpečení čtyř základních bezpečnostních požadavků:

- Důvěrnost - zpráva je čitelná pouze u oprávněných příjemců.
- Autentizační služba - potvrzení původu zprávy (identita odesílatele).
- Služba integrity - zajištění nezměnitelnosti zprávy během přenosu.
- Nemožnost zapření - průkaznost původu zprávy vzhledem k identitě odesílatele (digitální podpis).

Pro lepší pochopení principů funkce jednotlivých metod zabezpečení elektronické pošty je nutné prostudování kapitoly 11 věnované kryptografickým metodám.

S/MIME. Standard S/MIME (Secure/Multipurpose Internet Mail Extensions) definuje protokol pro rozšíření elektronické výměny zpráv o bezpečnostní mechanismy. S/MIME umožňuje šifrování zpráv a jejich digitální podepisování. Podle standardu S/MIME se obsah zprávy šifruje pomocí symetrické šifry a klíč (o velikosti až 2048 bitů) se poté šifruje asymetricky pomocí veřejného klíče příjemce zprávy. Autentizace je řešena pomocí algoritmů otisku zprávy a v rámci řešení problematiky digitálního podpisu zpráv podporuje S/MIME navíc certifikaci veřejných klíčů.

PEM. Standard PEM využívá opět jako přenosový mechanismus protokol SMTP; šifrování zpráv provádí rovněž symetrickou metodou. Symetrický šifrovací klíč se každému příjemci odesílá zašifrovaný algoritmem veřejného klíče. K ověřování veřejných klíčů využívá PEM certifikátů podle standardu X.509. Tento způsob zabezpečení zpráv je k dispozici i ve volné (bezplatné) verzi pro libovolného uživatele.

PGP. Standard PGP (Pretty Good Privacy) zabezpečuje důvěrnost a autentizaci opět kombinací symetrického a asymetrického šifrování jako standard PEM. Důvěrnost je zajištěna šifrováním zpráv pomocí symetrické blokové šifry s náhodně vygenerovaným klíčem o délce 128 bitů. Tento klíč se vloží do hlavičky zprávy, která se zašifruje pomocí asymetrické šifry s veřejným klíčem příjemce. Příjemce nejprve dešifruje hlavičku zprávy pomocí svého privátního klíče a tak získá klíč, jímž byla zašifrována původní zpráva. K zabezpečení autentizace dat se ve standardu PGP využívá technika digitálních podpisů.

Shrnutí

Služba elektronické pošty pracuje v režimu klient-server ve třech základních modelech, podporovaných příslušnými transportními protokoly. Pro přenos jiného obsahu než prostého textu používá protokol SMTP rozšíření MIME, které umožňuje bezchybný přenos libovolného obsahu elektronické pošty. Pro zvýšení bezpečnosti bylo navíc definováno rozšíření S/MIME.

Pojmy k zapamatování

- SMTP - základní transportní protokol služby elektronické pošty
- metody přístupu klienta ke službě elektronické pošty (off-line, on-line a odpojený model)
- protokoly pro přenos pošty ze serveru na klienta - POP3, IMAP
- rozšíření MIME a S/MIME
- adresa klienta elektronické pošty (poštovní schránky)

Kontrolní otázky

1. Jaký úkol plní protokol SMTP a protokoly POP3 resp. IMAP?
2. Za jakým účelem bylo vytvořeno rozšíření MIME?
3. Jaké technologie se používají pro zabezpečený přenos elektronické pošty ?

7.1.8 E-mailoví klienti

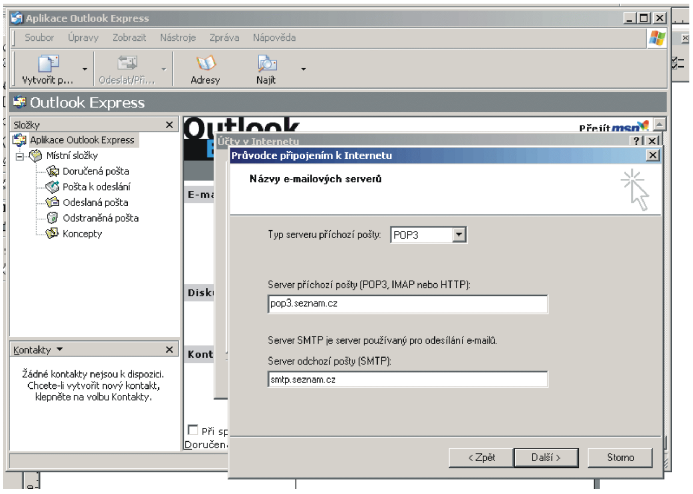
Pro funkci poštovního klienta byla vytvtořena řada programů. V systémech typu Unix se používají programy mail a komfortnější pine. V OS MS Windows patří mezi nejpoužívanější e- mailové klienty MS Outlook nebo MS Outlook, z alternativních pak lze uvést na UP Olomouc značně rozšířený Pegassus Mail, který je podobně jako další. klienti (např. Popcorn) dostupný jako tzv. freeware (bezplatně dostupný software). Další e-mailoví klienti jsou součástí webových prohlížečů (např. Mozilla), což je případ i klienta Outlook. Nutno podotknout, že v prvé řadě musí uživatel zaregistrovat u některého poskytovatele svou poštovní schránku, bez níž nelze žádného klienta poštovní služby používat. Obvykle je využívána tato služba bezplatně tak, jak ji poskytují vyhledávací portály (např. Seznam), kde je k dispozici i jednoduché webové rozhranní pro práci s poštou, kterému uživatelé s rychlým připojením k Internetu dávají přednost před vlastním e-mailovým klientem v lokálním počítači.

7.1.8.1 Nastavení e-mailového klienta pro práci s poštou

Pro názornost bude celé nastavení klienta ukázáno na klientovi MS Outlook. Program se spustí pomocí nainstalované ikony, resp. prostřednictvím prohlížeče MS Internet Explorer, kde z nabídky Nástroje vybereme položku Pošta a příspěvky a z ní pak položku Přečíst poštu. Při prvním spuštění klienta (každého) je nutno nejprve nadefinovat základní parametry práce s elektronickou poštou. Celým procesem nastavení klienta MS Outlook provede uživatele jednoduchý instalační program - Průvodce připojení .... Ten se nejprve dotáže na jméno uživatele - tímto zadaným jménem budou podepisovány odesílané zprávy. Dále je uživatel dotázán na svou e-mailovou adresu (tu musí mít přidělenu od správce příslušného serveru elektronické pošty). Následný dotaz požaduje zadání e-mailových serverů pro příjem a odesílání pošty (viz obrázek). Pro příjem pošty je stále nejčastěji používán již zmíněný POP3 protokol, takže obvykle název serveru pro příjem pošty začíná tímto názvem protokolu, následovaný jménem příslušné domény, ve které je server lokalizován, (např. pop3.seznam.cz). Pro odesílání pošty je standardně používán protokol SMTP a proto i název serveru obvykle začíná jeho jménem, opět následovaný jménem domény, (např. smtp.seznam.cz), jak ukazuje obrázek 7.1.

Poté již jen uživatel zadává jméno, pod kterým se přihlašuje ke svému účtu na poštovním serveru a heslo k tomuto účtu (není příliš bezpečné povolit zapamatování hesla programem). Tím je základní nastavení poštovního klienta ukončeno a lze jej ihned používat ke čtení i psaní e-mailů. Podrobnější nastavení zejména způsobu šifrování odesílaných hesel a e-mailů umožňuje nastavení dosažitelné v programu klienta přes volbu Nástroje a následně položky Účty... . Po zobrazení všech nastavených účtů programu vybereme ten, jehož vlastnosti chceme nastavit a tlačítkem Vlastnosti vyvoláme možnosti nastavení příslušného poštovního účtu.

Vlastní používání všech e-mailových klientů je velmi jednoduché. Podobně jako v MS Outlook stačí pro napsání dopisu stisknout tlačítko Vytvořit p... (poštovní zprávu): Do okénka Komu: vepíšeme e-mailovou adresu příjemce pošty, do okénka Kopie: dalšího případného adresáta (pokud chceme ovšem poslat kopii někomu dalšímu, aniž by o tom ostatní



Obrázek 7.1: Mailový klient.

příjemci věděli, je třeba použít položku Skrytá). Důležité je políčko Předmět:, protože text, který zde napíšeme, se zobrazí adresátovi společně s naší adresou v seznamu došlé pošty. Z tohoto textu bude adresát odhadovat jak důležitý dopis dostal. Vlastní text zprávy napíšeme do textového okna a poté stačí stisknout tlačítko Odeslat.

Pro psaní zpráv tři drobné poznámky:

1) V MS Outlook (ale i v jiných e-mailových klientech) lze vytvořit vlastní adresář (seznam adres), s jehož pomocí můžeme odesílat poštu příslušným osobám bez zdlouhavého vypisování jejich konkrétní adresy (tlačítko Nástroje, položka Adresář).

2) Rovněž většina e-mailových klientů podporuje tzv. automatický podpis, což je text, který se při odeslání dopisu připojuje na jeho konec a obsahuje informace o odesílateli. Tento text je třeba nejprve vytvořit a uložit – v MS Outlook přes tlačítko Nástroje, položka Možnosti... a záložka Podpisy).

3) Při psaní dopisu je vhodné nepoužívat diakritická znaménka, zejména v tom případě, pokud víme, že adresát nepoužívá stejného e-mailového klienta – pak totiž není zaručena správná interpretace znaků české abecedy a je tím ohrožena čitelnost dopisu adresátem.

K odesílanému dopisu lze připojit soubor, který společně s dopisem zašleme adresátovi. Po stisknutí tlačítka Vložit při psaní zprávy se objeví okno podobné MS Windows Exploreru, s jehož pomocí lze nalézt příslušný soubor a tlačítkem Připojit jej přidat k poštovní zprávě. Ještě jednou je třeba zdůraznit, že není dobré přesahovat rozumnou velikost přílohy, která se pohybuje na hranici cca 1-2 MB, ovšem díky zvýšené propustnosti sítí a růstu velikosti přiděleného odkládacího prostoru na poštovních serverech povolují správci poštovních serverů dnes i několikanásobně větší přílohy.

Přijetí doručené pošty se realizuje v poštovních klientech a tedy i v MS Outlook pomocí seznamu doručené pošty, kde si patřičný e–mail vybereme a po otevření poklepnutím na jeho jméno můžeme číst jeho obsah. Opět většina poštovních klientů umožňuje přímou odpověď (Replay) na doručený e-mail (u MS Outlook tlačítko Odpovědět), přičemž lze do odpovědi zahrnout i došlý text. Stejně tak lze pohodlně přeposlat došlý e-mail dalším adresátům – v MS Outlook tlačítkem Předat dál.

MS Outlook a i další poštovní klienti umožnují další práci s e-maily a nabízejí podprogramy pro jejich třídění, editaci, obsluhu síťového připojení šetřící naše výdaje za telefonní linku atd.

Průvodce studiem

Stejně jako tomu bylo v předchozích kapitolách, i zde je pro lepší pochopení činnosti služby elektronické pošty a způsobu nastavení jejího klienta velmi vhodné provádět celý popisovaný postup přímo na počítači. Za tímto účelem je vhodné pracovat přímo s nastavovacími prvky již zmíněného klienta MS Outlook či např. freewareového klienta, který je tak jednoduchý, že nevyžaduje vlastní instalaci do počítače, takže si při jeho použití nenarušíme jinou instalaci poštovního klienta v použitém počítači. Ovšem je třeba dát pozor na jeden specifický rys protokolu POP3, který bývá v klientech implicitně nastaven na stažení veškeré pošty ze serveru na klientský počítač okamžitě po připojení. Tak by se mohlo stát, že veškerou poštu, kterou máme uloženu na serveru, přesuneme do cizího počítače. Proto je třeba před zahájením načítání zpráv ze serveru provést nastavení protokolu POP3, umožňující ponechání e-mailů na serveru (přenáší se pouze kopie zpráv). Na závěr této kapitoly jedna perlička, kterou poskytuje i e-mailový klient MS Outlook - tou je zobrazení hlavičky e-mailu se všemi informacemi, které e-mail získal u odesílatele i při své cestě Internetem. Po otevření zprávy stačí pod nabídkou Soubor vybrat položku Vlastnosti a následně záložku Podrobnosti. V zobrazené hlavičce e-mailu tak uvidíme nejen kdo e-mail odeslal (snadno pozměnitelná informace), ale hlavně adresy serverů elektronické pošty, přes které tento e-mail prošel. Jako poslední je v seznamu ten, přes který šla zpráva jako první - tak lze snadno vystopovat alespoň doménu, odkud skrytý odesílatel svůj e-mail poslal (na http://www.ripe.net/ je např. k dispozici databáze domén). Samozřejmě specialisté se poměrně snadno přes správce domény mohou dostat až k počítači, odkud byl e-mail odeslán, i když byl identita zfalšována (k tomuto účelu existuje na Internetu spousta volných programů, např. Crook Sender).

Shrnutí

Pro využití služeb elektronické pošty mimo rozhranní WWW je nutný klient elektronické pošty. Tento klient musí být nastaven alespoň v základních parametrech pro komunikaci s příslušným serverem elektronické pošty. Toto základní nastavení zahrnuje definici uživatele této služby (resp. identifikace jeho e-mailové schránky) a definici metody (modelu) přístupu klienta k této poštovní schránce. Existující tři modely - off-line, on-line a odpojený - využívají maximálně daný typ připojení. Tedy podle způsobu připojení k Internetu je třeba při nastavení zvolit vhodný připojovací model (ovšem pokud poskytovatel služby takový výběr umožňuje).

Pojmy k zapamatování

- e-mailový klient
- schránka elektronické pošty - identifikace
- příloha e-mailu
- falešná identita e-mailu

Kontrolní otázky

1. Poštovní klient může být součástí klienta jiné informační služby Internetu. Kterého?
2. Co může být součástí přílohy e-mailu?
3. Je informace o odesílateli e-mailu v hlavičce zprávy vždy věrohodná?

7.2 Rich Site Summary – RSS

Rovněž se používá název Really Simple Syndication. Jsou to informační zdroje, které jsou samy schopny uživatele upozorňovat na nové zprávy. RSS patří svým formátem do rodiny XML. Technicky vzato pro provoz RSS na serveru (větš. zpravodajském) je třeba na web umístit soubor, ve kterém je ve stanoveném formátu výtah nabízených informací. Tento výtah (soubor) lze pak za pomocí skriptu automaticky aktualizovat. Tento soubor se nazýváme RSS kanálem (RSS feed, RSS stream nebo RSS channel). Existují programy – RSS čtečky (i v cloudu), které tento soubor umí v pravidelných intervalech stahovat a upozorňovat tak uživatele na nové zprávy. RSS čtečky bývají k dispozici v emailových klientech, jako samostatné aplikace (i pro mobilní zařízení), jako zásuvné moduly pro internetové prohlížeče (Sage pro Firefox) nebo on-line aplikace (GoogleReader, NetVibes).

7.2.1 Verze RSS

RSS vynalezla firma Netscape pro svůj portál MyNetscape, verze byla označena jako RSS v0.90. Dnes se už nepoužívá. Dnes se běžně pouzívá RSS v0.91 nebo 2.00 a řada jejich subverzí. RSS v0.91 je velmi jednoduchý a obsahuje jen název příspevku, URL a popis. Oproti tomu RSS v2.00 nabízí možnost připojení dalších informací jako je autor a datum příspěvku. V přípravě je již RSS v3.00.

Existují další formáty se stejnou úlohou. První je CDF (Channel Definition Format) od Microsoft, který se ale neuchytil. Druhým je ATOM 1.0 (The Atom Syndication format).

Exsituje speciální verze zvaná **audio RSS** (podcasting), která obsahuje informaci ve formě audio záznamu. Slovo podcasting vzniklo spojením názvu přehravače iPod (Personal on Demand) firmy Apple a slovem broadcasting (vysílání). Právě přehravač iPod umí RSS audio stahovat i organizovat (starší verze jen za pomocí iTunes). Čtečky podobně jako pro klasické RSS lze instalovat téměř na libovolné mobilní zařízení nebo PC (Doppler, iPodder, GoogleListen).

7.3 Cloud computing

Jsou to technologie, které využívají hardwarové a softwarové zdroje prostřednictvím počítačových sítí (např. Internet). Specifikum cloud služeb je, že uživatel nekupuje ani software, ani hardware, ale platí jen nájem za to co skutečně využije.

Nabídka konkrétních aplikací je velmi široká od kancelářských aplikací (docs.google.com, office.live.com) přes služby pro distribuované výpočty (mole.upol.cz) až po celé virtuální pracovní plochy a operační systémy (eyeOS).

Charakteristickými znaky cloudu jsou:

Škálovatelnost - uživatelé používají toluk výpočetních zdrojů, které aktuálně potřebují.

Pay as you go - uživatel zaplatí jen to co využije.

Multitenancy - "vícenájmový" systém; uživatelé sdílí stejné výpočetní zdroje.

Up-to-date - uživatel se nemusí starat o aktualizaci, bezpečnost apod.

Dostupnost - uživatelé se mohou připojit přes internet většinou pomocí jakéhokoliv zařízení (smartphone, notebook, tablet).

7.3.1 Typy cloud služeb

- Infrastructure as a service (IaaS)
  - Infrastruktura jako služba - dodavatel cloud řešení poskytnoutuje infrastrukturu. Typicky je to virtualizace. IaaS je vhodné pro ty, kteří vlastní software (licenci) a nechtějí se starat o hardware. Příkladem IaaS jsou Amazon WS, Rackspace nebo Windows Azure.
- Platform as a service (PaaS)
  - Dodavatel poskytuje kompletní webové aplikace a služby na Internetu, bez nutnosti stažení softwaru. To zahrnuje různé prostředky pro vývoj aplikace jako IDE nebo API. Nevýhodou tohoto přístupu je proprietární uzamčení, kdy může každý poskytovatel používat např. jiný programovací jazyk. Příkladem poskytovatelů PaaS jsou Google App Engine nebo Force.com.
- Software as a service (SaaS)
  - Aplikace je licencována dodavatelem a jako služba pronajímána uživateli. Uživatelé si tedy kupují přístup k aplikaci, ne aplikaci samotnou. SaaS je ideální pro ty, kteří potřebují jen běžné aplikační software a požadují přístup odkudkoliv a kdykoliv. Příkladem může být známá sada aplikací Google Apps, nebo v logistice systém Cargopass.
- Network as a service (NaaS)
- Storage as a service (STaaS)
- Security as a service (SECaaS)
- Data as a service (DaaS)
- Desktop as a service (DaaS - see above)
- Database as a service (DBaaS)
- Test environment as a service (TEaaS)
- API as a service (APIaaS)
- Backend as a service (BaaS)
- Integrated development environment as a service (IDEaaS)
- Integration platform as a service (IPaaS), see Cloud-based integration

Výčet služeb je, jak je vidět, velký. Většina cloudových služeb se však kombinuje do balíčků podle potřeb uživatelů.

7.4 Elektronické konference, IRC, Chat, ICQ

Internet je díky své rozsáhlosti ideální platformou pro výměnu názorů mezi svými uživateli. A nutno říci, že i když ještě donedávna výrazně převažovala komunikace hlavně e-mailová, dnešní doba obrací poměr ve prospěch interaktivní výměny názorů, nejčastěji ve formě chatu. Ten se stává pomalu náhražkou i přímé komunikace zejména u mladé generace, pro které je Internet stejně přirozenou záležitostí jako televize pro jejich rodiče, či rádio pro jejich babičky.

7.4.1 Off-line komunikace - elektronické konference a diskusní skupiny

V počátcích svého rozvoje počítačové sítě neumožňovaly rychlé přenosy větších objemů dat a tak i přenos prosté textové informace mezi více uživateli sítě v reálném čase představoval vážný technický problém. Proto se v této době rozvinula komunikace nepřímá, využívající počítačové sítě k prostému přenosu zpráv mezi skupinou uživatelů pomocí osvědčené služby elektronické pošty - tak vznikly elektronické konference a diskuzní skupiny.

7.4.1.1 Elektronické konference

Elektronické konference provozované na principech elektronické pošty byly za doby začátků rozvoje Internetu jedním z nejčastějších způsobů komunikace mezi jeho uživateli. Dnes s rozvojem novějších komunikačních technologií umožňujících komunikaci v reálném čase význam klasických elektronických konferencí poklesl, ovšem konference z Internetu zcela nevymizely, např. elektronická konference věnovaná problémům handicapovaných lidí na serveru:

http://www.tereza.fjfi.cvut.cz/elektronicka-konference

Konferenční servery (list servery) umožňují snadný způsob získávání informací o určitém tématu a aktivní účasti v diskusi. za pomoci elektronické pošty. Každá zpráva elektronické pošty, kterou někdo odešle na konferenční server, se automaticky rozesílá všem členům konference. I veškerá komunikace s konferenčním serverem probíhá za pomoci e-mailu. Pro přihlášení do konference stačí např. odeslat e mail s jednoduchým obsahem - Subscribe. Hlavní nevýhodou elektronických konferencí je příjem velkého množství e-mailů (v závislosti na aktivitě a počtu členů konference), takže může snadno dojít k zahlcení poštovní schránky nebo jejího uživatele touto lavinou zpráv. Tomuto problému se dá předejít obvykle tak, že místo jednotlivých zpráv bude uživatel dostávat jejich souhrn v jediném e-mailu.

Konference se dělí na moderované, kdy příspěvky třídí a rozesílá moderátor - jeden z členů konference, a nemoderované, kdy jsou do konference zahrnuty všechny příspěvky. Spravování konferencí zajišťují výše zmíněné systémy, většinou s názvem listserv či maiser.

Seznam nejdůležitějších příkazů listserveru nabízí následující přehled:

- HELP – pošle informace o tom, jak listserver na daném serveru pracuje
- LIST - vrací seznam konferencí na tomto listserveru.
- SUBSCRIBE nebo SUB ¡jméno skupiny¿ -přihlásí nás do dané skupiny.
- UNSUBSCRIBE nebo SIGNOFF nebo UNSUB ¡jméno skupiny¿ - odhlásí nás z dané skupiny.
- INDEX - dostaneme seznam souborů, které jsou přístupné prostřednictvím e-mailu.
- SEND ¡jméno souboru¿ - požádáme listserver, aby nám zaslal jmenovaný soubor. Elektronické konference lze vyhledat pomocí obvyklých webových vyhledávacích strojů (např. Google). Pro chemiky je k dispozici elektronická konference o chemii na serveru http://www.tabulka.cz/. Další informace o elektronických konferencích provozovaných v ČR lze nalézt na serveru listserv.cesnet.cz.

Průvodce studiem

V dnešní uspěchané době mílokdo hodlá čekat na názory druhých a když je konečně pozná, má chuť okamžitě se s ostatními podělit o svůj názor k tématu. To bohužel off-line komunikační služby neumožňují. Ovšem díky této neinteraktivnosti, má jejich uživatel dostatek času nad každým názorem (svým i cizím) v klidu přemýšlet. To je ohromný rozdíl oproti prázdnému tlachání na chatu. Proto zkuste opravdu v reálu, jaké to je opravdu nad názory přemýšlet. A můžete se i docela dobře při čtení a psaní konferenčních příspěvků zdokonalit ve své znalosti angličtiny (ale i jiných jazyků - i Japonci mají své konference).

7.4.1.2 Diskusní skupiny – USENET (Network News)

Účastníci diskusních skupin (uživatelé služby Usenet) si vyměňují své názory opět pomocí e-mailů, kterým se v tomto případě říká články. Zpráva, kterou někdo odešle diskusní skupině, se předá každému uživateli přihlášenému do této skupiny. Každá zpráva je označena určitým tématem neboli hlavičkou, ta identifikuje diskusní skupinu, do níž zpráva náleží. Výměna článků mezi jednotlivými servery a také mezi klienty a servery probíhá na základě protokolu NNTP (Network News Transfer Protocol).

Oproti elektronickým konferencím člen diskusní skupiny musí mít speciální program pro účast v diskusní skupině - obvykle je tento klientský program využívající protokol NNTP přímo součástí poštovního klienta (např. MS Outlook). Prostřednictvím tohoto programu pak uživatel vstupuje do diskusní skupiny, může zjišťovat jaké články jsou k dispozici a selektivně je číst. Diskusní skupiny nepodléhají žádné centrální administraci. Jedná se o volné sdružení jednotlivých počítačů a serverů - proto název USENET. Jména diskusních skupin se vytvářejí podle určité konvence: jméno se skládá vždy z několika částí oddělených tečkami, přičemž první část jména označuje kategorii diskusní skupiny - biz pro obchod a ekonomii, comp pro počítačové technologie, sci pro vědecká témata, soc pro společenské vědy atd. Tyto hlavní skupiny jsou definovány poměrně široce a proto se dále dělí na úžeji zaměřená témata.

Práci s News si ukážeme opět na příkladu e-mailového klienta MS Outlook. Pro účast v diskusní skupině je jej třeba nejprve nastavit - v nabídce Nástroje vybereme podnabídku Pošta a příspěvky a následně Přečíst příspěvky. Pokud to činíme poprvé, spustí se průvodce nastavení diskusní skupiny - mimo jména uživatele a jeho e-mailové adresy je třeba zadat diskusní server, např. news.fi.muni.cz. Tím nastavení skončí a klient přejde do módu výběru konkrétní diskusní skupiny na serveru a po jejím výběru ke čtení zpráv z této diskusní skupiny (obrázek XXX). Tlačítkem Přihlásit odběr se přihlásíme k odběru příspěvků z vybrané skupiny. Naopak tlačítkem Odhlásit odběr zrušíme odebírání příspěvků této skupiny. Seznam všech skupin, které odebíráme zjistíte v záložce Odebírané. Tlačítkem Obnovit seznam se aktualizuje seznam všech skupin. Po výběru diskusní skupiny se objeví se všechny její zprávy. Jednotlivé příspěvky můžeme poté číst podobně jako e-mailové zprávy. Na Internetu je mnoho možností výběru diskusních skupin, nalezitelných přes vyhledávací servery (např. groups.google.com), některé servery udržují archivy diskusí (např. usenet.jyxo.cz).

Shrnutí

Internetové konference a diskusní skupiny představují skupinu tzv. off-line komunikačních služeb Internetu. Důvodem pro toto označení je skutečnost, že pro komunikaci mezi účastníky je používána služba elektronické pošty, která neumožňuje komunikaci v reálném čase. Hlavním nástrojem těchto služeb je tak klient elektronické pošty, který má v sobě obvykle zakomponován i modul obsluhy diskuzních skupin (protokol NNTP).

Pojmy k zapamatování

- elektronické konference

- diskuzní skupiny (Usenet, News)
- protokol NNTP

Kontrolní otázky

1. Jaký klient je nutný pro využití komunikační služby elektronických konferencí?
2. Je nutný speciální klient pro použití služby Usenet (diskusní skupiny)?
3. Znáte nějaký archiv příspěvků diskusních skupin v českém jazyce?

7.4.2 On-line komunikace - textové konference

Doposud probírané komunikační možnosti Internetu představovaly služby založené na principu elektronické pošty, tedy časově nesynchronizovaném přenosu zpráv mezi uživateli. Ovšem Internet umožňuje i komunikaci mezi jeho uživateli v reálném čase.

7.4.2.1 Talk

Nejjednodušší službu komunikace v reálném čase představuje unixovská aplikace Talk. Oba komunikující uživatelé musí být přihlášeni na vhodný unixovský server a musí mít k dispozici program talk (obvykle za pomoci služby Telnet). Uživatel abc@prfnw.upol.cz, který zahajuje komunikaci napíše příkaz:

talk xyz@lfnw.upol.cz

uživateli xyz@lfnw.upol.cz se vypíše na monitoru informace, že s ním chce někdo komunikovat a že má zadat příkaz

talk abc@prfnw.upol.cz

Pokud vyzvaný uživatel zadá požadovaný příkaz, rozdělí se oběma uživatelům obrazovka na dvě poloviny. V jedné polovině mohou psát, ve druhé polovině čtou text psaný druhým uživatelem. Komunikaci lze ukončit kombinací kláves ¡Ctrl¿¡D¿.

7.4.2.2 Protokol IRC

Protokol IRC (Internet Relay Chat) umožňuje opět textovou komunikaci tentokráte více uživatelů současně. Každý server IRC obsluhuje několik konverzačních kanálů, z nichž každého se účastní několik klientů. Komunikační kanály jsou obvykle tematicky zaměřeny - např. fotbal, finance, počítačové technologie atd. V nejjednodušším případě hovoří několik klientů s jediným serverem IRC. Často jsou vytvářeny sítě IRC, které tvoří několik propojených serverů IRC, což umožní klientovi připojenému k jednomu serveru přístup do kanálů i na dalších serverech IRC. Pro komunikaci v rámci služby IRC je nutný speciální klient, získatelný např. na webu http://irc.diary.cz/. Mimo textové zprávy lze přenášet i binární soubory (bezpečnostní problém).

7.4.2.3 Prostředí MUD

Víceuživatelské herní prostředí MUD (Multi-User Dungeon) je virtuální prostředí, v němž uživatelé komunikují vzájemně mezi sebou a s počítačem vytvořenými postavami; pohybují se ve virtuální krajině, kterou rovněž vytváří počítač. Jde tedy o herní prostředí, nejčastěji

používané hráči fantazy her, vycházejících např. z žánru tzv. fantasy literatury (typického autora představuje J. R. Tolkiena). Bližší informace lze nalézt na mnoha českých a slovenských serverech, např. www.mudy.cz nebo mud.fandom.sk.

Prostředí MUD implementuje server MUD, který se stará o fyzické uložení světa MUD a o koordinaci vzájemné komunikace mezi jednotlivými uživateli. Uživatelé se k serveru MUD připojují buďto pomocí klienta Telnet (jehož uživatelské rozhraní je čistě textové) nebo pomoci klienta MUD (ten mívá často příjemnější uživatelské prostředí).

Existují různé variace na toto herní prostředí, nejznámější představuje prostředí MUME (viz www.fantasyplanet.cz/eporedax/mume).

Průvodce studiem

Textové konference v reálném čase jsou v poněkud jiné situaci, než off-line textové konference. Vždy je používali vyhranění uživatelé a tento okruh příznivců jim přetrvává i v době pohodlněji provozovatelné komunikace podporované službou WWW. Vkus tohoto okruhu příznivců nejlépe oceníme po nahlédnutí do oblasti vyhrazené hráčům v prostředí MUD. Kdo ví, jestli nepropadnete kouzlu tohoto způsobu Internetové komunikace.

Shrnutí

Textové konference představují jednoduchou možnost komunikace meži uživateli v reálném čase. Nejjednodušší klient této služby, program Talk, je součástí protokolu TCP/IP a je na rozdíl od dalších služeb tohoto typu (IRC, MUD) určen pouze pro komunikaci mezi dvěmi uživateli Internetu připojenými k nějakému serveru provozujícímu službu Telnet.

Pojmy k zapamatování

Talk textová komunikace v reálném čase mezi dvěmi uživateli Internetu

IRC textová komunikace v reálném čase mezi více uživateli Internetu

MUD textová komunikace v reálném čase zaměřena na tvorbu herního prostředí

Kontrolní otázky

1. Jaké jsou základní podmínky použití komunikačního programu Talk?
2. Vyžaduje služba IRC vlastní protokol, nebo jí postačuje protokol TCP/IP?
3. Vysvětli zkratku komunikační služby MUD.

7.4.3 Konferenční služby podporované službou WWW

Služba WWW nezpůsobila revoluci jen v oblasti publikace hypertextových dokumentů, ale díky své univerzálnosti pronikla i do oblastí, vyhrazených původně jiným technologiím. Jednou z nich je Internetová komunikace v reálném čase, kde nabídla nezávazný „pokec“ - chat.

7.4.3.1 Chat

Technologie služby WWW, je při své univerzálnosti použití uživatelsky příjemnější než již zmíněné komunikační technologie Internetu. Proto i v oblasti on-line komunikací vládne, tentokrát v podobě služby zvané prostě Chat. Dnes tento způsob komunikace umožňuje prakticky každý veřejný WWW server, nejčastěji servery vyhledávacích portálů (např. chat.lide.cz). Chat bývá realizován jako diskusní klub, ve kterém jsou místnosti, kde sedí diskutující u daného tématu. Mimo textu se v chatu používají smajlíci - jednoduché ikony vyjadřující základní lidské pocity (viz např. smile.parcon.cz).

7.4.3.2 ICQ

Dalším komunikačním nástrojem na Internetu, umožňujícím nejen debaty, ale i výměnu dat, příjem a posílání pošty a třeba i telefonování z počítače je komunikační program ICQ (fonetický přepis věty I Seek You). ICQ vyžaduje speciálního klienta, kterého musí mít uživatel instalován na svém lokálním počítači (freeware, získatelný např. na webu http://www.icq.com/). ICQ server ověřuje, který uživatel je připojen, takže lze snadno zjistit s kým lze v daný okamžik komunikovat. Vzhledem k rozšířeným možnostem výměny dat představuje tato služba obvykle závažnou bezpečnostní díru do počítače, kterou se šíří spyware či počítačové viry.

7.4.3.3 MS NetMeeting

Další komunikační prostředek využívající služeb Internetu pochází od fy Microsoft a je součástí rozšířené instalace MS Internet Exploreru. MS NetMeeting umožňuje nejen textovou konverzaci, ale při patřičném vybavení počítače lze komunikovat nejen zvukem ale i obrazem (videokonference). S pomocí MS NetMeetingu lze sdílet i počítačové aplikace (např. společně malovat na jedné tabuli, přenášet soubory apod.). Vhodný server pro zahájení komunikace v ČR je přednastaven v instalaci české verze MS Internet Exploreru – ils.atlas.cz a poskytuje opravdu dostatečnou oblast pro komunikaci všeho typu. Po počátečních problémech se zneužíváním této služby přistoupil Microsoft k přísné personifikaci užívání této služby (viz MSN Messenger).

7.4.3.4 MSN Messenger

Personifikovanou verzí MS NetMeeting se stal MSN Messenger (viz messenger.msn.com), umožňující členům komunikační skupiny využití nejmodernějších technologií dostupných v současnosti na Internetu (internetová telefonie, videokonference atd.). Obě služby se v současnosti doplňují a což odráží i jednotná přístupová registrace k oběma službám v rámci další služby fy Microsoft - NET Passport. Tato registrace umožňuje jednoznačnou identifikaci účastníka diskuse ať již v rámci MS NetMeeting či MSN Messenger.

Shrnutí

Mimo speciální služby umožňující komunikaci mezi uživateli Internetu, zasahuje do této oblasti služba WWW, která díky své univerzálnosti a jednoduchosti, převládá v současnosti i v komunikačních technologiích Internetu. Na rozdíl od speciálních služeb zde postačuje pouze klient služby WWW - Internetový prohlížeč, který každý uživatel Internetu umí poměrně dobře ovládat. Díky své univerzálnosti navíc služba WWW umožňuje komunikaci zvukem i obrazem.

Pojmy k zapamatování

- Chat
- ICQ
- MS NetMeeting, MSN Messenger, NET Passport

Kontrolní otázky

1. Kdo jsou hlavní poskytovatelé služby chat?
2. Vystačí služba ICQ s klientem služby WWW?
3. Jaké možnosti komunikace nabízí služby MS NetMeeting a MSN Messenger?

7.5 Služba přenosu souborů – FTP

Služba FTP umožňuje jednoduchý přenos souborů po Internetu v režimu klient - server. I když vzhledem k bezpečnosti dat pracuje obvykle v režimu autorizovaného přístupu, existuje i možnost jejího anonymního provozu bez nutné registrace na veřejných FTP serverech. S rozvojem možností služby WWW a bezpečnostním rizikům jejího provozu význam služby FTP pomalu klesá, díky jejímu jednoduchému zprovoznění prakticky na libovolném počítači připojeném k Internetu je však stále užitečná. Základní klient služby FTP je součástí protokolu TCP/IP, takže pokud jej máme nainstalovaný lze službu FTP okamžitě používat. V OS Windows se tento klient spouští z příkazové řádky (DOSovské okno) odesláním jednoduchého příkazu ftp. Po spuštění se klient ohlásí změnou systémové proměnné na ftp¿. Nyní lze pomocí příkazu open následovaném adresu vzdáleného FTP serveru požádat o jeho služby (jako adresu ftp serveru lze použít IP i symbolickou adresu). Vzdálený server odpoví žádostí o zadání Login Name (přihlašovací jméno). Pokud nejsme na serveru zaregistrováni a víme, že poskytuje služby i neregistrovanému uživateli (anonymní server) zadáme jako Login Name: anonymous či jiné jméno (např. ftp, ale obvykle server zasílá současně nápovědu pro přihlašovací jméno a heslo. V následné žádosti o heslo se pak neregistrovaný uživatel řídí nápovědou - obvykle je heslem e-mailová adresa uživatele nebo obecné heslo guest (host). Pokud přihlašovací procedura proběhla v pořádku oznámí vzdálený FTP server uživateli, že je připojen a může využívat jeho službu.

V dalším textu je uvedeno několik základních příkazů služby FTP pro vlastní přenos souborů:

- pwd - zjistí jméno stávajícího adresáře (current directory), ve kterém se na vzdáleném anonymním serveru nacházíme
- ls resp. dir - zobrazí seznam všech souborů a podadresářů stávajícího adresáře
- cd - spolu se jménem podadresáře nás převede do tohoto podadresáře (s dvojtečkou přechod na nadřazený adresář).
- get jmenosouboru - soubor daného jména se ze vzdáleného serveru přenese do aktuálního lokálního adresáře na počítači, kde běží klient FTP. Soubor se uloží pod stejným jménem. Nutno vypsat soubor i s příponou, čeština obvykle činí potíže.
- put jmenosouboru - soubor daného jména se přenese z počítače, kde běží klient FTP, do aktuálního adresáře na vzdáleném serveru FTP. Soubor se uloží pod stejným jménem.
- binary, ascii - zajišťují přepínání mezi standardním textovým módem (ASCII) pro textové soubory a binárním módem pro binární soubory (programy, apod.).
- help - vypíše seznam příkazů daného programu pro FTP klienta. Jestliže jako parametr uvedeme nějaký příkaz, získáme jeho stručný popis.
- quit (bye) - ukončuje FTP přenos.

Pokud nechceme ukládat přenášené soubory do aktuálního adresáře odkud byl FTP klient na našem lokálním počítači spuštěn, lze obvykle při přenosu s pomocí parametru /cd jmenoadresare změnit lokální adresář, kam budou soubory ukládány.

Pohodlnější využití služby FTP nabízí klient služby WWW, kde lze FTP přenos spustit zadáním následující adresy do adresní řádky v okně klienta WWW (web prohlížeče):

ftp://DNSadresa

kde DNSadresa je DNS adresou volaného FTP serveru.

Po absolvování přihlašovací procedury lze pak pracovat s adresáři vzdáleného serveru a jeho soubory stejně jako s adresáři a soubory našeho lokálního počítače.

Pro službu FTP existují i specializovaní klienti (např. WebLeech, FTPCute), nebo jsou zabudováni do souborových manažerů (např. Total Commander).

A na závěr několik adres užitečných FTP serverů:

- ftp.zcu.cz
- ftp.jcu.cz
- ftp.sunet.se

Průvodce studiem

Při vlastním studiu pracujte přímo s počítačem a vyzkoušejte zde probírané služby - FTP a Telnet - přímo v akci, tedy v Internetu. K vyzkoušení těchto služeb využijte adresy uvedené přímo v textu, případně využijte služeb některého z vyhledávačů.

7.6 Vzdálený přístup – Telnet

Služba Telnet (Telecommunication Network) umožňuje připojení ke vzdálenému počítači nejen pro přenos souborů, jako je tomu u služby FTP, ale i pro další práci na tomto vzdáleném počítači (spouštění programů, zpracování elektronické pošty atd.), tedy obdobné služby, jaké nám poskytuje server v naší LAN. Telnet je obdobně jako FTP realizován dvojicí klient - server. Vzhledem k tomu, že poskytuje širší služby, vyžaduje prakticky ve všech případech autorizovaný přístup - uživatel tedy musí mít na vzdáleném počítači svůj účet chráněný heslem.

Program Telnet spouštíme jednoduše buď v příkazové řádce nebo v nabídce Spustit... příkazem:

telnet DNSadresa.

nebo z prostředí Web prohlížeče zadáním do adresní řádky:

telnet://DNSadresa

Vzdálený počítač zahájí poté přihlašovací proceduru - zeptá se na uživatelské jméno a příslušné heslo. Základní příkazy zobrazí služba po odeslání příkazu help. Pomocí Telnetu můžeme hledat v automatizovaných knihovnách např. na Web adresách:

telnet://anezka.vc.cvut.cz/ pro knihovnu ČVUT v Praze s Login Name anonym, heslo se nevyžaduje

telnet://omega.nkp.cz/ pro Národní knihovnu v Praze s Login Name visitor, heslem je e-mailová adresa.

Nutno podotknout, že s rozvojem služby WWW jsou mnohé funkce Telnetu (např. knihovní katalogy) nahrazeny mnohem komfortnějšími metodami.

Shrnutí

Hlavní funkci Internetu - přenos informace mezi jeho uživateli - zabezpečují tzv. informační služby, z nichž nejpoužívanější jsou WWW a elektronická pošta. Vedle těchto hlavních služeb existují služby specializované na konkrétní typ přenosu informace, kam patří služba přensou souborů FTP a služba připojení ke vzdálenému počítači Telnet.

Pojmy k zapamatování

- informační služby Internetu
- služba přenosu souborů FTP
- služba připojení ke vzdálenému počítači Telnet

Kontrolní otázky

1. Vyjmenuj základní informační služby Internetu.
2. Vysvětli k čemu slouží služba FTP.
3. Popište postup (a současně proveďte) stažení souboru se jménem index.zip, umístěném v adresáři pub/win/winsite/win95 ze serveru ftp.zcu.cz za pomoci služby FTP.
4. Vysvětli k čemu slouží služba Telnet.

Část III

Bezpečnost

Již předchozí kapitola upozornila na možnost napadení počítače připojeného k Internetu uživateli, jejichž zájmem je spíše jiným škodit, než jim poskytovat služby či informace. Proto by každý uživatel Internetu měl být schopen rozeznat základní možnosti napadení svého počítače a umět těmto napadením předcházet využitím všech dostupných bezpečnostních prvků.

Připojení počítače k Internetu přináší mimo pozitiva přístupu k bohatým informačním zdrojům i negativa spojená s nebezpečím napadení připojeného počítače programy a uživateli, kteří nalézají svou zábavu či možnost obohacení právě v ohrožení počítačů jiných uživatelů Internetu.

Kapitola 8

Počítačové viry a základní principy obrany proti jejich působení

Principielně nejčastější možnost ohrožení počítače připojeného k Internetu představují viry – ty se mohou ovšem šířit i jinými způsoby než po Internetu, zejména při přenosu SW z počítače na počítač. Klasické viry z období počátku rozvoje počítačových technologií se šířily převážně tímto způsobem prostřednictvím spustitelných programů, do nichž se při své činnosti zabudovávaly. Tento způsob šíření umožňoval snadnou detekci virové infekce, protože u většiny spustitelných souborů byla známa jejich správná velikost a připojení viru k programu jeho velikost měnilo. Situace se prudce zhoršila s existencí nové generace virů - makrovirů. Tyto viry využívají ke své funkci speciální programovací jazyk pro tvorbu maker, používaný zejména pro práci s dokumenty v nejrůznějších textových či tabulkových editorech. Takové soubory již nemají definovanou velikost, takže jednoduchá možnost odhalení infekce jako v předchozím případě padá a tak každý potencionální cíl makroviru musí antivirový program prozkoumat, zda se v něm nevyskytují sekvence typické pro konkrétní makrovir. Takový postup je samozřejmě podstatně časově náročnější operace než prosté porovnávání velikosti souborů.

Jiný typ viru představují trojští koně, což mohou být programy, které mohou navenek vykonávat užitečné funkce, ale skrytě vykonávají další, škodlivé funkce jako je např. odposlech klávesnice, který může vést k prozrazení hesel používaných uživatelem nejen pro přístup do počítače, ale i k dalším Internetovým službám, jako je např. Internetové bankovnictví. Rovněž se tento typ škodlivých programů nazývá jako adware či spyware. Množí-li se tento typ viru sám prostřednictvím sítě, říká se mu obvykle červ. Tento typ představuje spustitelný soubor (může být opět makrem, např. nechvalně známý virus Melissa či „I Love You“), který se množí sám prostřednictvím sítě tak, že se rozesílá jako e-mail z napadeného počítače na všechny e-mailové adresy, které v napadeném počítači najde. Rozesílání e-mailů nebo dotazů na vybraný server z nakažených počítačů synchronizované do stejného okamžiku pak může vést ke zhroucení tohoto serveru - tento útok se nazývá Distributed Denial of Service (DDoS) a zažil je již mnohý z důležitých serverů na Internetu (např. servery fy Microsoft). Základem obrany proti virům je antivirový program, který ovšem může účinně bojovat proti virům pouze tehdy, je-li pravidelně (nejlépe automaticky) aktualizován. Antivirový program hlídá obsah paměti počítače na výskyt virové infekce, umožňuje kontrolovat elektronickou poštu a je dokonce schopen v reálném čase kontrolovat data při práci s informačními zdroji Internetu, např. při prohlížení WWW stránek. Mnohé počítačové firmy (i české, např. AVAST) nabízí své antivirové programy pro domácí použití

bezplatně (tzv. freeware), ale i investice řádově ve stokorunách za jednu instalaci dobrého antivirového programu se skutečně v dnešním světě počítačů rychle vrátí. Ztráta důležitých dat vlivem virové infekce je mnohdy nenahraditelná a což teprve, pokud nějaký špiónský program zjistí heslo k našemu účtu!

Hlavní informační službou Internetu je v současnosti služba WWW. Klasické WWW stránky byly psány v jazyce HTML, který vlastně jen popisuje způsob zobrazení informací ve webovém prohlížeči a tak nemůže být zneužit k jiným účelům. Vývoj ale dal vzniknout dalším technologiím, kdy jsou do základní struktury WWW stránky vloženy další struktury - spustitelné aplikace (napsané v jazycích Java či ActiveX). Stránky tím sice získávají dynamičnost a tedy i nové možnosti, ale současně jsou tyto technologie zneužitelné k napadení počítače a získání informací z něj v případě jeho připojení na příslušnou WWW stránku. Prohlížeč sice takové spustitelné aplikace při běhu kontroluje, zda nevykonávají nějaké nebezpečné operace, ale pokud tato běžící aplikace požádá uživatele o rozšíření pravomocí a on tak bez rozmyslu učiní, může se tento program snadno stát pánem ovládající daný počítač. Z tohoto hlediska jsou aplikace vytvořené v ActiveX ještě nebezpečnější než aplikace napsané v Javě (ta má implementováno více bezpečnostních prvků proti zneužití). Při prohlížení Internetových stránek tak může uživatel zákazem spouštění těchto aktivních prvků (viz předchozí kapitola 12 o nastavení Internetového prohlížeče) výrazně zvýšit bezpečnost svého počítače, ovšem za cenu toho, že mnohé stránky ztratí při prohlížení značnou část svých komponent. Je tak nutno zvolit vhodný kompromis mezi bezpečností a zobrazením maxima prvků na WWW stránkách.

Ještě větší nebezpečí představují některé další služby Internetu určené ke komunikaci mezi uživateli Internetu v reálném čase. Obzvláště velkou bezpečnostní díru představuje komunikace za pomocí ICQ. Uživatelé spolu komunikují nešifrovaně (dokonce i přihlašovací procedura včetně přenosu hesla probíhá nešifrovaně), takže není nejmenší problém je odposlouchávat. Protože ICQ umožňuje přenos souborů mezi uživateli, je zde i zvýšené nebezpečí přenosu virů. Mnohé z nich se totiž maskují třeba jako nevinné obrázky - ICQ zobrazuje při přijímání souboru jen určitý počet znaků, takže není problém vytvořit spustitelný soubor nazvaný obrazek.jpg.exe, kde při vhodné volbě délky názvu nebude přípona .exe zobrazena. Uživatel potom v domnění, že prohlíží obrázek, spustí ve svém počítači vir. Přitom obrana je poměrně jednoduchá, stačí soubor nejprve uložit na disk a zobrazit si nejprve jeho vlastnosti - pak snadno zjistíme plný název a tedy i skutečnou funkci souboru. Obdobně využívají nekompletní zobrazování jména souboru i viry šířící se pomocí e-mailu.

Důležitou obranou proti napadení našeho počítače zvenčí je mimo aktualizovaný antivirový program i aktualizovaný operační systém a všechny programy používané ke komunikaci na Internetu. Mnozí nepřátelští uživatelé Internetu (hackeři) využívají chyb v OS či programech právě pro průnik do systému vašeho počítače a k jeho ovládnutí - tento útok se nazývá Denial of Service (DoS). Typický případ představuje OS MS Windows XP a virus Lirva, využívají bezpečnostně neošetřený přístup přes některé komunikační porty.

Dobrou ochranu proti odposlechu přenosu dat po Internetu za pomoci webového prohlížeče představuje šifrování, o kterém bude podrobněji pojednáno dále v kapitole 11. Komunikace mezi serverem a prohlížečem je šifrována symetrickou šifrou, přičemž kvalitu použitého šifrování můžeme ovlivnit i my sami. Postačí aktualizovat svůj prohlížeč na použití maximální délky šifrovacího klíče - určitě nejsou postačující hodnoty jeho délky pod 80 bitů. V MS Internet Exploreru zjistíme délku šifrovacího klíče snadno výběrem položky O aplikaci Internet Explorer z menu Nápověda. V tomto místě je i odkaz na případné provedení bezpečnostních aktualizací. Stejně jako komunikace v rámci služby WWW může probíhat šifrovaně, lze šifrovaně používat i elektronickou poštu, k dispozici jsou i freewarové zásuvné moduly podle standardu PGP, použitelné ve většině běžně používaných e-mailových klientů. Důležité, zejména jako obrana před červy, je i podepisování všech e-mailů (samozřejmě nejlépe za využití digitálního podpisu), takže příjemce, který ví, že své e-maily podepisujete, může s nepodepsaným e-mailem od vás zacházet obezřetněji a včas

tak zachytit množícího se červa.

Příkladem implementace bezpečnostních mechanismů na úrovni přenosu dat, které navíc zajišťují soukromí přenášených dat, může být vrstva Secure Sockets Layer (SSL) původně vyvinutá firmou Netscape, či Private Communications Technology od Microsoftu. Ani Secure Sockets Layer, ani Private Communications Technology však nejsou jen kryptografickými aplikacemi, ale rovněž poskytují aplikační programové rozhraní (API) pro programátory, vytvářející aplikace na úrovni přenosu dat.

Základní principy obrany před virovou nákazou:

- Spolehlivý a aktualizovaný antivirový program i pro kontrolu komunikace po Internetu.
- Aktualizovaný OS počítače a programy používané pro komunikace po Internetu.
- Pravidelná kontrola počítače programem odhalujícím skryté škodlivé programy - adware a spyware.
- Použití osobního firewallu (viz následující text).
- Zákaz automatického otevírání příloh a spouštění aplikací v těchto přílohách v poštovním klientovi.
- E-maily s podezřelým odesílatelem či názvem (např. I Love You) neotevírat, ale okamžitě mazat. Stejně tak nespouštět spustitelné soubory z příloh pokud není známa jejich funkce.

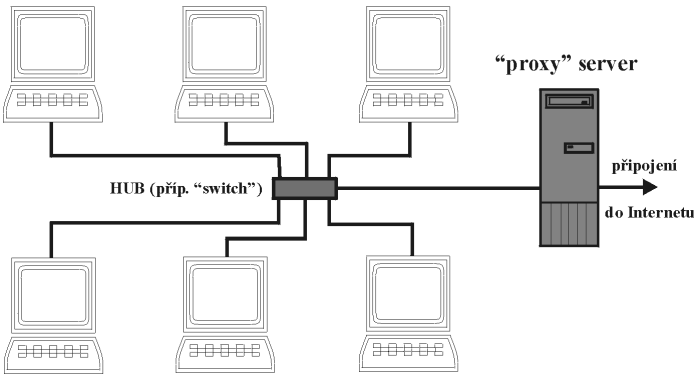
Průvodce studiem

Mnoho firem vyvíjejících antivirové programy poskytuje omezené verze svých produktů zdarma pro nekomerční či domácí použití (např. česká firma). Nic tedy nebrání uživateli používat moderní a aktualizovaný antivirový program. Navíc při objevení se nějaké závažné virové nákazy poskytuje většina firem operujících v této oblasti zdarma jednoúčelové antiviry likvidující příslušnou infekci. Objevení se těchto jednoúčelových antivirů na Internetu se prakticky počítá na hodiny od chvíle projevení se této nákazy, takže lze velmi rychle reagovat na nastalou situaci a zabzepečit příp. vyléčit svůj počítač.

Kapitola 9

Proxy-server

Proxy-server představuje aplikaci, zabezpečující propojení LAN s Internetem pomocí jediné IP adresy. Tato aplikace běží totiž na počítači připojeném do Internetu a ostatní počítače v síti přistupují do Internetu přes tento počítač za řízení aplikací proxy-server, jak ukazuje obrázek 9.1. Mimo ekonomické výhody přináší toto řešení i výhody snadného sledování a řízení provozu mezi počítači v LAN a Internetem, takže jsou chráněny před přístupem neoprávněných osob mimo LAN. Aplikace proxy-server obvykle pracuje současně ve funkci tzv. firewallu. Typickým příkladem takovéto aplikace je program WinProxy.



Obrázek 9.1: Proxy server jako provek oddělující LAN od Internetu.

Řízení provozu mezi počítači v LAN a Internetem je realizováno tak, že každý počítač v LAN musí nejprve zaslat žádost o spojení s jiným počítačem (serverem) v Internetu počítači, na kterém běží proxy-server. Tento počítač po vyhodnocení žádosti buď spojení zamítne nebo spojení naopak povolí a pak jej sám žádajícímu počítači zprostředkuje. Protože ale veškerý datový tok jde neustále přes něj, může dále kontrolovat jeho obsah. Naopak, pokud bude nějaký počítač vně LAN chtít navázat spojení s počítačem v LAN, proxy-server např. na základě tabulky povolených přístupových IP adres toto spojení buď umožní nebo mu zabrání. Do vnitřní sítě LAN tak mohou opravdu přistupovat jen jednoznačně definovaní oprávnění uživatelé - např. pracovníci organizace na služební cestě, zákazníci firmy apod..

Kapitola 10

Firewall

Firewall (v doslovném překladu protipožární zeď) je softwarové nebo hardwarové zařízení, které zabraňuje neautorizovanému přístupu buď do celé LAN nebo do jednotlivého klientského počítače (osobní firewall). Firewall při své práci využívá tzv. filtry tří úrovní:

Bezstavové filtry (filtry na úrovni paketů) Filtry na úrovni paketů zasílají nebo blokují příchozí pakety výhradně na základě povahy paketu (např. podle použitého protokolu) bez ohledu na jeho historii či stav (IP adresy a porty). Taková jednoduchá pravidla filtrování provozu dovolují rychlý přenos dat, ale malou bezpečnost.

Filtr okruhů rozhoduje o směrování paketu nejen podle jeho obsahu, ale také podle jeho historie. Filtrování zohledňuje zdrojovou a cílovou adresu a typ služby. Z hlediska činnosti tyto filtry poskytují vyšší bezpečnost bez výrazného zpomalení datového toku. Firewall se v tomto případě chová jako brána, se kterou primárně komunikuje klient a ta propouští podle nastavených kritérií data až k jejich cíli.

Filtry na úrovni aplikací pracují na proxy-serveru, který odděluje aplikační server od Internetu. Klient se připojuje k firewallovému serveru, jako by to byl příslušný aplikační server. Proxy-server před odesláním požadavku na aplikační server vyhodnotí žádost a pokud je neoprávněná, zamítne ji. Protože vyhodnocení žádosti probíhá obvykle podle složitých pravidel dané aplikace, dochází k výraznému snížené rychlosti přenosu, ovšem bezpečnost celého systému je v tomto případě nejvyšší.

Pojmy k zapamatování

- Počítačové viry - klasické, makroviry, trojské koně, červi.
- Adware a spyware.
- Firewall a proxy-server.

Kontrolní otázky

1. Jaký je rozdíl mezi klasickým počítačovým virem a makrovirem?
2. Jakou funkci zabezpečuje firewall?
3. Jakým způsobem blokuje proxy-server útoky z Internetu do chráněné LAN?

Kapitola 11

Základy kryptografie a bezpečnosti

Kryptografie se zabývá kódováním dat do podoby, nečitelné neoprávněnou osobou. Kódování se provádí pomocí šifrovacího algoritmu (matematická operace). Mimo kódování dat pro zajištění jejich důvěrnosti je třeba při provozu na Internetu zajistit i autentizaci těchto dat, tedy zabezpečit správnou totožnost uživatele nebo procesu (serveru), s nímž je komunikace vedena.

11.1 Metody šifrování

Existují dva základní typy šifrovacích metod - symetrické (konvenční) a asymetrické šifrování (neboli šifrování veřejným klíčem).

Symetrické šifrování

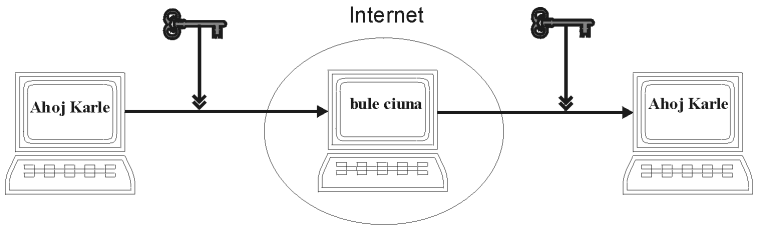
Při symetrickém šifrování používají odesílatel a příjemce dat stejný šifrovací klíč, jak ilustruje obrázek 11.1. Důvěrnost je zajištěna tím, že je tento klíč tajný, proto se symetrickému šifrování také říká šifrování s tajným klíčem. Vlastní metody šifrování lze rozdělit do dvou skupin. Při blokovém šifrování se zašifruje blok dat o pevné délce jako celek. Při proudovém šifrování se data šifrují bit po bitu.

Standard šifrování dat algoritmem DES (Data Encryption Standard) je příkladem blokového šifrovacího algoritmu, který pomocí 56bitového klíče zpracovává bloky dat dlouhé 64 bitů. I při poměrně krátkém klíči je tento algoritmus pokládán za dostatečně bezpečný pro běžný provoz na Internetu a navíc je extrémně rychlý. Tam, kde nedostačuje bezpečnost klasického DES algoritmu, bývá využívána jeho modifikace nazvaná Triple-DES. Podle něj se nejprve data zašifrují klasicky podle algoritmu DES. Tato zašifrovaná data se opět zašifrují podle druhého klíče a data z tohoto druhého šifrování se opět zašifrují podle třetího klíče. Všechny tři klíče jsou přitom vzájemně nezávislé.

Rovněž algoritmus IDEA (International Data Encryption Algorithm) blokovým šifrovacím mechanismem, který ovšem používá klíč o délce 128 bitů. Algoritmus IDEA je evropským standardem a ve srovnání s algoritmem DES nezaostává v rychlosti a mírně jej převyšuje v bezpečnosti.

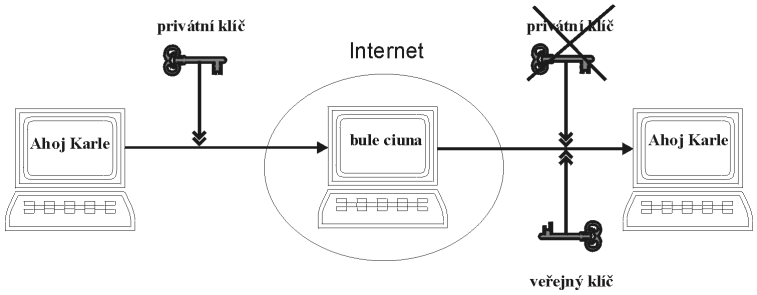
Asymetrické šifrování

V algoritmech asymetrického šifrování se na rozdíl od symetrického používají dva různé klíče. První klíč je privátní a zná jej pouze vlastník klíče. Druhý klíč dává vlastník privát-



Obrázek 11.1: Princip symetrického šifrování zpráv tajným šifrovacím klíčem.

ního klíče veřejně k dispozici všem, s nimiž šifrovaně komunikuje - veřejný klíč. Funkce obou klíčů je dvojí - data zašifrovaná privátním klíčem lze dešifrovat pouze příslušným veřejným klíčem a data zašifrovaná veřejným klíčem (např. odpověď příjemce odesílateli) pouze příslušným privátním klíčem, což ozřejmuje obrázek 11.2. Tato vlastnost asymetrického šifrování se využívá rovněž při realizaci digitálních podpisů.



Obrázek 11.2: Princip asymetrického šifrování zpráv s provátním a veřejným šifrovacím klíčem.

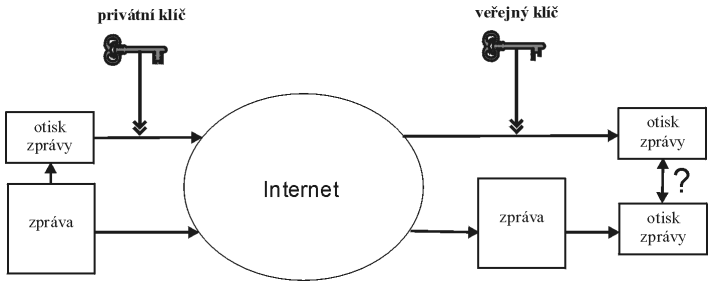
Algoritmus RSA byl pojmenován podle svých tvůrců (Rivest, Shamir, Adieman), zakládajících členů výboru RSA Data Security. Principem realizace klíčů pro asymetrické šifrování algoritmu RSA je předpoklad, že lze jen obtížně rozložit dostatečně velké číslo na součin dvou prvočísel, na nichž je založena každá dvojice klíčů. Z daného veřejného klíče se dá tedy jen poměrně dosti obtížně zjistit odpovídající privátní klíč. Algoritmus RSA byl důkladně analyzován a obecně se považuje za bezpečný, jestliže pracuje s dostatečně dlouhým klíčem. Proto se uvažuje se zavedením délky klíče až 2048 bitů, což by mělo postačovat i do budoucna, i když s rostoucím výkonem počítačů roste nebezpečí prolomení šifry „hrubou silou“.

11.2 Algoritmy otisku zprávy

Algoritmy otisku (hash) zpráv, Message Digest Algorithms (MDA), společně s asymetrickým šifrováním vytváří základ metody digitálních podpisů. Z každé zprávy je vybrán vhodným algoritmem proměnný počet bitů, z níž se vytvoří řetězec o pevné délce, charakteristický resp. jedinečný pro tuto zprávu. Algoritmy MD2, MD4 a MD5 jsou algoritmy otisku zprávy, které vytváří z každé zprávy 128bitový otisk. Algoritmus MD2 je nejpomalejší a MD4 nejrychlejší. Algoritmus MD5 je variantu algoritmu MD4 s vyšší bezpečností. Další algoritmus pro vytváření otisku zprávy se jmenuje SHA (Secure Hash Algorithm) a vytváří 160bitový otisk, čímž je bezpečnější než algoritmy MDA.

11.3 Digitální podpisy

Digitální podpisy umožňují ověření obsahu zprávy a totožnosti jejího odesílatele. Pro realizaci digitálního podpisu se využívají technologie asymetrického šifrování a otisku zprávy. Základní princip vytvoření digitálního podpisu je poměrně jednoduchý. Odesílatel vytvoří otisk odesílané zprávy a zašifruje jej svým privátním klíčem. Tento zašifrovaný otisk odešle společně se zprávou příjemci. Příjemce si vytvoří svůj otisk zprávy a porovná jej s dešifrovaným otiskem zprávy od odesílatele. Pokud oba otisky souhlasí, je zaslaná zpráva originální (neupravená během své cesty Internetem). Princip demonstruje obrázek 11.3. Současně je potvrzena totožnost odesílatele, protože dekódování je provedeno jeho veřejným klíčem. Pro digitální podpisy se používá šifrovací algoritmus RSA či jiné algoritmy k tomuto účelu speciálně vyvinuté, jako je DSS (Digital Signature Standard) či EC (Eliptic Curve). Algoritmus DSS se ukázal jako méně spolehlivý, takže je dnes využíván jen minimálně, naopak algoritmus EC patří mezi nejbezpečnější šifrovací algoritmy dneška.



Obrázek 11.3: Princip digitálního podpisu využívajícího asymetrické šifrování otisku zprávy.

11.4 Autentizace

Výše zmíněný digitální podpis představuje jednu z možností autentizace dat zasílaných po Internetu. Obecně autentizace potvrzuje, že oba partneři při elektronické komunikaci jsou skutečně ty identity, za které se prohlašují. Mimo digitální podpis (resp. vlastnictví konkrétního šifrovacího klíče) poskytují autentizační služby i další bezpečnostní mechanismy používané při komunikaci na Internetu - např. bezpečnostní mechanismus SSL (Secure Socket Layer), používaný při zabezpečené komunikaci v rámci služby WWW - protokol HTTPS (HyperText Transfer Protocol – Secure) či v rámci služby elektronické pošty.

Další metodu autentizace vyvinul Microsoft v podobě protokolu NTLM Challenge/Response. Tento autentizační mechanismus je založen na použití tajného hesla. Klient požádá server o připojení načež server odešle klientovi výzvu k přihlášení (autentizaci). Klient na tuto výzvu odešle odpověď, kterou tvoří otisk jeho uživatelského hesla. Server systému Microsoft Windows NT na základě uloženého hesla daného uživatele vypočte svůj otisk a může tak snadno ověřit, jestli je odpověď správná. Výhodou tohoto systému je, že se nikdy neposílá skutečné heslo uživatele, pouze jeho otisk.

11.5 Certifikáty

Jedním z hlavních problémů asymetrického šifrování je možnost ověření, zda určitý veřejný klíč náleží konkrétnímu uživateli Internetu, který to tvrdí. Tento problém vyřešil institut

certifikátů. Certifikát jednoznačným a ověřitelným způsobem definuje vazbu uživatele a jeho klíče včetně doby platnosti této vazby (certifikáty se vydávají jen na omezenou dobu). Certifikáty vydává certifikační autorita - Certification Authority (CA). Úlohu CA hrají tzv. certifikační servery, které podle stanovených pravidel udržují seznam certifikátů včetně doby jejich platnosti. Každý uživatel Internetu může vstoupit do databáze certifikačního serveru a ověřit si platnost uváděného certifikátu (to mohou dělat i servery informačních služeb Internetu případně i klienti těchto služeb). Certifikační servery provozují důvěryhodné organizace (např. Microsoft či Netscape), které obdržely oprávnění od nadřazené certifikační autority (stromová struktura CA). Základní (kořenová) certifikační autorita má oprávnění definováno zákonem (USA).

Formát a syntaxe certifikátů (ale i autorizačních služeb) je definována standardem X.509. Certifikáty standardu X.509 využívají různé standardy, spojené s potřebami důvěrnosti a autentizace dat v rámci různých služeb Internetu - například SSL, Secure-HTTP či PEM (Privacy Enhanced Mail). Protože základním smyslem certifikátů je, jak již bylo řečeno, spojit jednoznačně uživatele s jeho veřejným klíčem, musí certifikát obsahovat údaje jako identifikátor algoritmu certifikační služby; jméno autority, která certifikát vydala; období platnosti certifikátu a informace o veřejném klíči.

Průvodce studiem

I když většina šifrovacích metod je vyhrazena zejména pro profesionální využití při tvorbě prostředků pro zabezpečenou komunikaci po Internetu, i jeho běžný uživatel se stále častěji setkává s těmito technologiemi. Stále více WWW serverů využívá pro komunikaci s klientem šifrovaný přenos zpráv na základě bezpečnostního rozšíření protokolu HTTP - HTTPS (viz kapitola 14).Typický případ představuje server www.msn.com www.msn.com www.msn.com www.msn.com www.msn.com jednoho z předních výrobců softwaru pro osobní počítače - fy Microsoft. A s připravovanou komunikací občana i firem s orgány státní zprávy přenáší problém zabezpečené komunikace do reálné roviny, která se záhy může dotknout každého z nás. Koneckonců uživatelé tzv. internetového bankovnictví již důvěrně znají z vlastní zkušenosti co je to digitální podpis či zabezpečená komunikace po Internetu.

11.6 Použití šifrování v praxi

Základní problém praktické aplikace je, jakou metodu šifrování - symetrickou nebo asymetrickou - při komunikaci v Internetu použít? Nejobvyklejší praktické řešení tohoto problému vede k současnému použití obou metod. Protože asymetrické šifrování je mnohem pomalejší, ale pro změnu bezpečnější než symetrické, používá se k zašifrování dat náhodně vygenerovaný privátní klíč symetrického algoritmu šifrování. Tento privátní klíč se posílá při zahájení komunikace protějšku po síti zašifrovaný ovšem pomocí asymetrické šifry. Zbývající část komunikace tak probíhá s pomocí symetrického šifrování, které komunikaci minimálně zdržuje.

Konkrétním příkladem takového postupu je požadavek bezpečné elektronické transakce při obchodování na Internetu. Pro tyto účely byl vyvinut společnostmi Visa a MasterCard ve spolupráci s fy Microsoft, Netscape, IBM a GTE protokol SET (Secure Electronic Transaction). Protokol má tři základní součásti - obchodní popis, vlastní popis protokolu a návod pro programátory. Technologie protokolu SET slouží na Internetu k bezpečnému přenosu informací o kreditních kartách a současně definuje rozhraní API, nutné pro programování komerčních aplikací s tímto protokolem. Pro šifrování dat používá protokol SET algoritmus DES, přičemž pro šifrování symetrického šifrovacího klíče a čísla kreditní karty při přenosu po Internetu je použit algoritmus RSA.

Shrnutí

Zabezpečení přenosu informace v Internetu proti jejímu odposlechu či pozměňování zabezpečuje kryptografie, jejíž hlavní metodou je šifrování. Při zabezpečení komunikace na Internetu se používají dvě základní metody šifrování - symetrické a asymetrické. Při symetrickém šifrování se používá jediný tajný klíč, při asymetrickém jsou klíče dva - privátní a veřejný. Existence dvou klíčů v metodě asymetrického šifrování je použita v technologii digitálního podpisu zpráv ve spojení s technologií otisku zprávy.

Pojmy k zapamatování

- Symetrické šifrování.
- Asymetrické šifrování.
- Privátní a veřejný klíč.
- Otisk zprávy.
- Digitální podpis.
- Certifikace digitálních podpisů.

Kontrolní otázky

1. Jaký je rozdíl mezi metodami symetrického a asymetrického šifrování?
2. V jakém vztahu jsou vůči sobě privátní a veřejný klíč?
3. Popiš základní principy technologie digitálního podpisu.
4. Co znamená institut certifikace v oblasti digitálních podpisů?

Část IV

WWW stránky

Služba World Wide Web, zkráceně WWW, se stala vůdčí službou informačních služeb Internetu díky využití desítek let vyvíjené technologie hypertextových dokumentů, umožňujících vzájemné propojení různých inmformačních zdrojů bez ohledu na jejich lokalizaci v síti. I když počátky této technologie sahají do období, kdy neexistovaly prostředky pro její realizaci, její skutečný zrod lze datovat do devadesátých let 20. století. Již Vannevar Bush v roce 1945 předpověděl existenci takové služby, a již v šedesátých letech 20. století se Douglas Engelbert a posléze Ted Nelson snažili zrealizovat technologii vzájemně provázaných dokumentů. Ovšem doba a hlavně technologie dozrály až na konci devadesátých let 20. století, kdy počítačové technologie již dosáhly bodu, umožňující realizaci tak náročného projektu..

Kapitola 12

Internetové prohlížeče a jejich nastavení

Internet bez inteligentního a uživatelsky příjemného klientského rozhranní by těžko dosáhl v tak krátkém čase tak ohromného rozmachu a označení fenoménu doby. I zakladatel fy Microsoft, Bill Gates, vidí budoucnost počítačových technologií právě v rozvoji Internetu. A i to je důvod, proč tato jedna z vůdčích firem v oblasti vývoje počítačového softwaru, věnuje takovou pozornost vývoji vlastního Internetového prohlížeče jako jednoho z nejdůležitějších produktů firmy. Proto nelze v našem přehledu Internetových technologií nevěnovat samostatnou kapitolu tomuto nejdůležitějšímu klientovi Internetových informačníéch služeb.

12.1 Internetové prohlížeče (browsery)

Internetový prohlížeč (webový prohlížeč, WWW klient, WWW browser) je program zobrazující obsah zadané internetové adresy, zejména webových stránek, ale umí obvykle pracovat i s jinými službami Internetu (FTP, Telnet apod.). Internetových prohlížečů existuje celá řada, prvním grafickým webovým prohlížečem byl Mosaic, vytvořený v National Center for Supercomputing Applications (NCSA). Dnes nejznámějšími prohlížeči jsou Microsoft Internet Explorer a Netscape Navigator, jako alternativní prohlížeče pak Opera, Neoplanet, Arachne nebo čistě textový Lynx. V poslední době zažívá renesanci jeden z prvních prohlížečů Mozilla, univerzálně použitelný v prostředí MS Windows či Linux.

Důležité ovládací prvky a nastavení internetového prohlížeče si ukážeme u nejrozšířenějšího prohlížeč pro OS MS Windows – MS Internet Explorer v.6. U alternativních prohlížečů se mohou jednotlivé nabídky či nastavení mírně lišit, základní funkce a ovládání jsou však podobné. Protože základy práce s prohlížečem byly již probrány v předmětu Základy práce s PC, zde se budeme věnovat skutečně jen otázkou nastavení prohlížeče.

12.1.1 Nastavení připojení počítače k Internetu

Prvním krokem úspěšné práce s prohlížečem je nastavení připojení počítače k síti Internet (pokud spouštíme prohlížeč poprvé po instalaci počítače, resp. jeho připojení k síti). V rámci OS musí být provedena instalace sítě (viz kapitola **??**), resp. tato instalace může proběhnout v rámci nastavení připojení k Internetu podle následujícího schématu (průvodci pro instalaci sítě a nastavení připojení k Internetu jsou v OS MS Windows lokalizovaní

v nabídce `Připojit`, která je umístěna v hlavní nabídce otevírající se po stisku tlačítka `Start`):

1. V prvním okně nás `Průvodce` přivítá a oznámí, co všechno dokáže. Po stisku tlačítka `Další` nám pak nabídne čtyři různé možnosti. Zatržením prvního políčka `Připojit k Internetu` a klepnutím na tlačítko `Další` zvolíme možnost nastavení připojení k Internetu. V případě zatržení třetího políčka s názvem `Nastavit síť pro domácnost nebo malou kancelář` přejdeme na průvodce nastavení připojení k síti, jak bylo diskutováno v kapitole **??**.

2. Pokud máme již u některého z poskytovatelů připojení k Internetu (ISP) nadefinován svůj účet, zvolíme políčko Nastavit připojení ručně, jinak políčko Vybrat ze seznamu poskytovatelů....

3. V případě výběru Nastavit připojení ručně, jsme v dalším okně vyzváni k zadání způsobu připojení, v případě výběru Připojení pomocí modemu (nejběžnější způsob pro domácí uživatele) následuje poté okénko pro zadání názvu tohoto připojení a následně je nastavení dokončeno zadáním telefonního čísla ISP a parametrů již existujícího účtu u tohoto ISP (jméno uživatele a jeho heslo). Tímto způsobem se lze připojit i k ISP, kteří poskytují službu připojení k Internetu zdarma a anonymně (není třeba mít osobní uživatelský účet u ISP) - např. Internetový portál iDnes nabízí tuto službu na telefonním čísle 971101201 s uživatelským jménem idnes a heslem opět idnes.

4. V případě, že ještě nemáme u žádného ISP založen uživatelský účet, zvolíme políčko Vybrat ze seznamu poskytovatelů ..., přičemž v následujícím okně je nabídnuta služba MSN od společnosti Microsoft, případně výběr jiného ISP přes místní nabídku dosažitelnou přes odkazovací službu na čísle 233090016. Po výběru ISP ze získané nabídky bude vytvořen osobní účet uživatele Internetu u vybraného ISP a poté již nic nebrání ve využívání služeb Internetu pomocí tohoto nastaveného připojení.

12.1.2 Základní nastavení webovského prohlížeče

Před zahájením využívání služeb Internetu je ovšem vhodné zkontrolovat zejména bezpečnostní nastavení používaného prohlížeče. U prohlížeče MS Internet Explorer je to zejména nabídka Možnosti Internetu umístěná v roletovém menu souhrnně nazvaném Nástroje v horní části základního okna prohlížeče. Po vybrání této nabídky se objeví okno s řadou podnabídek. V té prvé, nazvané Obecné, jde především o nastavení tzv. domovské stránky, to je stránky, která se objeví v okně při startu prohlížeče. Mimo tuto možnost nabízí podnabídka ještě nastavení ukládání dočasných souborů na lokální počítač (tyto dočasné soubory jsou využívány k rychlejšímu zobrazení stránek, které byly v nedávné minulosti navštíveny) a historie navštívených stránek. Je vhodné čas od času provést vymazání těchto souborů a zejména uložených souborů cookie (textové soubory sbírající informace o práci na klientském počítači, resp. o jeho uživateli, informace jsou následně odesílány tvůrci příslušného souboru cookie, viz www.sezob.cz/tiptrik/cookie.htm) www.sezob.cz/tiptrik/cookie.htm) www.sezob.cz/tiptrik/cookie.htm) www.sezob.cz/tiptrik/cookie.htm) www.sezob.cz/tiptrik/cookie.htm) a stejně tak historie navštívených stránek. Promazávání se sice automaticky odehrává na základě zde nastavených pravidel, ale nemusí být zcela dokonalé (obzvláště, nastavíme-li dlouhé časové intervaly pro ukládání těchto souborů).

Z dalších podnabídek je z bezpečnostního hlediska důležitá podnabídka Zabezpečení, která umožňuje jemně nastavit bezpečnostní pravidla pro provoz v různých segmentech sítě, resp. Internetu. Mimo standardně přednastavených úrovní zabezpečení lze provést individuální

nastavení zejména prvků, které zvyšují nebezpečí napadení počítače zvenčí (prvky ActiveX a Java), což jsou samostatně spustitelné programy na lokálním počítači, realizující zejména její dynamické prvky, ale zneužitelné i k jiným účelům v neprospěch návštěvníka WWW stránek (např. přesměrování telefonického připojení na jiného ISP s podstatně vyššími cenami za připojení). Obdobně lze v další podnabídce Osobní údaje upravit pravidla používání souborů cookie. V další podnabídce Obsah lze mimo omezení zobrazování vybraných WWW stránek nastavit metody certifikace komunikace po Internetu. Poslední významná podnabídka z hlediska bezpečnosti komunikace na Internetu nese název Upřesnit a obsahuje řadu možností doladění bezpečnostních pravidel a způsobu zobrazování navštívených WWW stránek. Jedná se zejména o nastavení práce s programy v jazyce Java a se skripty, dále práce s FTP a nastavení systému zabezpečení komunikace včetně certifikace serverů a programů vystupujících při komunikaci na Internetu.

Poslední důležitá položka nastavení aplikace MS Internet Explorer (a samozřejmě i dalších browserů) je správná volba kódování znaků národní abecedy pro zobrazované dokumenty. Pokud tvůrce WWW stránek neuvede korektně použitý způsob kódování znaků národní abecedy v hlavičce HTML dokumentu, nebude pravděpodobně prohlížeč schopen správně zobrazovat specifické znaky české abecedy a zobrazovaný text se tak může stát obtížně či zcela nečitelným. Položka pro toto nastavení se nalézá v nabídce Zobrazit pod položkou Písma. Pro správné zobrazování znaků české abecedy je nutné, aby zde byla nastavena středoevropská znaková sada, kde je ovšem výběr z několika možností kódovacích tabulek, nejčastěji však bývá v HTML dokumentech používáno kódování standardu MS Windows.

Průvodce studiem

Nastavení pravidel bezpečného přístupu ke službě WWW by měl věnovat zvýšenou pozornost každý uživatel Internetu. I když moderní operační systémy včetně Internetových prohlížečů, mají zabudován poměrně solidní systém zabezpečení, jejich automatické přednastavení málokdy odpovídá potřebám toho určitého uživatele. Proto vždy překontrolujet alespoň základní nastavení bezpečnostních prvků vašeho prohlížeče, tak jak jej popisuje tato kapitola. Počítač, používaný pro přístup k našemu účtu v bance musí pracovat s podstatně přísnějšími bezpečnostními pravidly, než počítač, který slouží jako prostá stanice pro brouzdání Internetem.

12.1.3 Off-line browsery

Off-line browsery umožňují stažení celých www stránek nebo i obsahu celých www serverů na lokální počítač, kde je lze následně prohlížet, i když počítač není připojen k Internetu. Tuto službu v omezené podobě nabízejí i standardní webové prohlížeče, ovšem nejkomfortnější práci nabízejí specializované programy – HTTrack Website Copier, Web Spider a další.

Shrnutí

Internetový prohlížeč je klientem služby WWW jako jedné z hlavních informačních služeb Internetu. Pro jeho správnou a zejména bezpečnou funkci je nutné zkontrolovat případně provést přenastavení způsobu práce prohlížeče s některými potenciálně nebezpečnými technologiemi používanými jak pro tvorbu WWW stránek, tak i pro doprovodné služby. Jedná se zejména o prvky cookie, Java skripty a prvky ActiveX.

Pojmy k zapamatování

- Internetový prohlížeč
- ISP - poskytovatel připojení k Internetu

- Cookie
- Java skript
- ActiveX

Kontrolní otázky

1. Vysvětlete pojem ISP (Internet Service Provider).
2. Jakou funkci zabezpečují soubory cookie?
3. Co jsou to Java skripty a prvky ActiveX?

Kapitola 13

Vyhledávací služby a metody jejich použití

Internet a zejména jeho informační služba WorlWideWeb dosáhla za několik málo let své existence rozměrů, nezvládnutelných jediným člověkem. Se stroji zase člověku pomáhá stroj - tentokrát stroj vyhledávací. Neúnavný, pilný a neomylný. To poslední slůvko by spíše patřilo do úvozovek. Ovšem stroje a tedy i počítače se nemýlí, dělají jen to, co jim přikáže člověk. Ovšem někdy jsou tyto příkazy tak špatně definované, že po jejich přesném provedení strojem, zůstává výsledkem omyl. S tím se asi každý, kdo již používal vyhledávací služby Internetu, potkal. Mezi tisíci vyhledanými odkazy jen několik málo skutečně něco o hledaném tématu vypovídá. Zmýlil se snad stroj?

13.1 Základní přehled vyhledávacích služeb

Najít potřebnou informaci v nepřeberném množství jiných informací na Internetu bez použití speciálních pomůcek (programů) je prakticky nemožné. Klasická metoda prohlížení Internetu na základě náhodných přeskoků mezi odkazy, které se nám zdají být zajímavé - surfování - jen málokdy vede k vytouženému cíli. Pro tuto metodu existují na webu startovní body (starting points, starting point pages), odkud lze nasměrovat počáteční vyhledávání potřebným směrem:

http://infoeagle.bc.edu/cwis/webstart.html

http://www. ncsa.uiuc.edu/SDG/Presentations/Carle/StarPts.html

Startovním místem chemiků mohou být Web stránky např. na adresách: http://www.ct.utwente.nl/cheminf.html nebo ryze české

http://chemie.upce.cz

http://fch.upol.cz/other/odkazy.htm

13.1.1 Přehled vybraných světových a českých vyhledávacích služeb

Podstatně efektivnější způsob vyhledávání konkrétní informace na Internetu představují specializované servery provozující službu vyhledávání informací umístěných nejčastěji na WWW stránkách - vyhledávací služby (portály). Vyhledávací služby udržují seznamy stránek, s jejich obsahem a umožňují uživateli Internetu v tomto obsahu hledat klíčová slova

- hlavní pojmy související s obsahem vyhledávané informace. Dle způsobu vytváření seznamů dělíme tyto služby na ručně udržované seznamy (odkazy i další informace přidává správce případně uživatel) a automaticky udržované seznamy, tzv. vyhledávací stroje (zde si veškeré informace získává a udržuje samotný obslužný program). Do seznamu pak vyhledávač ukládá stručné charakteristiky všech web dokumentů, které prohlédl nebo které mu byly zadány. Některé vyhledávací nástroje jsou orientovány tematicky, což znamená, že vyhledávací stroj může omezit hledání podle oboru našeho zájmu. Např. na obor organické chemie či biochemie v případě DNA (pokud ovšem uživatel takovýto složitý dotaz umí vyhledávači zadat a pokud vůbec nějaké takové WWW stránky vede vyhledávač ve svém interním seznamu).

Nejznámějšími (celosvětově mnohdy i v ČR) webovými vyhledávači jsou:

AltaVista (http://www.altavista.com/) – udržuje asi největší databázi indexovaných WWW stránek několik desítek milionů! Z důvodu tak velké databáze AltaVista disponuje možností rozšířeného zadávání vyhledávacího dotazu využívajícího mimo jiné k jeho tvorbě logické operátory.

Google (http://www.google.com/) – dnes vlastní možná již rozsáhlejší databázi WWW stránek než AltaVista. Má rovněž rozsáhlý aparát pro zadávání i kopmlikovaných vyhledávacích dotazů. Má českou lokalizaci a je v ČR velmi oblíbený. InfoSeek Guide (http://www. infoseek.com) – je rychlý a obsažný. Lehce se používá a poskytuje přehledný výstup s kratičkými výňatky z nalezených stránek

Lycos (http://www. lycos.com) – byl prvním opravdu velkým hledačem a velmi dlouho byl hledačem největším. Bývá také považován za nejlepší velký hledač (odkazy, které uvádí jako první, podle řady uživatelů nejlépe odpovídají zadaným kritériím).

Yahoo (http://www. yahoo.com) – je asi nejpopulárnější hledač, často doporučovaný začátečníkům jako jedno z prvních míst, odkud mohou začít prozkoumávat Internet. Nabízí hierarchickou strukturu adresářů rozdělených podle tematických okruhů. Výhodou je, že podobně zaměřené WWW uzly zde najdeme pohromadě.

ChemCenter (http://www. chemcenter.org/) – je pravděpodobně největším chemicky zaměřeným vyhledávačem. Z hlediska svého zaměření obsahuje rejstřík informací převážně z oblasti chemie.

Na další řadu vyhledávačů odkazuje služba Eureka (http://gocee.com/eureka), kde lze najít i podrobnější informace o možnostech těchto vyhledávačů.

Ovšem i užší zaměření nějakého vyhledávače neznamená, že bude při hledání informací z oboru, na který je specializovaný, tím nejúspěšnějším vyhledávačem. Při pokusu hodnotícím počet nalezených chemických odkazů ve světových hledačích po zadání prostého hesla “chemistry“ nejvíce odkazů nabídlo Yahoo s 17 700 000. Druhý skončil InfoSeek s 10 700 000 odkazy a třetí AltaVista se 4 129 089 odkazy. (20.10. 2003)

Vyhledávací nástroj k lokálním účelům (např. k vyhledávání informací z web stránek v LAN) existuje jako volně dostupný program EWS (eXcite for Web servers) na adrese http://www. excite.com/navigate pro servery běžící pod Windows NT i UNIXem.

Průvodce studiem

V této kapitole je uvedena řada funkčních odkazů. Pokud příslušné vyhledávací portály ještě neznáte, využijte této příležitosti a podívejte se na jejich nabídku možnosti vyhledávání dokumentů na Internetu a dalších rozšířených služeb. I když se to zdá být při tom množství nemožné, opravdu každý vyhledávací portál má svá specifika a tím pádem má své uživatele, kteří tyto zvláštnosti opravdu ocení. Možná tak najdete svůj optimální vyhledávač i vy.

13.1.2 Zastaralé vyhledávací protokoly a služby

V období přibližně do roku 1993, kdy již jako hlavní informační služba Internetu prorazila služba WWW, byly k vyhledávání a přenosu dokumentů používány jiné metody a protokoly jako je Archie, který sbírá udržuje informace zejména o souborech dostupných službou FTP, nebo Veronica, která plní tytéž služby v systému Gopher (zastaralý distribuovaný systém doručování dokumentů postavený na modelu klient/server). Z dalších vyhledávacích protokolů je důležitý zejména protokol Z39.50, který představuje definici služeb načítání informací a specifikaci protokolů pro knihovní aplikace, přičemž je schopen prohledávat různé databáze bez potřeby znalosti specifik konkrétního systému a konkrétní databáze dané knihovny. Podobné vlastnosti má i šířeji pojatý projekt WAIS (Wide Area Information Server), který definuje klientský i serverový software a síťový protokol, jehož prostřednictvím mohou uživatelé vyhledávat informace v různých databázích pomocí dotazů formulovaných v přirozeném jazyce. Jeho služby ovšem opět podstatně lépe nahradila služba WWW. Stejný je i osud systému Harvest, který představuje distribuovaný indexový systém, jehož úkolem je sbírat, extrahovat, uspořádávat, vyhledávat, a replikovat informace. Pro přístup ke službě Harvest neexistuje žádný speciální klientský protokol ani protokol pro komunikaci klient/server. Uživatelé mohou ke službě Harvest přistupovat pomocí běžného webového prohlížeče, který komunikuje se serverem. Harvest používají nepřímo, prostřednictvím serveru HTTP, dokonce některé webové vyhledávače pro své potřeby.

13.1.3 Webové katalogy a webové vyhledávací stroje

Rychlý růst informačního obsahu služby World Wide Webu v 90. letech 20. stol. podnítil vývoj nástrojů, jejichž pomocí by bylo možno jednoduše zvládnout tento rostoucí počet informací v hypertextových dokumentech. Webové rozhranní vyhledávání informací má podobu dokumentu jazyka HTML - formulář - do nějž uživatel vyspecifikuje hledanou informaci. Vyplněný formulář je webovým klientem odeslán protokolem HTTP na server, kde je požadavek zpracován pomocí skript rozhraní CGI (Common Gateway Interface) a rozhraní ISAPI (Internet Server Application Programming Interface). Prohledávání přitom probíhá v databázi dokumentů uložené na serveru. Důležitý úkol naplnění této databáze má několik řešení. Mimo již zmíněné ruční zadávání (databáze = předmětový katalog) lze obsah databáze vytvořit za pomoci tzv. vyhledávacího robota (robots, crawlers, spiders, worms). Vyhledávací robot je samozřejmě pilnější a výkonnější než člověk, takže je schopen prohledat a zkatalogizovat více WWW stránek, ovšem jejich správné zařazení je závislé na tvůrci stránek, resp. na tom, jak přesně obsah stránek vystihují klíčová slova v hlavičce HTML dokumentu. I když jsou tito roboti ve většině případů klienti protokolu HTTP, existují možnosti využití i dalších protokolů Internetu jako je NNTP (Network News Transfer Protocol), FTP a elektronická pošta. Protože ovšem roboti nemusí být vítáni na každém serveru či některých jeho částech, byl vyvinut speciální protokol pro řízení jejich prohledávání obsahů serverů - REP (Robot Exclusion Protocol). V prvé řadě jej používají administrátoři serverů HTTP, mohou jej využít ale také autoři stránek HTML.

Možnosti práce robota na daném serveru definuje soubor se jménem `robots.txt`, který se nachází v kořenovém adresáři serveru HTTP. Při prvním vstupu na server robot načte tento soubor a podle něj řídí dále svoji činnost. V souboru jsou v podobě prostého ASCII textu uloženy jednoduché příkazy (ALLOW či DISALLOW), určující, kam robot na daném serveru může a kam ne. Pokud takový soubor chybí, chová se robot tak, jako by byl přístup povolen všude. Prohledávání dokumentů HTML může ovlivnit i jejich tvůrce, neboť příkazy pro robota lze vkládat přímo do hlavičky HTML dokumentu. Samozřejmě i protokol pro řízení práce vyhledávacího robota se dále vyvíjí zejména proto, že původní protokol pouze zakazuje, ale neumožňuje navedení robota do žádaných oblastí. Robot Guidance Project je jednou z možností jak takového vylepšení dosáhnout.

Díky růstu výkonnosti počítačů ve funkci serverů i nárůstu ukládacího prostoru pro databáze a v neposlední řadě i díky stále rychlejšímu přenosu dat po Internetu pracují dnešní vyhledávače ve fulltextovém módu - mimo standardní prohledávání hlaviček HTML dokumentů prohledají i celý jejich obsah i obsahy jiných typů dokumentů umístěných na příslušném serveru.

Shrnutí

Exponenciální nárůst počtu informačních zdrojů přístupných po Internetu nelze zvládnout bez efektivních metod vyhledávání dokumentů podle jasně zadaných kritérií. Pro tento účel vznikly specializované servery - Internetové vyhledávací portály, které sbírají a udržují informace o dokumentech publikovaných na Internetu. Tyto vyhledávače pak své informace zpřístupňují uživatelům Internetu za pomoci jednoduchého rozhranní katalogového či dotazníkového typu.

Pojmy k zapamatování

- Vyhledávací portál (vyhledávač).
- Startovní stránka.
- Webový katalog.
- Vyhledávací robot.
- Meta-vyhledávač.

Kontrolní otázky

1. Jaký význam mají v systému vyhledávání informací na Internetu tzv. startovní stránky?

13.2 Postupy používané při vyhledávání informací na Internetu

13.2.1 Rozšířené možnosti zadávání vyhledávacího dotazu

Při zadání vyhledávání určité informace na Internetu, mnohdy vyhledávač nalezne přemíru stránek obsahujících nějakou zmínku o hledané informaci. Proto je důležité jak přesně zadáme vyhledávací dotaz, případně jaké další možnosti pokročilého vyhledávání vyhledávač nabízí. Tak mimo klíčových slov jsou pro konkretizaci dotazu používány logické operátory:

AND (&) - systém vyhledá jen ty dokumenty, ve kterých se klíčová slova vyskytují současně, např. Chemistry AND Spectra

OR (I) - systém vyhledá dokumenty, ve kterých se vyskytuje alespoň jedno z uvedených klíčových slov, např. Organic OR Anorganic

NOT (N) - systém vyhledá všechny dokumenty, ve kterých se vyskytuje jedno klíčové slovo a nevyskytuje se jiné klíčové slovo, např. Book NOT Journal

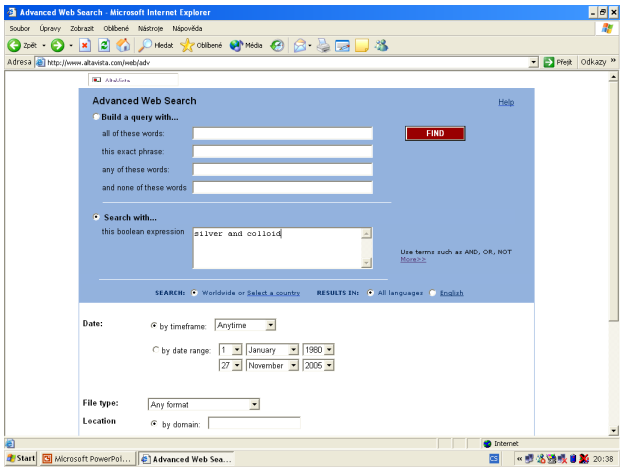
Pro složitější výrazy můžeme použít závorek. Použití logických operátorů se mírně liší podle typu vyhledávacího nástroje; AND se nahrazuje znaménkem + a NOT znaménkem −. České vyhledávače obvykle využívají českých ekvivalentů anglických výrazů logických operátorů. Další pomoc nabízí znak *, který lze použít pro náhradu libovolného počtu

znaků ve slově (vhodné pro nahrazení pádových koncovek apod.). Obvykle nezáleží na velikosti písmen, zadáváme je malá. Tedy dotaz brno bude mít za odpověď i stránky s textem Brno, BRNO apod. (to ovšem neplatí obecně).

Mnohé vyhledávače umožňují zadat celou hledanou frázi – tak se pak vyhledává v uložených dokumentech v kompletním znění. Fráze se obvykle zadává do uvozovek. Dotaz “Václav Havel„ vyhledá všechny stránky, na nichž se vyskytují slova Václav Havel ihned za sebou a v daném pořadí. Zatímco dotaz Václav Havel vyhledá stránky, na nichž je slovo Václav, ale ne nutně Havel, nebo Havel, ale ne nutně Václav, nebo stránky se slovy Václav i Havel, ale ne nutně v uvedeném pořadí.

Většina vyhledávačů umožňuje volbu jazyka vyhledaného dokumentu. Tak např. můžeme vynechat stránky v čínštině, když ji zrovna neumíme.

Některé vyhledávače podporují další omezení vyhledávání pomocí výrazů From: a To:, dovolujících specifikovat, v jakém období měla být hledaná stránka naposledy změněna. Tedy zajímá-li nás rok 2005, bude to From: 01/Jan/05, To: 31/Dec/05. Ukázku možností pokročilého vyhledávacího dotazu, jak jej umožňuje vyhledávač Altavista představuje obrázek 13.1.



Obrázek 13.1: Pokročilý vyhledávací dotaz podle možností vyhledávače Altavista.

Pro snadnější orientaci uživatele, který hledá určitou informaci mají vyhledávače v záhlaví odkazy seřazeny do kategorií - sekcí. Přecházením mezi sekcemi smůže uživatel podstatně rychleji a cíleněji dosáhnout k určité předem dobře definovatelné informaci - např. seznamy prodejců fotoaparátů apod.

Dnešní vyhledávací servery soustředí na jednom místě mimo vyhledávací službu i spoustu dalších služeb pro uživatele Internetu. Mimo již standardní možnost připojení k Internetu (funkce ISP) poskytují též poštovní služby a odkládací diskové prostory o velikostech až v jednotkách GB, nabízejí slovníky pro vícejazyčné překlady, ale třeba i službu chatu, Internetové telefonie či videokonferencí. A samozřejmě nabízí i možnost prezentace vlastních WWW stránek bezplatně (bohužel v takovém případě s reklamními proužky).

Autor může své WWW stránky snadno přidat do některého z popsaných (ale i dalších) vyhledávačů, postup je vždy uveden v jeho nápovědě. Obvykle je při zaregistrování stránek nutno vyplnit registrační formulář.

Průvodce studiem

Pro otestování možností pokročilého vyhledávacího dotazu dobře poslouží nejen zmíněný vyhledávač Altavista, ale obdobné možnosti nabízí i dnes asi v ČR populárnější vyhledávač Google, který pro adresy z domény cz pracuje v lokalizované české verzi.

13.2.2 Internetové encyklopedie

Dalším obsažným zdrojem informací na Internetu jsou elektronické obdoby klasických encyklopedií. Původně se začínalo tím, že se převáděly tištěné encyklopedie do elektronické podoby (např. Encyclopaedia Brittanica, Ottův slovník naučný), v současnosti již existuje mnoho elektronických encyklopedií přístupných pomocí Internetu, které nemají dvojníky v tištěné podobě (např. MS Encarta). Existují i kombinované encyklopedie, kdy k základní tištěné verzi jsou doplňující informace a aktualizace přístupné pomocí Internetu (nechvalně proslulý encyklopedický projekt Diderot, který několikrát zkrachoval).

Některé z takto publikovaných encyklopedií jsou přístupné pouze za poplatek, obvykle tak, že podrobnější popis encyklopedického hesla je chráněn přístupovým heslem jako je tomu u Encyclopaedia Brittanica (www.britannica.com), MS Encarta (encarta.msn.com), Columbia Encyclopedia (www.encyclopedia.com) nebo česká encyklopedie Co to je? (www.coto.je).

Mnohé encyklopedie jsou však plně přístupné zdarma a mnohdy se na jejich tvorbě mohou podílet i samotní uživatelé. Jedním z nejúspěšnějších českých projektů tohoto typu je encyklopedie CoJeCo (www.cojeco.cz), celosvětově pak projekt encyklopedie Wikipedia (www.wikipedia.org), která má různé jazykové verze včetně české (cs.wikipedia.org).

Shrnutí

Vzhledem k ohromnému množství dokumentů publikovaných na Internetu nevede obvykle jednoduchý vyhledávací dotaz k nalezení toho obsahově správného dokumentu. Proto existují rozšířené možnosti vyhledávání za použití logických operátorů a dalších specifických funkcí (např. fráze) pro konstrukci pokročilého vyhledávacího dotazu.

Pojmy k zapamatování

- Pokročilý vyhledávací dotaz.
- Logické operátory AND, OR, NOT.
- Fráze.
- Internetové encyklopedie.

Kontrolní otázky

1. Jakým způsobem lze v pokročilém vyhledávacím dotazu uabezpečit, aby se v hledaných dokumentech nevyskytoval určitý pojem?
2. Jak zabezpečíme, aby se zadaná slova ve vyhledávacím dotazu vyskytovala v nalezených dokumentech přesně v tom pořad,í jak byla zapsána?
3. Jakými způsoby mohou vznikat Internetové encyklopedie?

13.3 Vyhledávání na sociálních sítích – Social Network Analysis

Dne 13. prosince 2003 v Iráku díky uplatnění metodologie Social Network Analysis (SNA) se americké armádě podařilo zadržet bývalého diktátora Sadáma Hussajna. Prozradila ho

detailní analýza jeho sociální sítě a následné zpravodajské akce v terénu. Dnes jsou základy SNA součástí armádního výcviku pro boj s teroristy. Svoje postavení si SNA vydobyla především v těch oblastech, kde jsou důležitější vztahy než osoby samy o sobě.

Dalším využitím SNA je v komerčním prostředí. Co se říká o vaší značce a firmě v sociální síti? Jak to zjistit a jak to vyhodnotit?

Účelem marketingu v sociální síti není komunikovat s každým členem v sociální síti a nastínit mu vaši pravdu, vaši myšlenku. Jde o to, komunikovat jen s těmi klíčovými lidmi. S těmi, kteří jsou rozhodující, kteří vedou a ovlivňují komunitu. Účelem je předat jim relevantní informace a vysvětlit jim je v kontextu trhu a značky.

Vaše reklama v sociální síti se musí především přelít přes klíčové uživatele. Až klíčoví uživatelé sítě jsou schopni zaujmout ostatní uživatele na dlouho, protože jsou nestranní a jsou schopni vlažný zájem běžných uživatelů proměnit v nákupní rozhodnutí stejně, jako dobrý prodavač v obchodě promění váš vlažný zájem o „možná novou televizi, jsou ty placaté vůbec dobré?“ na „jasně, tu novou Full HD LCD mi zabalte“.

SNA je tedy především nástrojem sociologickým.

13.3.1 Vertikální analýza — kdo je naše komunita?

Jde o to, najít „všechny“ důležité skupiny, weby, diskuzní fóra, blogy, diskuze pod články, které se zabývají vaším tématem. Často se stává, že tato fóra mají více uživatelů (nadšenců a specialistů) než by jste našli na Facebook nebo Twitter. Je dobré si udělat jejich seznam, aby jste věděli, kde se vaši uživatelé koncentrují a kde budete analyzovat.

13.3.2 Horizontální analýza — jak vyhledáme naši komunitu?

Detailně se obeznámíte s prostředím každé sítě, kterou jste zahrnuli do seznamu z vertikální analýzy, zjistíte její rozsah (počty registrovaných členů), zjistíte její alfauživatele, popíšete mechanismy fungování této sítě.

Specifickým příkladem jsou obecné sociální sítě, jako Facebook a Twitter. Když jste výrobcem softwaru pro windows mobile smartphony, jistě vás nezajímá celé osazenstvo Facebooku, ale jen ti, kteří jsou potenciální cílovou skupinou. Zatímco na mobil.cz se rychle zorientujete, na FB není tak jednoduché přesně určit, kdo je vaše cílová skupina. Velikou výhodou komunit je fakt, že téma je na nich stanovené. V rámci Facebooku musíte hledat. Nejprve si vypište všechna slova popisující váš produkt, obor, firmu, tj. všechno, co se používá např. do AdWords jako slova cílení. Tato slova pak postupně zadávejte do okénka vyhledávání na Facebooku. Odhalíte tak stránky a skupiny, které se věnují vašemu tématu. Můžete tak odhalit i přímo lidi, kteří se o téma zajímají, ale jen u Twitteru, kde se uzavřené účty prakticky nepoužívají.

13.3.3 Nalezení alfauživatele — jak najdeme klíčové uživatele?

Hledání alfauživatele začneme na jedněch ze stránek věnovaných vašemu tématu. Nemá smysl procházet všechny kontakty, to nám nic nečekne o tom jak jsou jednotliví uživatelé aktivní. Musíme tedy pročítat jednotlivé reakce uživatelů k tématům a vyfiltrovat ty nejaktivnější, především, ty co nejvíce k tématu odpovídají. Pokud takoví uživatelé mají zároveň hodně kontaktů, je velmi pravděpodobné, že jste nalezli svého alfauživatele. Rovněž je potřeba se podívat jak na alfauživatele reagují další alfauživatelé, pokud negativně,

pak je ze seznamu vyřadíme, pokud pozitivně, pak jsou to právě oni, co hledáme. Důležité je ale z těchto vytipovaných uživatelů vyfiltrovat ještě trolly.[1]

13.3.4 Sentiment analysis — analýza nálady

Na základě sentiment analysis (SA) lze usuzovat, co si o vás komunita myslí, ale rovněž lze předpovídat blízký vývoj situace u uživatelů a vyhnout se tak budoucím problémům. SA lze provádět aktivním nebo pasivním monitorováním.

13.3.4.1 SA - aktivní monitorování

Provádí se způsobem dotazníku, ankety, hlasování apod. Bohužel je zde úskalí, že se zapojují jen uživatelé, kteří jsou ochotni odpovídat nebo chtějí výsledky měnit ve svůj prospěch (např. ankety kolik by byli ochotni zaplatit za výrobek, je jasné, že se uživatelé snaží protlačit co nejnižší cenu). Vhodné je takový průzkum zacílit na určitou skupinu – naši zákazníci, zákazníci konkurence, obyvatelé určitého státu, matky apod. (tzv. sociálně-demografický profil).

13.3.4.2 SA - pasivní monitorování

Provádí se poslouchánim, prohledáváním zmínek o vaší značce, konkurenční značce, vašem oboru apod. Lze takto například i potvrzovat hypotézy.

[1] Troll je v internetovém slangu účastník online diskusních fór, chatů či blogů, který zasílá provokativní, hanlivé nebo irelevantní (off-topic) příspěvky k citlivým tématům, jejichž hlavním smyslem je vyprovokovat ostatní uživatele k vytoužené emotivní odezvě nebo jinak narušit normální věcnou diskusi. (zdroj: Wikipedia)

Kapitola 14

Základy tvorby WWW stránek

Zvládnutí tvorby WWW stránek zahrnuje dva základní podúkoly- zvládnutí technologie tvorby stránek (jazyka HTML) a zvládnutí úskalí publikování elektronických dokumentů, které se v mnoha směrech liší od publikování klasických tištěných dokumentů. Internet je mladé komunikační médium, jeho věk se měří na pouhé desítky let ve srovnání se stovkami let historie tištěných médií. I proto je zvládnutí toho druhého podúkolu tvůrcem WWW stránek podstatně složitější než zvládnutí technické otázky tvorby WWW stránek. O této skutečnosti svědčí množství odrazujících příkladů obsahově i graficky nepovedených stránek, jimiž se Internet jen hemží.

14.1 Nástroje použitelné pro tvorbu WWW stránek

Přestože pro tvorbu WWW stránek existují specializované programy, lze se bez nich velice snadno obejít. Základní datový formát WWW dokumentu, formát HTML, má totiž čistě textovou podobu. Pro tvorbu takového dokumentu tak postačí i ten nejjednodušší textový editor, jako je např. Notepad (Poznámkový blok), základní součást OS MS Windows. Při tomto způsobu tvorby HTML dokumentu ovšem musí autor znát všechny kódy a parametry formátu HTML a společně se zdrojovými texty je do dokumentu zapsat ručně.

Druhá cesta, využití specializovaných editorů HTML, má dva směry - práci v tzv. WYSIWYG módu nebo bez něj. WYSIWYG mód značí, že stránky vytváříme v okně editoru přímo v podobě, jak jsou zobrazovány webovým prohlížečem, bez nutné znalosti příkazů HTML. Do skupiny editorů, které WYSIWYG mód podporují patří např. editor MS FrontPage či Macromedia Dreamveawer MX. Práce je s nimi snadná i pro začátečníky, kteří kód HTML neovládají. Tyto editory ale obvykle vytváří velmi složitý výstupní soubor HTML, který je později velmi obtížné editovat. V případě editorů nepodporujících WYSIWYG mód je nutno pracovat přímo s kódem HTML (editor poskytuje pouze podporu tvorby) a konečný výsledek je pak nutno zjistit za pomoci prohlížeče. Příkladem takového editoru je program HomeSite.

Existuje i další způsob tvorby WWW stránek, založený na schopnosti mnoha programů ukládat dokumenty ve formátu HTML. To umí např. programy balíku Microsoft Office.

Původně statické WWW stránky, které pouze umožňuje vytvářet jazyk HTML byly rozšířeny o další prvky, které daly WWW stránkám dynamiku (proměnnost v čase) - např. pohyblivé obrázky (animace) apod. Tyto dynamické prvky jsou realizovány dalšími technologiemi, založenými na speciálně k tomuto účelu vytvořených programovacích jazycích jako je Java, resp. její zjednodušená verze JavaScript nebo jazyk z dílny fy Microsoft Visual Basic Script. Tyto programy určené k „rozhýbání“ WWW stránek (applety, skripty)

mohou ovšem vykonávat i jiné činnosti nebezpečné pro data uložené v našem počítači. Proto lze jejich provádění při prohlížení WWW stránek v prohlížeči zakázat, ovšem za cenu ochuzení o důležitou součást grafické prezentace, kterou autor na svých stránkách předvádí . Spojením HTML a těchto dynamických prvků včetně dalších technologií (kaskádové styly, CSS) přinesly jazyku HTML prvky, které v něm chyběly, jako je přesné umístění objektů, interaktivita stránky, překrývání objektů a řízené animace. Spojením HTML s těmito prvky vznikl dynamický HTML (DHTML) jako kombinace objektů tvořených vedle HTML pomocí CSS a skriptovacího jazyka (Java, ActiveX). Rozšířená verze jazyka HTML disponuje prvky ovládající i způsob zobrazení stránek pomocí rámů. Rámy umožňují rozdělit stránku na několik nezávislých oken. Některá okna pak zůstávají neměnná, ty obvykle zobrazují strukturu stránek v systému odkazů. V dalších oknech, se pak zobrazuje vybraná informace. Použití rámů není vždy vítáno, protože zejména prohlížeče pro OS Linux rámy obvykle nepodporují. Další skupinu zajímavých možností WWW stránek tvoří formuláře, sloužící ke komunikaci mezi uživatelem a tvůrcem stránek.

Po vytvoření WWW stránek je nutno vytvořené stránky zveřejnit na Internetu (vystavit), umístit je na počítač pracující jako WWW server, z něhož jej pak načítají další uživatelé Internetu. K tomuto účelu jsou k dispozici i volně šiřitelné programy, jako je např. WWW server Apache.

14.2 Základní zásady tvorby WWW stránek

Tvůrce WWW stránek musí znát nejen jazyk HTML, ale musí se řídit určitými zásadami publikování na Internetu, které jsou v mnohých aspektech odlišné od klasických způsobů publikování v tištěných dokumentech. Zásady tvorby WWW stránek představují soubor doporučení a zkušeností, které vedou k tomu, aby byly vytvořené stránky účelné, zajímavé, a aby proto byly často navštěvovány. Autor si musí zejména uvědomit, že návštěvník WWW stránek hledá určitou informaci a je obvykle při hledání této informace netrpělivý. Nezjistí-li hned z prvé stránky vaší webové prezentace, že mu může být něčím užitečná, okamžitě odchází na stránky jiné. Pouze pečlivé naplánování postupu může vést k vytvoření webu, který bude úspěšný u předpokládané cílové skupiny uživatelů Internetu.

Postup při tvorbě plánu obsahové náplně WWW by se dal vyjádřit asi takto:

1. Nejprve si je třeba ujasnit pro koho bude web tvořen.
2. Pak je třeba promyslet co nového, originálního můžeme uživateli nabídnout.
3. Dále je nutné promyslet systém uspořádání poskytovaných informací.
4. Následuje ujasnění, jakým způsobem (text, grafika, multimédia) budou stránky realizovány.
5. Rovněž musí být určeno, jak budou informace aktualizovány.
6. Poté teprve uvážíme vlastní technickou realizaci webu.

Z uvedených bodů se podrobněji dotkneme jen bodu třetího. Ten je totiž důležitý jak z hlediska lákavosti naší prezentace, tak i z hlediska její přehlednosti a hlavně rychlosti, s jakou budou stránky načítány. Stále je třeba počítat s tím, že existuje řada uživatelů s pomalým připojením o reálné rychlosti (ne té uváděné maximální) řádově několik jednotek až desítek kb/s. Při zakomponování několika obrázků o velikosti stovek kB na jednu stránku znamená, že se tato stránka bude uživateli stahovat několik minut. A to je už dost dlouhá doba na to, aby si rozmyslel, jestli chce naše stránky ještě vidět.

Když už se uživatel stránky dočká, měla by být jasná, přehledná, ale i poutavá. Prostý text samozřejmě vyhovuje podmínce rychlého stahování, ale určitě ne této další protichůdné potřebě. I s umisťováním hypertextových odkazů musíme být opatrní. Pokud se jimi stránky jen hemží, ztěžují orientaci jejich návštěvníka a navíc jej lákají některý z nich vyzkoušet. A pokud jej odvede mimo naše stránky, je otázka, jestli se ještě vrátí. Ovšem stránka, která naopak má minimální obsah určitě není optimální. Typické jsou úvodní stránky mnohých personálních webů s nic neříkajícím nápisem „Vítejte!“ či „Vstupte na mé stránky“. Již první stránka musí mít svůj informační obsah. Měla by v kostce sdělit, o čem daný web je.

Důležitá je i hierarchie stránek - klasická pyramidální výstavba bude u rozsáhlejších webů asi nejvýhodnější, ale návštěvník se nesmí ve složité struktuře ztratit. Přehledné musí být nejen jednotlivé stránky, ale i jejich uspořádání. Je dobré například vytvořit stránku s mapou celého webu, která netrpělivým návštěvníkům usnadní cestu do určitého místa. Orientaci rovněž usnadňuje stále viditelná lišta s hlavními odkazy - tu můžeme umístit s pomocí technologie rámů nebo ještě lépe za pomoci kaskádových stylů. Při snaze o přehlednost a grafickou poutavost stránky, je třeba rovněž myslet na její pozadí, kteréby nemělo zhoršovat čitelnost textu ani orientaci na stránce. Podobně orientaci zhoršuje situace, kdy se obsah stránky nevejde do jednoho okna prohlížeče. Uživatel musí rolovat, aby zjistil zbytek obsahu stránky a přitom ztratí zase začátek. Při dnešním optimálním rozlišení 1024x768 pixel se na jednu obrazovku vejde skutečně spousta informace. Ale pozor, přemíra textu unavuje. WWW stránky nejsou kniha, nad kterou je čtenář ochoten strávit celou noc.

Průvodce studiem

Protože jedním z vašich hlavních úkolů po prostudování tohoto textu bude vytvoření vlastních WWW stránek, nastala nyní chvíle pro vytvoření prvotního návrhu těchto stránek. Dokud máte hlavní zásady ještě v čerstvé paměti, zamyslete se nad tím co a komu byste chtěli prostřednictvím těchto stránek sdělit. Návrh si nezapomeňte zaznamenat na papír, nebo třeba i do počítače, aby nebyly důležité myšlenky při realizaci zapomenuty.

14.3 Autorská práva na Internetu

Snadnost kopírování elektronických dokumentů a jejich dostupnost zdarma na Internetu vede k představě, že se Internetových dokumentů autorská práva netýkají. Opak je však pravdou a proto bychom měli dodržovat při tvorbě WWW stránek příslušná pravidla zachování autorských práv, protože Bernská konvence o autorských právech doslovně říká, že „všechno je chráněno, pokud není výslovně řečeno jinak“. To se týká koneckonců i našich dokumentů na Internetu, jejichž ohranou je hlavně jméno autora a datum vytvoření dokumentu. Pokud chceme použít zajímavé části jiných dokumentů, lze využívat citace, ale samozřejmě ne celého díla.

Mimo ochranu autorských práv je třeba při tvorbě WWW dokumentů dodržovat základní pravidla slušnosti jako v běžném životě. Hlavně by obsah stránek neměl působit urážlivě na jejich návštěvníky, či nějakou jejich užší skupinu (jde hlavně o otázky menšin a lidských ras).

Shrnutí

WWW dokument má svá specifika elektronického dokumentu publikovaného na Internetu a proto při jeho tvorbě nelze beze zbytku využít postupy a zkušenosti s publikováním klasických tištěných dokumentů. Dokument zveřejněný na Internetu by měl zejména dodržovat zásady jasnosti a stručnosti sdělení obsahu zacíleného na určitou skupinu návštěvníků. Současně by neměla být při jeho tvorbě porušována autorská práva a zásady pravidel slušnosti vyjadřování.

Pojmy k zapamatování

- WYSIWYG editory HTML dokumentu.
- Zásady tvorby WWW stránek.
- Autorská práva na Internetu.

Kontrolní otázky

1. Jaké editory lze využít pro editaci HTML dokumentu?
2. Jaké jsou hlavní zásady tvorby WWW stránek?
3. Jsou dokumenty zveřejněné na Internetu chráněny autroskými právy?

Kapitola 15

Tvorba statických WWW stránek

Po důkladné rozvaze o obsahu a stylu vytvářených WWW stránek přichází chvíle pro jejich technické provedení. K tomu je nebytné buď ovládat alespoň v základech jazyk HTML, nebo mít k dispozici nějaký WYSIWYG editor a umět využívat jeho možnosti tvorby WWW stránek. My půjdeme cestou trnitější, ale ve svých důsledcích cestou čistější tzn. cestou prostého využití značek jazyka HTML pro vytvoření sice jednoduchých, ale účelných WWW stránek.

15.1 Jazyk HTML a jeho základní syntaxe

V úvodu této kapitoly byl naznačen historický vývoj jazyka HTML, který je v zásadě dnes již u konce. To má své výhody ve stabilitě syntaxe tohoto jazyka, nevýhodu v tom, že jednou přijde chvíle, kdy bude uživatel nucen přejít na jinou obecně používanou verzi značkovacího jazyka. Ale i tehdy získané znalosti a dovednosti nepřijdou nazmar, protože vývoj nesměřuje k úplné negaci omezené verze značkovacího jazyka jakou jazyk HTML je, ale k rozšíření jeho možností při zachování funkčnosti většiny jeho stávajících prvků.

15.1.1 Vývoj jazyka HTML

Vývoj jazyka HTML byl zpočátku nekontrolovaný a v převážné míře se jím zabývaly firmy, které vyvíjely prohlížeče www stránek (Microsoft, Netscape). Z tohoto důvodu do vývoje HTML jazyka zasáhla opakovaně organizace W3C (World Wide Web Consorcium), což vedlo nakonec v roce 1997 k vytvoření všeobecně dodržovaného standardu jazyka HTML označovaném jako verze HTML 4.01 (viz předchozí kapitola 14). Tato verze definuje možnost výběru ze tří pracovních režimů:

1) **Přechodový** (transitional) – lze zde používat i tzv. zastaralé prvky a atributy, zejména se jedná o ty prvky, které ovlivňují vzhled dokumentu (např. font, center, align). Příslušný HTML dokument pak musí začínat následujícícím zápisem:

```
1  <!DOCTYPE HTML PUBLIC \-//W3C//DTD HTML 4.01 Transitional//"EN \http://www.w3.
       org/TR/1999/REC-html401-19991224/loose."dtd>
```

2) S **rámy** (frameset) – stejný jako přechodový režim a navíc lze používat prvky pro tvorbu rámů (např. frame, frameset). HTML dokument začíná zápisem:

```
<!DOCTYPE HTML PUBLIC \-//W3C//DTD HTML 4.01 Frameset//"EN \http://www.w3.org/TR
    /1999/REC-html401-19991224/frameset."dtd>
```

3) **Přísný** (strict) – používá jen prvky nového standardu a ne zastaralé prvky. HTML dokument začíná zápisem:

```
<!DOCTYPE HTML PUBLIC \-//W3C//DTD HTML 4.01//"EN \http://www.w3.org/TR/html4/
    strict."dtd>
```

Na adrese http://www.w3.org/file-upload.html je možno zkontrolovat, zda napsaný HTML dokument odpovídá uvedeným pravidlům.

Verzí HTML 4.01 byl vývoj tohoto jazyka ukončen a další vývoj se ubírá směrem zjednodušení struktury hypertextového dokumentu. Zejména dochází k oddělení vlastního obsahu dokumentu od popisu jeho způsobu zobrazení vhodným prohlížečem. Internetové technologie se tak vrátily k počátkům svého vývoje, kdy za základ jazyka HTML byl vzat značkovací jazyk SGML. V tomto jazyce značky popisují jen jednotlivé části dokumentu a ne způsob jejich následného zobrazení vhodnou aplikací. V roce 1998 vznikl nový značkovací jazyk XML. Žádný z prvků tohoto jazyka již nenese popis výsledného vzhledu dokumentu. Značky slouží pouze k určení, co přesně je obsahem dané části dokumentu (např. toto je zboží a toto jeho cena). V roce 2000 pak díky aktivitě konsorcia W3C vznikl syntézou prvků jazyka HTML a XML nový standard XHTML, který ve verzi 1.0 umožňuje plnou kompatibilitu s HTML 4.01, ale v dalším vývoji se již více přibližuje snahám oddělení popisu obsahu dokumentu od definice jeho vzhledu při zobrazení – verze XHMTL 1.1 je již kompatibilní pouze s přísnou verzí HTML 4.01. Problém konečného vzhledu dokumentů je pak ponechán na jiných technologiích, z nichž nejúspěšnější se staly zejména kaskádové styly neboli CSS. Ty se od svého vzniku v roce 1996 velmi rychle rozšířily z původně pouze podpůrného prostředku pro lepší formátování HTML dokumentů do výkonného nástroje, který pomocí externích souborů řídí způsob zobrazování jednotlivých částí HTML resp. XHTML dokumentů.

15.1.2 Speciální znaky jazyka HTML

V jazyce HTML jsou některé znaky vyhrazené pro jiné účely než psaní textu a proto je nutné je v textu či adrese URL zapisovat kódovaně. Nejběžnější příklady uvádí následující tabulka.

Znak	Textový řetězec	Číselný řetězec	Popis
NBSP	&nspb;		pevná mezera
″	&quot;	&#34;	uvozovky
¡	&lt;	&#60;	závorka
¿	&gt;	&#62;	závorka
libovolný		&#číslo;	libovolná hodnota kódu ISO 8859-1

15.1.3 Přehled základních značek HTML jazyka

Většina značek jazyka HTML je párová - skládá se z počáteční koncové značky. Koncová se od počáteční liší zpravidla jen tím, že ohraničení značky lomenou závorkou je doplněno za levou závorkou lomítkem, např. značka `<p>` označuje začátek odstavce a značka `</p>` tento odstavec ukončuje. Některé značky jsou sice nepárové, např. značka zalomení řádku `<br>`, ale standardy vyšších verzí značkovacích jazyků nepárové značky neznají a jazyku HTML nečiní potíže neznámou značku neinterpretovat. Pro budoucí kompatibilitu je dobré proto všechny značky zapisovat jako párové. I když standard HTML 4.01 nerozlišuje v zápisu

značky velká a malá písmena, vyšší značkovací jazyky tak činí, takže je lépe používat pro značky jazyka HTML standardně malá písmena.

V následujících tabulkách jsou uvedeny vybrané základní značky jazyka HTML podle specifikace HTML 4.01 s rámy a jejich základní popis použití. Vyznačení zastaralý prvek znamená, že jeho používání v dokumentech HTML není do budoucna doporučováno. Principielně žádnou z dále uvedených značek nemusí HTML dokument obsahovat, postačí prostý text, který bude prohlížečem zobrazen tak jak je napsán. Aby prohlížeč poznal, že se jedná o dokument HTML, musí mít pouze soubor příponu htm respektive html.

Průvodce studiem

Následující přehled značek jazyka HTML není zdaleka vyčerpávající ať se již jedná z hlediska existujících značek, tak i jejich parametrů. Pro podrobnější a úplnější informaci použijte některou z knih ze seznamu doporučené literatury, např. knihu HTML 4 pro World Wide Web od E. Castra, vyšlou v nakladatelství SoftPress.

XXX ZNACKY XXX

Shrnutí

Jazyk HTML prodělal za krátkou dobu své existence rychlý vývoj, který je dnes již ukončen verzi 4.01, přijatou v roce 1997 za standardní. Tato verze má tři pracovní režimy, z nichž pouze režim *strict* bude plně podporován i v budoucnu. HTML je jazykem značkovacím, většina jeho značek je párových. Mimo vyznačení důležitých částí dokumentu řídí tyto značky způsob zobrazování jeho jednotlivých částí v okně prohlížeče, včetně zabezpečení funkce hypertextových odkazů. Standard jazyka rovněž předepisuje základní strukturu HTML dokumentu, který je tak rozdělen na dvě části - hlavičku nesoucí informace o dokumentu a tělo, tvořené vlastním obsahem dokumentu, který se zobrazuje v okně prohlížeče.

Pojmy k zapamatování

- Jazyk HTML verze 4.01 - režimy přechodový, s rámy a přísný (strict).
- Značky a jejich parametry jazyka HTML.
- Hlavička a tělo dokumentu HTML.

Kontrolní otázky

1. Jak se liší režimy jazyka HTML ve verzi 4.01 označované jako přechodový a přísný?
2. Na jaké hlavní části je členěn HTML dokument?
3. Jak se liší počáteční a koncová značka jazyka HTML?
4. Co jsou to parametry značek jazyka HTML?

15.2 Popis jednotlivých značek a příklady jejich použití v HTML dokumentu

Značky popsané v předchozí kapitole budou nyní využity k vytvoření základní struktury a úpravu formátování HTML dokumentu při jeho zobrazení v okně prohlížeče.

15.2.1 První krok – vytvoření základní struktury HTML dokumentu

I když HTML dokument je prohlížečem správně interpretován i bez značek, vymezujících jeho základní strukturu, je vhodné pro přehlednost dokumentu i pro jeho další případné zpracování automatizovanými prostředky (např. vyhledávací robot), dodržet zásady tvorby HTML dokumentu podle normy konsorcia W3:

```
<!DOCTYPE HTML PUBLIC \-//W3C//DTD HTML 4.01 Frameset//"EN \http://www.w3.org/TR
    /1999/REC-html401-19991224/frameset."dtd>
<html>
<head>
<title>

<!-- titul dokumentu -->
</title>
<!-- šídal části čhlaviky -->
</head>
<body>
<!-- ětlo dokumentu -->
</body>
</html>
```

Hlavička ¡!DOCTYPE¿ se používá ve stránkách podle definice HTML od verze 3.2. Značka `<html>` a `</html>` vymezuje celý dokument. Značka `<head>...</head>` označuje oblast metadat dokumentu (data určená pro základní popis dokumentu a jeho obsahu pro účely automatického zpracování) a obsahuje mimo jiné značky `<title>...</title>` (název dokumentu). Poslední značka definující základní strukturu HTML dokumentu je `<body>...</body>`, která vymezuje vlastní data dokumentu. V rámci definice těla dokumentu lze předdefinovat barvu pozadí dokumentu pomocí atributu bgcolor a barvu textu pomocí atributu text. Barvy se píší k atributu za rovnítko buď pro základních 16 barev textově do úvozovek (např. blue, red) nebo libovolnou barvu pomocí číselného kódu v šestnáctkové soustavě podle tabulky barev v notaci RGB (bílá má kód `#FFFFFF`, černá `#000000`).

15.2.2 Krok druhý – vytvoření hlavičky HTML dokumentu

Podobně jako vymezení struktury HTML dokumentu, není ani jeho hlavička povinná. Obsahuje pouze informativní údaje jednak pro samotného autora dokumentu, jednak pro další zpracování resp. interpretaci prohlížečem www stránek. Tyto informace zlepšují orientaci autora i pozdějšího čtenáře dokumentu a proto je doporučeno hlavičku uvádět v co nejplnější podobě.

Nejdůležitější částí hlavičky je značka `<title>...</title>`, uvádějící název dokumentu. Tento název se při prohlížení dokumentu zobrazuje v záhlaví okna prohlížeče, což je důležité zejména v případě pomalého načítání stránek, kdy uživatel z tohoto názvu získává první informaci o skutečném obsahu dokumentu (hlavička se načítá jako první). Další používaná značka v oblasti hlavičky `<meta>` podává základní informace o obsahu dokumentu zejména pro účely práce vyhledávacích robotů, bez nich se naše stránky těžko objeví v databázích vyhledávačů. Tato značka má dva atributy, upřesňující typ informace o obsahu dokumentu. Atribut name informuje, jaký typ informace o obsahu bude obsažen v textovém řetězci následujícího atributu content. Nejpoužívanější jsou tři typy atributu name: author, description a keywords. Tyto typy, stejně jako textový řetězec atributu content se uvádí za rovnítko, uzavřeny v úvozovkách:

```
<head>

<title>Olomouc - historie a ákrsy ěmsta na éHan</title>
<meta name = "description" content = "áStrnky␣ěévnovan...">

<meta name = "keywords" content = "Olomouc,␣historie,...">

<meta name = "author" content = "Franta␣Historik">
```

```
9
10  </head>
```

15.2.3 Krok třetí – vytvoření základního textového obsahu HTML dokumentu

Jakýkoliv text (mimo značky HTML kódu) umístěný mezi značkami `<body>...</body>` je prohlížečem interpretován jako vlastní dokument HTML a je zobrazován v okně prohlížeče jako příslušná WWW stránka. Výjimkou je text uzavřený mezi již uvedené značky `<!-- ... -->`.

Vzhled prostého textu není ovšem graficky příliš vhodný pro elektronickou publikaci informací na Internetu, proto kód HTML obsahuje i značky pro jednoduché formátování textu. Jeho složitější úpravy pak ovládají vyšší technologie, jako jsou již zmíněné kaskádové styly. Pro počáteční úpravu našich www stránek budeme používat pouze prvky HTML kódu.

Základní možností úpravy vzhledu zobrazovaného textu je odlišení nadpisu od zbývajícího textu. Kód HTML nabízí jednoduchou párovou značku `<hn>...</hn>`, kde n j číslice označující úroveň nadpisu. Definováno je šest úrovní, jednotlivé úrovně se liší velikostí písma, poslední šestá úroveň má definovánu velikost menší než je standardní velikost písma HTML dokumentu. Z tohoto důvodu i důvodu přehlednosti HTML dokumentu není vhodné využívat na jedné stránce všechny úrovně nadpisů, dvě až tři je obvykle více než dost.

Další prvek pro formátování zobrazovaného textu je značka odstavce `<p>...</p>` (opticky oddělí text odstavce od dalšího textu, pomocí parametrů lze ovlivnit zobrazování textu). Pokud potřebujeme pouze ukončit řádek a novou větu začít na novém, poslouží k tomu nepárová značka `<br>`. Současné použití značek `<p><br></p>` vloží do dokumentu prázdný řádek.

Oddělovat jednotlivé části textu mezi sebou lze i grafickými prvky, nejjednodušeji čarou. V kódu HTML pro tvorbu čar existuje jednoduchá značka `<hr>`, která společně s atributy `size` (tloušťka čáry v pixelech) a width (délka čáry v procentech šířky stránky nebo v pixelech) umožňuje širokou variaci typů dělících čar. Lze využít navíc atribut noshade, který odstraňuje standardní stínování dělící čáry, mnohdy u tlustých čar rušící.

Další jednoduchou možnost formátování zobrazovaného textu umožňuje atribut align, použitelný jak ve značce pro nadpis tak i pro odstavec. Zarovnávat lze na střed stránky `align="center"`, nebo na její levý (`left`) či pravý okraj (`right`). Zarovnání na střed umožňuje i značka `<center>...</center>`, která ale není součástí *strict* verze normy HTML 4.01.

Text se dá ovšem předformátovat a pak přikázat prohlížeči, aby neměnil při zobrazování toto formátování. K tomuto účelu slouží párová značka `<pre>...</pre>`. Další způsob formátování textu je tvorba tzv. seznamů – ty mohou být nečíslované nebo číslované. Nečíslované seznamy se formátují pomocí párové značky `<ul>...</ul>`, s atributem type pro styl značek (circle a square) a značek `<li>...</li>` pro jednotlivé položky seznamu. Číslované seznamy se vytváří podobně, jen značka pro začátek a konec seznamu je `<ol>...</ol>` a parametr `type` určuje typ číslování – i nebo I pro římské číslice, a nebo A pro použití abecedy (malé a velké). Standardně, bez uvedení type, je použito arabské číslování.

Barvu textu lze v dokumentu měnit pomocí atributu color ve značce `<font>...</font>` (tato značka není součástí *strict* verze HTML 4.01). Barva textu se zadává opět textově nebo v RGB notaci. Mimo barvu textu lze měnit velikost písma pomocí atributu size s hodnotou v rozmezí 1–7, kde 1 značí nejmenší písmo. Skutečná velikost je závislá při vlastním zobrazení na nastavení velikosti standardního písma v prohlížeči. Velikost písma lze rovněž nastavovat zvětšením či zmenšením – do atributu size se zapíše číslo se znaménkem + pro zvětšení a − pro zmenšení písma oproti standardní velikosti. Atribut face mění typ použitého písma.

Velikost písma můžeme ovšem o bod zmenšit či zvětšit snadno jiným způsobem – k dispozici jsou i v budoucnu podporované párové značky `<small>...</small>` a `<big>...</big>`.

Typ písma se dá částečně měnit pomocí značek pro tučné písmo ..., kurzívu ... a podtržené písmo <u>...</u>. Lze využít i změnu typu písma na neproporcionální párovou značkou <tt>...</tt> (obvykle se použije typ písma Courier). Nakonec i barvu textu můžeme změnit v odstavci či jiné části textu definované značkou ... s parametrem pro změnu barvy textu color , lze ovlivnit i zarovnání textu parametrem align:

```
<body bgcolor"="pink>

<font color"="blue>
<h1 align=center>Olomouc { historie a ákrsy ěmsta na éHan</h1></font>

<hr size=5 width=80%>

<center><h2>Historie Olomouce</h2></center>

<p>éJmno Olomouc řpatilo époprv v histori éstaroslovanskmu hradisku, řžíístecmu
     brod na řece ěMorav. Hradisko nechal řpebudovat na hrad ížkne <b>řBetislav</
     b> okolo roku 1017. <br>řPed svou ísmrt ížkne řBetislav ěrozdlil Čechy a
     Moravu mezi ýsvch ěpt ůsyn, Olomouc řpipadla <b>Vratislavovi</b>. O tu sice
     řšpiel v boji se ýsvm bratrem <b>ěSpytihnvem</b>, ale po íříusmen mu ji
     ěSpytihnv ávrtil a dokonce po jeho smrti v roce 1061 řpipadl Vratislavovi
     čýesk ůtrn. V ét ědob  se stala Olomouc i ůžýdleitm íícrkevnm centrem, ťnebo
      zde Vratislav nechal žzaloit íbiskupstv émoravsk. To bylo íposleno v roce
     1078, kdy v Olomouci žzaloil ížkne <b>Ota čýSlin</b> ýbenediktinsk áškter
     na <i>Hradisku</i>.
</p>
```

Průvodce studiem

V textu uváděné příklady použití značek jazyka HTML tvoří kostky stavebnice, jejichž poskládáním vznikne úplná WWW stránka. Její podobu při zobrazení v okně prohlížeče MS Internet Explorer ukazuje obrázek 15.1. Využijte tohoto příkladu a stvořte takový dokument za využití toho nejjednoduššího nástroje - editoru obsaženém v MS Windows - Poznámkovém bloku (Notepadu).Při postupné tvorbě dokumentu můžete průběžně sledovat změny způsobené zapojením jednotlivých značek přímo v okně MS Internet Exploreru a tak současně ověřit správnost příslušné konstrukce.

15.2.4 Krok čtvrtý – vložení hypertextového odkazu v HTML dokumentu

Nejdůležitějším prvkem HTML dokumentu je hypertextový odkaz. Ten může buď odkazovat na jiný dokument ve stejném či jiném adresáři dokonce i v jiném počítači kdekoliv na světě a nebo jen na jiné místo v aktuálním dokumentu (pak se odkazu říká záložka). Odkaz se vkládá do HTML dokumentu párovou značkou ¡a¿...¡/a¿ se dvěma parametry – href je odkaz na jiný dokument či záložku a name pro vytvoření záložky v dokumentu. Pokud se odkazujeme na jiný dokument, používáme parametr href, za nějž musíme uvést buď absolutní adresu URL dokumentu (např. http://www.upol.cz/UP/Struktura/Prf/sidlo.htm) nebo jeho relativní adresu URL (pouze tu část cesty od aktuálního dokumentu k volanému), např. olomouc.html, pro dokument ve stejném adresáři, nebo ../olomouc.html, pokud je dokument o adresář výše, nebo cr/olomouc.html, pokud je dokument v adresáři cr, umístěném ve stejném adresáři jako aktuální dokument.

Pokud se odkazujeme na jinou část téhož dokumentu voláme záložku v tomto místě opět parametrem href, přičemž musí být v daném místě vložena záložka stejného jména, v odkazu uvedeného znakem #. Záložku vytvoříme v daném místě dokumentu stejnou značkou, ale s parametrem name, za nímž následuje název záložky.

Nutno podotknout, že všechny texty za parametry href či name se uvádí po znaku = a jsou uzavřeny v uvozovkách.

Příklady: Olomouc odkazuje na dokument s názvem olomouc.html,

umístěným ve stejném adresáři jako dokument s odkazem `<a href="#kasny">éolomouck škany</a>` odkazuje na záložku v textu vytvořenou pomocí `<a name="kasny">éOlomouck škany</a>`

Pokud se odkazujeme na více dokumentů, umístěných na jiném počítači, lze nastavit jeho absolutní URL adresu značkou `<base>` s parametrem `href` tak, abychom se mohli na příslušné dokumenty odkazovat jen relativními URL adresami.

Barva zvýraznění odkazů se dá ovlivnit parametry ve značce těla HTML dokumentu ¡body¿. Atribut link udává barvu pro nenavštívené odkazy, alink pro právě vybraný odkaz a vlink pro již navštívený odkaz. Obvykle je vhodné ponechat standardní nastavení a neměnit je, protože většina uživatelů je na toto standardní zabarvení odkazů přivyklá.

15.2.5 Krok pátý – vložení obrázků do HTML dokumentu

WWW stránky v čistě textové podobě jsou sice úsporné, ale chybí jim něco do krásy. Obrazová informace. Ovšem vložit obrázek do dokumentu není vůbec žádný problém, takže se naopak můžeme na Internetu potkat se stránkami, které se obrázky hemží až moc. To také není dobré. Je třeba používat tyto prvky s rozmyslem a pro doplnění textové informace, nejen pro okrasu. Navíc, protože obrázky jsou mnohdy rozměrné (datově), zdržují načítání stránek a odrazují tak uživatele od dalšího prohlížení těchto stránek. Proto je vhodné do základního dokumentu vložit zmenšené kopie obrázků (pokud ty původní jsou příliš veliké) a pro případ, že chceme nabídnout návštěvníkovi našich stránek i obrázek v plné kvalitě, vytvoříme ze zmenšeného obrázku odkaz na ten kvalitnější. V každém případě i ten by měl mít rozumnou velikost, proto používáme úsporné grafické formáty, přednostně formát JPEG.

Obrázek umístíme na stránky pomocí nepárové značky `<img>`. Protože HTML kód nabízí pro tuto operaci větší množství parametrů, probereme je postupně podle jejich užitečnosti.

src parametr udávající URL adresu grafického souboru, který má být na stránce zobrazen. Adresa může být uvedena relativně či absolutně, stejně jako u hypertextových odkazů.

alt parametr nabízející alternativně text popisující obrázek. Je důležitý v případě pomalého načítání stránek, či u uživatelů, kteří mají zobrazování obrázků vypnuto.

width parametr vymezující šířku obrázku při jeho zobrazení na stránce (v pixelech).

height parametr vymezující výšku obrázku při jeho zobrazení na stránce (v pixelech).

Použití parametrů `width` a `height` zjednodušuje zobrazení obrázků při malé rychlosti načítání stránky – prohlížeč vytvoří odpovídající rámeček a stránka se pak po načtení nemusí znovu přepisovat.

align parametr popisující obtékání obrázku textem – může to být vlevo (left), vpravo (right) a přitom může být zarovnán k horní hraně obrázku (top), středu obrázku (middle) či jeho dolní hraně (bottom).

hspace, vspace parametr nastavující vzdálenost textu od okraje obrázku (v pixelech).

border parametr definující rámeček okolo obrázku, resp. tloušťku čar (v pixelech) ohraničujících obrázek. Pokud rámeček nechceme, musíme zadat tloušťku nula.

Jak již bylo řečeno výše, obrázek může být zároveň součástí hypertextového odkazu:

```
1  <a href"=bigobrazek."jpg><img src"=smallobrazek."gif></a>
```

15.2.6 Krok navíc – umístění obrázku na stránce pomocí tabulky

Pokud chceme umístit samotný obrázek na určité místo stránky, není v kódu HTML k dispozici mnoho nástrojů. Můžeme provést jeho vycentrování na stránce pomocí značky ¡center¿, kterou ovšem není doporučeno používat. Podstatně více možností nabízí využití tvorby tabulek, kde pomocí umístění obrázku do buňky tabulky můžeme obrázek umisťovat na stránce prakticky libovolně.

Značka pro tvorbu tabulky `<table>...</table>` může být doplněna atributy align (umístění tabulky na stránce) a border (šířka čáry ohraničení tabulky – pokud se nezadá, je standardně nula). Parametr width určuje šířku tabulky (v pixelech či % šířky stránky).

Značku tabulky doplňují další dvě značky – značka pro vytvoření řádku `<tr>...</tr>` a značka pro vytvoření buňky v řádku `<td>...</td>`. Obě značky mají parametry width (šířka řádku či buňky v pixelech nebo % šířky tabulky) a align (způsob zarovnávání textu v buňkách na daném řádku nebo jen v dané buňce – center, right, left).

Využití značek pro umístění hypertextového odkazu a obrázku včetně jeho umístění pomocí tabulky ilustruje poslední část příkladu HTML dokumentu o Olomouci. Příklad rovněž ilustruje syntaxi vnořených značek - jako první se zakončuje ta značka, která byla použita jako poslední.

```
<html>
<body>
<center><h2>Olomoucka radnice</h2></center>

<p>Dominantou Horniho namesti je <a href="radnice.html">radnice</a>. Ta tu stoji
     od roku 1378, kdy zde <u>Premysl Otakar II.</u> povolil mestanum postavit
    kupecky dum, ktery se stal soucasne  radnici. Stavba byla mnohokrat
    upravovana, na konci 15.stoleti bylo pristaveno druhe patro a velky goticky
     sal a na prelomu 16. a 17.stoleti byly provedeny jeji renesancni upravy.
</p>

<table width=100%>
 <tr>
 <td align=center>
 <img src="radnice.jpg" width=282 height=403 alt="radnice">
 </td>
 </tr>
</table>

<p><br></p>

<center><h2>Olomoucke kasny</h2></center>

<p>Soubor<a href="http://www.historicka.olomouc.cz/clanky/kasny_hanus.htm"> sest
     baroknich kasen</a> v historickem jadru Olomouce je jednou z vyznamnych
    pamatek nasi republiky a tvori jej tyto kasny:
</p>

<ul>
 <li>Caesarova a Herkulova kasna na Hornim namesti</li>
 <li>Neptunova a Jupiterova na Dolnim namesti</li>
 <li>Merkurova kasna na ulici 1. maje</li>
 <li>Tritonova kasna na namesti Republiky</li>
</ul>

</body>
</html>
```

Spojením všech dílčích příkladů vznikne jednoduchý HTML dokument, jehož vzhled v okně webového prohlížeče MS IE Exploreru ukazuje obrázek 15.1.

Shrnutí

Základní strukturu dokumentu HTML definují tři značky – značka `<html>...</html>` vymezuje začátek a konec dokumentu, značka `<head>...</head>` hlavičku dokumentu a značka `<body>...</body>` jeho tělo. Nejdůležitější součástí hlavičky je název dokumentu, v těle jsou pak umístěny informace zobrazované v okně prohlížeče. Jazyk HTML poskytuje prostředky pro jednoduché formátování textu, vkládání hypertextových odkazů a obrázků do HTML

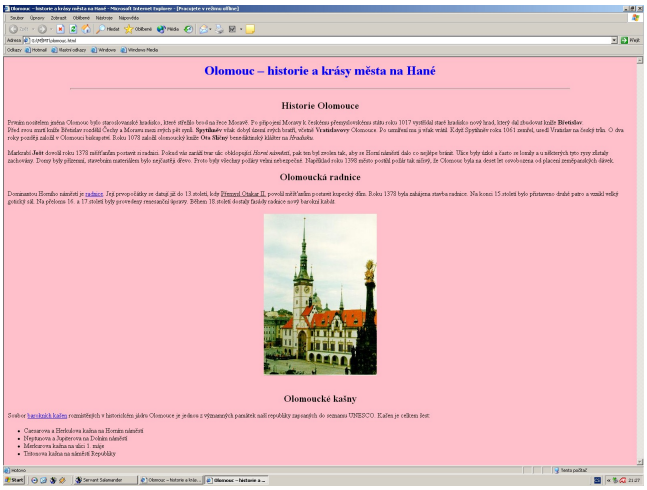
dokumentu. Z pokročilejších funkcí je to pak tvorba seznamů a tabulek, které lze navíc použít pro rozšířené formátování HTML dokumentu při jeho zobrazení v okně prohlížeče.

Pojmy k zapamatování

- Značka pro vymezení HTML dokumentu `<html>...</html>`.
- Značka pro vymezení hlavičky HTML dokumentu `<head>...</head>`.
- Značka pro vymezení těla HTML dokumentu `<body>...</body>`.
- Značka pro vložení hypertextového odkazu `<a href="jmeno_dokumentu">...</a>`.
- Značka pro vložení obrázku `<img src="jmeno_souboru">`.

Kontrolní otázky

1. Jak by měl začínat a končit každý dokument HTML?
2. Jak se vloží do HTML dokumentu hypertextový odkaz?
3. Jak se vloží do HTML dokumentu obrázek?
4. Existuje v HTML jazyku zančka pro tvorbu seznamů?



Obrázek 15.1: Vzhled HTML dokumentu podle probíraného příkladu v okně MS Internet Exploreru.

Kapitola 16

Závěr

Cílem tohoto učebního textu bylo seznámení studujícího se základy technologií Internetu a jeho informačních služeb. Protože tento text i předmět je zaměřen opravdu na začátečníky (neinformatiky) v této oblasti, byla hlavní pozornost věnována, vedle vysvětlení základních principů problematice, základním možnostem nastavení programů, používaných uživateli k přístupu k jednotlivým informačním službám Internetu. Závěrečné kapitoly textu pak byly věnovány nejpoužívanější informační službě Internetu - službě World Wide Web, včetně základů tvorby WWW stránek, tedy HTML dokumentů. Pro zájemce o rozšíření svých znalostí v této oblasti existuje navazující předmět Tvorba WWW stránek, věnovaný již výhradně technologiím služby WWW a rozšířeným možnostem tvorby WWW stránek za využití formátování pomocí kaskádových stylů a dynamických prvků vytvořených v jazyce Java Script.