Zo zákulisia elektronickej pošty (1.)

Najpopulárnejšou službou dnešných počítačových sietí je bezpochyby elektronická pošta, ktorá priťahuje stále viacej užívateľov. Aj keď ide o službu, ktorá môže byť v sieťach rôzneho typu implementovaná odlišným spôsobom, jej celkový efekt je pre užívateľa prakticky vždy rovnaký.

Elektronickú poštu je možné označiť za novodobý fenomén, ktorý zásadne mení spôsob, akým ľudia spolu komunikujú. Ak sa vrátime do minulosti, tak napríklad v 18. storočí trvalo niekoľko týždňov, než sa nejaká správa dostala z Európy do Ameriky, zatiaľ čo dnes sa prenos správ aj na druhú stranu planéty meria na sekundy. Vďaka elektronickej pošte a ďalším moderným spôsobom komunikácie dnes nie je problémom komunikovať s ktorýmkoľvek človekom na Zemi.

História a dostupnosť elektronickej pošty

Prvé e-mailové systémy boli vyvinuté koncom 60. a začiatkom 70. rokov. Tieto systémy boli prevažne malé súkromné systémy v rámci oddelení, s malou snahou sprístupniť jednotlivým e-mailovým systémom komunikáciu medzi sebou. Koncom 70. a začiatkom 80. rokov sa stali dostupné verejné e-mailové služby prostredníctvom poskytovateľov AT&T Mail, MCI Mail a CompuServe. Výskumné a akademické e-mailové služby sa vyvinuli do toho, čo sa neskôr stalo internetom. Pretože služby pre posielanie správ sa stávali populárnejšie a viacej používané, rástla aj potreba vzájomnej interoperability. Ako výsledok toho boli vyvinuté tieto štandardy:

* Štandardy pre elektronické posielanie správ a poštu zaistila rada doporučení X.400 od CCITT (Consultative Commitee for International Telegraphy and Telephony). Prvá verzia štandardov X.400 sa objavila v roku 1984 a je známa ako MHS 84 (Message Handling System, 1984). Systémy X.400 dnes bežne slúžia ako chrbtica pre doručovanie správ medzi e-mailovými systémami.
* Protokol SMTP (Simple Mail Transfer Protocol) v sade protokolov IP (Internet Protocol) zaistil e-mailové štandardy a protokoly pre internet.
* Koniec 90. rokov a začiatok tisícročia sľubujú pre elektronickú poštu niekoľko ďalších vývojových krokov:
* Rast šírky pásma, cez e-mail bude možné posielať aj obrovské súbory. Prebieha už plánovanie pre gigabitové úrovne a diskutuje sa dokonca o sieťach s terabitovými rýchlosťami.
* Podpora pre video, audio a grafiku v poštových službách posielania správ. Smernice týkajúce sa spôsobu, akým sa má s týmito dátami pracovať, zabezpečujú rozšírenie Multipurpose Internet Mail Extension (MIME). Pretože tieto rozšírenia predstavujú iba začiatok, je pravdepodobné, že v tejto oblasti dôjde k zásadnému vývoju.
* Vznik inteligentných agentov, ktorý pomáhajú s obsluhou a doručením pošty.
* Vývoj bezdrôtových poštovných služieb bude pokračovať a prispeje tak k podnieteniu zlepšenia v oblasti bezdrôtových sietí.
* Zobecnenie elektronickej pošty a posielanie správ, ktoré zasahuje do elektronického obchodu (napríklad prostredníctvom EDI, Electronic Data Interchange).
* Použitie šifrovania, digitálnych podpisov a ďalších bezpečnostných techník, ktoré uchovajú obsah e-mailových správ skrytý pred neautorizovanými očami.

Toto sú základné vylepšenia e-mailu, pokiaľ sa má stať prostriedkom pre elektronický obchod. Príkladom takéhoto bezpečnostného opatrenia je PEM (Privacy Enhanced Mail). Pre šifrovanie je možné použiť tiež algoritmus PGP (Pretty Good Privacy).

Systém prenosu správ elektronickej pošty

UA (User Agent) - v systéme spracovania správ CCITT X.400 aplikačný proces (program), ktorý poskytuje užívateľovi prístup k systému prenosu správ (MTS). UA vytvára rozhranie, prostredníctvom ktorého môže užívateľ využívať služby elektronickej pošty. Používateľ ho spúšťa až na základe potreby.

MTA (Message Transfer Agent) - programy, ktoré majú na starosti vlastný prenos správ a nevšímajú si obsah správy. Zaujíma ich predovšetkým adresa príjemcu. Bežia na jednotlivých počítačoch a musia vzájomne spolupracovať. Takto vzájomne spolupracujúce MTA nazývame Message Transfer Systems.

V modeli X.400 je MTA súčasť systému obsluhy správ (Message Handling System - MHS), ktorá je zodpovedná za ukladanie alebo prenos správ ďalším MTA, užívateľským agentom alebo inému autorizovanému príjemcovi. MTA je v prostredí TCP/IP porovnateľný s poštovým agentom Mail Transfer Agent.

MTS (Message Transfer System) - proces, ktorý prenáša správy medzi užívateľmi. Za týmto účelom MTS využíva iba vlastné komponenty (MTA). MTS sa vyznačujú tým, že používajú jednotné konvencie a protokoly.

X.400 - štandard spracovania správ definovaný organizáciou CCITT.

Elektronická pošta v prostredí TCP/IP

Elektronická pošta je bezpochyby najrozšírenejšia zo všetkých služieb, ktoré internet ponúka. Elektronická pošta je ako väčšina služieb internetu založená na modeli klient - server (obr. 2). Základom elektronickej pošty je existencia tzv. poštovej schránky Mail Box, ktorá vychádza z filozofie Post Office Boxu. Každý užívateľ má vlastnú elektronickú poštovú schránku (mailbox, jedinečný adresár pre ukladanie elektronickej pošty) a ostatní užívatelia mu môžu posielať e-mailové správy. Tieto správy sa posielajú na e-mailovú adresu. E-mailová adresa je určená dvojicou údajov: identifikátorom schránky v rámci daného počítača a adresou počítača. Pokiaľ je pošta uložená v schránke príjemcu, môže užívateľ tejto schránky vyvolať akékoľvek pre neho dôležité alebo zaujímavé správy. Pokiaľ nejaká e-mailová správa nemôže byť doručená, môže byť dočasne uložená v poštovnom úrade (post office). To je služba, ktorá umožňuje ukladať správy s možnosťou periodicky kontrolovať, či je príjemca pripravený doručenú poštu prevziať. Elektronická pošta nie je nikdy zaisťovaná jediným programom, vždy ide o spoluprácu viacerých programov, ktoré sú rôznym spôsobom špecializované. Napríklad existujú programy, ktoré sa starajú iba o prenos správ, prezeranie správ, vytváranie a ich odosielanie. Základnými RFC dokumentmi, ktoré sa zaoberajú elektronickou poštou, sú:

RFC 821 [11] - definuje základný model elektronickej pošty a jej prenos pomocou protokolu SMTP;
RFC 822 [12] - špecifikuje formát textových správ pre elektronickú poštu;
RFC 1521 [13] - definuje rozšírenie elektronickej pošty MIME, ktoré umožňuje prenos aj iných súborov ako textových.

Okrem týchto základných dokumentov existuje ešte veľa ďalších, ktoré ich dopĺňajú, avšak všetky vychádzajú z uvedených RFC dokumentov.

Adresovanie správ

Pôvodný systém UUCP (Unix-to-Unix Copy) používal adresy v tvare:

počítač!užívateľ

Výkričník sa vyslovuje ako bang, takže tomuto spôsobu adresovania sa hovorilo "bang notáciaŽ. Pokiaľ je cieľový počítač vzdialený, musí sa obyčajne špecifikovať kompletná cesta, po ktorej sa bude správa uberať. Príkladom môže byť UUCP adresa v tvare

počítač1!počítač2!počítač3!počítač4!užívateľ

Význam tejto adresy je taký, že správa sa najprv odošle na počítač1, ten ju po prijatí odošle na počítač2, počítač2 ju ďalej odošle na počítač3 , ten ju odošle na počítač4, kde ju obdrží konkrétny užívateľ. Cesta v tomto tvare môže obsahovať až 20 počítačov. Základný dokument RFC 822 definuje nový spôsob takzvaného doménového adresovania, ktorý sa používa dnes. Takáto adresa má tvar

užívateľ@doménové_meno

kde doménové_meno je utvorené podľa pravidiel Domain Name System (DNS). Užívateľ je identifikátor poštovej schránky v rámci daného počítača. V doménovom adresovaní je možné špecifikovať medzistanicu (poštovú bránu), cez ktorú má daná správa prejsť. Formát takejto adresy je nasledujúci:

užívateľ%cieľový_počítač@brána

Ak je na strane odosielateľa správne nakonfigurovaný poštový software, je formát tejto adresy potrebný len veľmi zriedka.

Formát poštovej správy

Každá poštová správa sa skladá z dvoch častí: hlavičky (header) a tela správy (body). Telo správy obsahuje vlastný text správy a z pohľadu systému elektronickej pošty nie je nijako štruktúrované - ani užívateľské zložky (UA), ani prenosové zložky (MTA) túto časť správy neinterpretujú (okrem špeciálnych prípadov, ako napríklad pri potrebe konverzie z jednej znakovej sady do druhej). Naopak hlavička musí byť veľmi presne štruktúrovaná, lebo obsahuje informácie, podľa ktorých sú jednotlivé správy odosielané, prenášané a doručované. Každý systém elektronickej pošty (MHS, Message Handling System) musí presne definovať, čo má byť v hlavičke obsiahnuté a akým konkrétnym spôsobom to má byť vyjadrené. To preto, aby si užívateľské zložky (UA) a prenosové zložky (MTA) dokázali v hlavičke správy nájsť tie informácie, ktoré potrebujú k svojej činnosti. Syntaxom hlavičky sa podrobne zaoberá dokument RFC 822 [12]. Hlavička sa musí nachádzať pred telom správy a telo správy musí byť od hlavičky oddelené najmenej jedným prázdnym riadkom (CRLF CRLF). To z toho dôvodu, že všetko, čo nasleduje za prvým prázdnym riadkom, sa považuje za text správy. Hlavičku správy dokument RFC 822 definuje ako postupnosť položiek, ktorým sa v origináli hovorí header fields (polia hlavičky). Každá položka hlavičky musí začínať na novom riadku (na prvej pozícii riadku) a môže pokračovať na ďalších riadkoch (v takom prípade ale nesmie začínať od prvej pozície riadku). Každá položka začína nejakým kľúčovým slovom (zakončeným dvojbodkou), ktoré definuje jej význam. Za kľúčovým slovom a dvojbodkou nasleduje vlastný obsah príslušnej položky. Hranaté zátvorky majú význam v mene počítača; signalizujú, že meno počítača nemá byť prekladané pomocou DNS (obr. 3). Bodkočiarka má význam separátora, používa sa napríklad pri oddeľovaní adresátov v hlavičke v poli To:. Text uzatvorený v oblých zátvorkách je považovaný za komentár a pri interpretácii niektorých polí hlavičky je ignorovaný. Lomené zátvorky (< >) zase označujú údaje prednostne určené pre poštový program. Napríklad poštovú adresu je možné zapísať aj takto:

"Bill Gates" <bill@microsoft.com>
Bill Gates <bill@microsoft.com>
<Bill.Gates@microsoft.com>

Poštový program si vezme iba údaje uzatvorené v lomených zátvorkách. Dokument RFC 822 nepredpisuje povinné poradie jednotlivých položiek hlavičky. Údaje uvedené v hlavičke musia byť kódované v klasickom 7-bitovom ASCII formáte.

Položky hlavičky

Najdôležitejšie hlavičkové polia (obr. 3) sú definované v dokumente RFC 822 takto:

From: E-mailová adresa odosielateľa, prípadne jeho skutočné meno. Pre toto pole existuje veľa formátov zápisu adresy. Jeden z možných zápisov je na obr. 3 .

To: E-mailová adresa, eventuálne i meno príjemcu.

Cc: Carbon Copy. Za týmto kľúčovým slovom nasledujú adresy tých používateľov, ktorým sa dáva list alebo správa na vedomie. Jednotlivé adresy sa oddeľujú čiarkou.

Bcc: Blind Carbon Copy. Tu sa špecifikujú adresy príjemcov kópie, u ktorých nechceme, aby túto skutočnosť adresát vedel. Toto pole sa pred odoslaním správy zmaže.

Reply-To: Pole obsahuje adresu, na ktorú sa má odosielateľovi poslať prípadná odpoveď. Môže byť užitočné vtedy, ak máte niekoľko poštových adries, ale pritom chcete dostávať poštu iba na jednu adresu, ktorú používate najčastejšie.

In-Reply-To: Obsah tohto poľa identifikuje predchádzajúcu korešpondenciu, ktorá je odpoveďou na vašu správu.

Subject: Stručný popis obsahu správy.

Sender: Špecifikuje odosielateľa správy (ak je to niekto iný než autor správy, pre ktorého je určená položka From:).

Date: Dátum odoslania správy, vrátane údajov o časovom posuve vzhľadom k svetovému času.

References: Obsah tohto poľa identifikuje inú korešpondenciu, na ktorú sa táto správa odkazuje.

Message-ID: Reťazec, ktorým je správa identifikovaná - je automaticky generovaný poštovým programom.

Keywords: Kľúčové slová charakterizujúce obsah. Jednotlivé slová sú od seba oddelené čiarkou.

Comments: Poznámka; komentár.

Encrypted: Šifrované (zastaralé).

Received: Toto pole vloží do hlavičky každý poštový uzol (e-mailový server) na ceste medzi stanicami odosielateľa a príjemcu, ktorý sa danou správou zaoberal. Pole obsahuje názov poštového uzla, číslo id správy, čas a dátum, kedy daný uzol správu obdržal, ďalej od ktorého poštového uzla správa

pochádza a ktorý transportný software bol použitý k doručeniu správy. Tieto informácie sa uvádzajú z toho dôvodu, aby bolo možné vystopovať, kadiaľ správa išla, a hľadať zdroj eventuálnych problémov. Pole Received: sa správne číta zdola nahor. V tomto poli sa môžu vyskytovať nasledujúce slová: from - počítač, z ktorého bola správa prijatá, by - počítač, ktorým bola správa prijatá, via - fyzická cesta, with - sieťový alebo poštový protokol, id - príjemcova identifikácia správy, for - pre koho je správa určená (napr. ak je adresátom bill@microsoft.com, potom sa tu zachováva pôvodný adresát, t.j. bill@microsoft.com).

Return-Receipt-To: Pokiaľ hlavička obsahuje toto pole, zašle sa po úspešnom doručení do schránky adresáta potvrdenie na uvedenú adresu. Hodnotu takéhoto potvrdenia je treba brať s rezervou, pretože jeho nedoručenie nemusí znamenať, že správa nedorazila na miesto určenia.

X-anything: Tento reťazec sa používa kvôli implementácii doplnkových vlastností, ktoré zatiaľ neboli uverejnené v dokumentoch RFC, alebo ktoré ani uverejnené nebudú. Príkladom je položka X-Mailer:, ktorá zvyčajne obsahuje typ a verziu poštového programu, z ktorého bola správa odoslaná. Ak poštový program nepozná význam niektorého poľa začínajúceho X-, mal by ho ignorovať. Ďalšie položky tohoto typu sú napríklad X-Accept-Language:, X-Priority:, X-UIDL a pod.

Resent- Pri automatickom odovzdávaní správy (napr. vráteniu nedoručiteľnej správy) sa pred pôvodné hlavičkové polia vloží reťazec Resent- (napr. Resent-From alebo Resent-Cc a pod.).

Nie všetky uvedené kľúčové slová sú povinné, RFC 822 určuje minimálne požiadavky na hlavičku správy takto:

Date: 26 Aug 76 1429 EDT
From: Jones@Registry.org
Bcc:

alebo

Date: 26 Aug 76 1429 EDT
From: Jones@Registry.org
To: Smith@ Registry.org

Záznam v poli Bcc: môže byť prázdny, zatiaľ čo v poli To: je požadovaná aspoň jedna adresa.

Formát tela správy - rozšírenie MIME

Pôvodný dokument RFC 821 a RFC 822 obsahoval iba rámcové smernice pre formát tela poštovej správy. Znaková sada bola obmedzená základným 7-bitovým ASCII kódom a počet znakov v jednom riadku bol obmedzený číslom 1000. To bol aj dôvod, prečo pri písaní poštových správ nebolo možné používať znaky s interpunkčnými znamienkami (ASCII kód takéto znaky neobsahuje). Okrem toho sa elektronická pošta ukázala byť vhodným prostriedkom aj pre prenášanie rôznych binárnych súborov (obrázky, audio, formátovaný text a pod.). Preto sa používali rôzne externé kódovacie schémy, napríklad v Unixe programy uuencode a uudecode, ktoré umožňovali transformovať ľubovolný binárny súbor do tvaru, ktorý vyhovoval norme RFC 821 [11]. Systémové riešenie bolo dosiahnuté prostredníctvom takzvaných rozšírení MIME (Multipurpose Internet Mail Extensions), špecifikácia ktorých je obsiahnutá v normách RFC 1521 a RFC 1522. MIME je štandardom, ktorý doplňuje normu RFC 822 a zároveň zabezpečuje spätnú kompatibilitu. Rozšírenie MIME zaviedlo tieto nové hlavičkové polia (obr. 4):

MIME-Version: Indikuje, že správa je zostavená podľa noriem RFC 2045 až RFC 2049.
Content-Type: Špecifikuje typ a podtyp dát posielaných v tele správy (text, audio, video a pod.).
Content-Transfer-Encoding: Špecifikuje typ kódovania, pomocou ktorého je správa transformovaná do formátu, ktorý vyhovuje RFC 821, t.j. do krátkych riadkov v 7-bitovom ASCII kóde.
Content-ID: Identifikácia správy použiteľná v možnom odkaze.
Content-Description: Textový popis obsahu správy.

Peter Gašparovič

Literatúra:

[1] Feiber, W.: Encyklopedie počítačových sítí, Computer Press, Praha, 1996
[2] Břehovský, P.: Praktický úvod TCP/IP, KOPP, České Budějovice, 1994
[3] Mrázek, L.: První kroky INTERNETEM aneb Je to na WWW!, KOPP, České Budějovice, 1995
[4] Šmrha, P. - Rudolf, V.: Internetworking pomocí TCP/IP, KOPP, České Budějovice, 1995
[5] Hejna, L.: Lokální počítačové sítě, GRADA, Praha, 1994

[6] Falk, B.: Průvodce světem Internetu, Computer Press, Praha, 1995
[7] Lhotka, L.: SERVER v INTERNETU, KOPP, České Budějovice, 1997
[8] Peterka, J.: Co je čím ... v počítačových sítích, COMPUTERWORLD č. 4, 7, 9, 17, 21, 3 5, 44, 1994
[9] Sterling, B.: Short History of the Internet, The Magazine of Fantasy and Science Fiction, 1993
[10] RNDr. Dostálek, L., Ing. Kabelová, A.: MIME - Multipurpose Internet Mail Extension, http://info.pvt.net/mime.htm, 1997
[11] Postel, J. B.: Simple Mail Transfer Protokol, RFC # 821, August 1982
[12] Crocker, D. H.: Standard For The Format Of Arpa Internet Text Messages, RFC # 822, August 1982
[13] Borenstein, N., Freed, N.: MIME (Multipurpose Internet Mail Extension) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies, RFC # 1521, September 1993
[14] Borenstein, N., Freed, N.: Multipurpose Internet Mail Extension (MIME) Part One: Format of Internet Message Bodies, RFC # 2045, November 1996
[15] Rose, M.: Post Office Protocol - Version 3 , RFC # 1225, May 1991
[16] Rose, M., Myers, J.: Post Office Protocol - Version 3 , RFC # 1725, November 1994
[17] Dresslerová, B., Veselský, J., Gombik, G.: Linux Dokumentační projekt, Computer Press, Praha, 1998
[18] Šovčík, J.: Login, PC Revue č. 4 až 8, 1995
[19] Palúch, P.: Poznáte Linux?, PC Revue č. 2, 1998
[20] Rivest, R.: The MD5 Message-Digest Algorithm, RFC # 13 21, Apríl 1992
[21] RNDr. Dostálek, L. a kol.: Velký průvodce protokoly TCP-IP Bezpečnost, Computer Press, Praha, 2001

Vysvetlivky

RFC (Request for Comments) Sada článkov, v ktorých sa dokumentujú a zverejňujú štandardy internetu, návrhy štandardov a obecne odsúhlasené myšlienky.

DNS (Domain Name System) Systém doménových mien. Distribuovaný hierarchický informačný systém využívaný v IP sieťach, umožňujúci preklad symbolických doménových mien (napr. www.zoznam.sk) na číselné IP adresy (195.85.36.45).