Aplikačná vrstva

Ciele

Čo by mal študent vedieť:

- ✓ funkcie aplikačnej vrstvy
- ✓ riadenie procesov na aplikačnej vrstve
- ✓ služby aplikačnej vrstvy – podporné (DNS, Telnet) a špecifické (e-mail, www, multimédiá)
- ✓ protokoly aplikačnej vrstvy (SMTP, http, FTP, VoIP, SIP,....)
- ✓ architektúru sietí klient-server a peer to peer

Úvod

Aplikačná vrstva je najvyššou vrstvou v OSI modelu a vrstvou, ktorá je najbližšie k používateľovi. Definuje spôsob, akým komunikujú so sieťou aplikácie.
Prostredníctvom aplikácií sú poskytované služby koncovému zákazníkovi.
Nižšie vrstvy ju izolujú od technických problémov prenosu a rieši len aplikačnú problematiku.
Možno povedať, že poskytuje služby používateľským aplikáciám, ktoré sú mimo OSI modelu, nie niektorej vrstve OSI modelu. Využíva služby prezentačnej vrstvy.
Dôvodom existencie aplikačnej vrstvy je, aby umožnila aplikáciám prístup do sietí na báze ISO/OSI modelu. Funguje ako brána medzi aplikáciami, ktoré sú v rôznych uzloch a vzájomne si vymieňajú informácie.
Základnou funkciou aplikačnej vrstvy je teda poskytovať používateľským programom ucelené a dobre definované služby.
Zaradenia používané v aplikačnej vrstve sú počítače.
Dátový formát sú dáta.

Aplikácia

V tejto súvislosti je potrebné vymedziť pojem aplikácia – aplikačný program, aplikačný proces, aplikačné úlohy ako jednej časti programového vybavenia, ktoré zaisťujú tie funkcie počítača, kvôli ktorým sa počítač používa. Druhou časťou programového vybavenia počítača je zaistenie tých funkcií, ktoré zaisťujú vlastný chod počítača ako takého a vytvára aplikáciám také prostredie, v ktorom aplikácie môžu pracovať.

Aplikácia

Aplikáciami počítača sú používateľské programy a zvyšná časť programového vybavenia je operačný systém, ktorý používateľským programom sprostredkovanie využitia rôznych zdrojov a prostriedkov daného počítača, ako diskov, operačných pamätí, klávesnice, displejov, a iných zariadení. Aplikáciami sú napríklad databázové systémy, elektronická pošta alebo programy pre emuláciu terminálov, web prehliadač ale aj tabuľkové procesory, textové editory a programy bankových terminálov.
V prípade uzlových počítačov, ktoré sú zapojené v komunikačnej sieti je odlišnosť v tom, že sieťový operačný systém implementuje v sebe jednotlivé vrstvy sieťového modelu a sprostredkováva aplikáciám naviac ešte všetko, čo ponúka sieť, predovšetkým možnosť

komunikácie s inými aplikáciami, ktoré sú na iných uzlových počítačoch, prípadne prístup k iným technickým prostriedkom iných uzlových počítačov.

Proces

V **informatike je proces bežiaca inštancia programu** vrátane všetkých hodnôt premenných a stavu. Multitasking operačného systému prepína medzi procesmi, čím vzniká dojem súčasného behu viacerých procesov, hoci v skutočnosti je vo všeobecnosti možné vykonávať iba jeden proces v jednom jadre CPU (*central processing unit).*
Neformálne povedané, **proces je úloha, ktorú vykonáva počítač**, často súčasne s inými.
Mnohé procesy môžu existovať súčasne, pričom sa striedajú pri využívaní CPU.
Operačný systém tiež poskytuje mechanizmy komunikácie medzi procesmi, aby bola umožnená komunikácia bezpečným a predvídateľným spôsobom.
Z hľadiska prístupu aplikačných procesov ku komunikačným funkciám sú v sieťach používané **sieťové operačné systémy**. Operačný systém riadi poskytovanie kapacít servera a spoluvytvára sieťové prostredie. Ako sieťové operačné systémy sú používané produkty firmy Microsoft.
Pre malé skupiny postačuje sieť peer-to-peer. Operačný systém WINDOWS 95, 98, 2000, XP poskytuje sieťové služby pre takúto sieť do maximálne 10 počítačov.

Pre siete s vyhradeným serverom možno použiť operačný systém **Windows Server** pre server a WINDOWS 95, 98, 2000, XP pre pracovné stanice siete.

Funkcie aplikačnej vrstvy

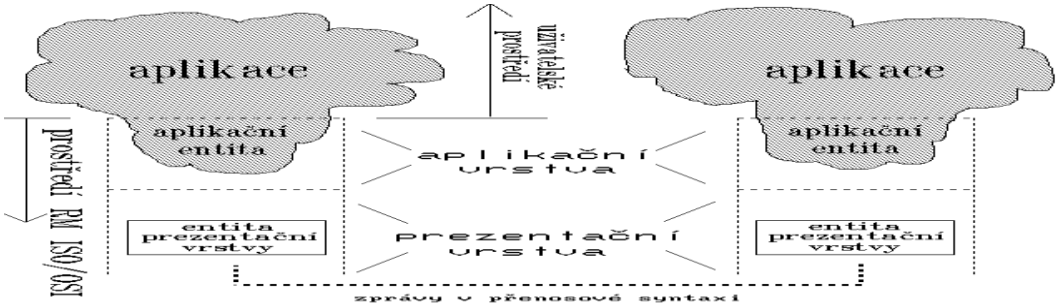
Okrem **základnej funkcie aplikačnej vrstvy (L7)**, ktorou je poskytovať služby používateľským aplikáciám, možno uviesť ďalšie dielčie funkcie, ktoré sú zabezpečované aplikačnou vrstvou:

- identifikácia účastníkov komunikácie,
- zaistenie dostupnosti účastníka komunikácie,
- rozhodovanie o povolení komunikácie žiadateľom,
- určenie metódy pre stanovenie cien (kto to bude platiť),
- umožnenie prístupu k požadovaným zdrojom,
- stanovenie metód pre opravu chyby, potvrdzovanie prijatých správ,
- vlastný prenos dát spolu so začiatočnou a ukončovacou procedúrou.

Využitie uvedených dielčích funkcií je závislé od použitej služby a jej aplikačného protokolu.

Vývoj a kategórie funkcií aplikačnej vrstvy

Funkcie aplikačnej vrstvy prešli zložitým vývojom. Pôvodná predstava v prvej verzii referenčného modelu predpokladala, že jednotlivé používateľské aplikácie budú zasahovať do aplikačnej vrstvy.
Tie časti aplikácie, ktoré sa budú bezprostredne týkať využitia siete budú priamo súčasťou aplikačnej vrstvy ako aplikačné entity (*application entities*). Znázornenie tejto predstavy je na obr. 7.1.

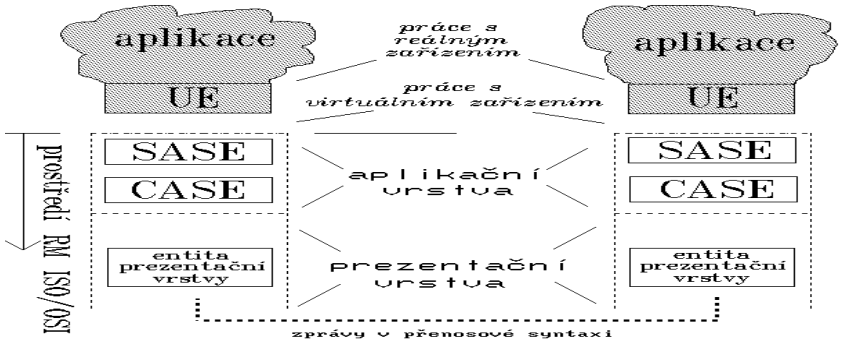


Obr. 7.1 Pôvodná predstava aplikačnej vrstvy

Takáto predstava znamenala, že jednotlivé aplikácie, resp. ich časti, ktoré tvorili aplikačné entity si museli zabezpečovať všetky služby aplikačnej úrovne samé pomocou služieb prezentačnej vrstvy. Referenčný model ISO/OSI tieto služby na úrovni aplikačnej vrstvy nijako podrobne nešpecifikoval, len vymedzil, ktoré sú potrebné pre vzájomnú komunikáciou otvorených systémov. Neboli špecifikované žiadne protokoly prostredníctvom ktorých by mali byť služby realizované. Bolo to v čase, keď neexistovali protokoly aplikačnej vrstvy.
Neskôr, v priebehu prác na implementácii sieťových aplikácií sa ukázalo, že väčšina týchto aplikácií má mnoho spoločného a nie je potrebné, aby si každá aplikácia implementovala vždy to, čo na aplikačnej vrstve potrebuje. Preto sa pôvodná predstava referenčného modelu zmenila a zaistenie služieb na aplikačnej vrstve prebrali aplikačné entity, ktoré nie sú súčasťou jednotlivých aplikácií, ale sú súčasťou sieťového programového vybavenia.
Neskôr sa zistilo, že takto koncipované aplikačné entity je najvýhodnejšie zostavovať z ešte menších celkov, ktoré zabezpečujú dielčie služby. Tieto prvky sa označujú **ASE** (**Application Service Elements**). Tieto prvky sú na aplikačnej úrovni dvojakého typu:

- **CASE - Common Application Service Element,** potrebné na podporu aplikácií rôznych typov.
- **SASE, Specific Application Service Element,** ktoré realizujú špecifické služby, potrebné len pre konkrétny typ aplikácií.

Príklad prvkov služby aplikačnej vrstvy (*Application Service Elements)* je na obr. 7.2.



Obr. 7.2 Znázornenie *Service Elements* aplikačnej vrstvy

Príkladmi všeobecných aplikačných prvkov sú služby komunikácie a iné podporné služby. Komunikácia môže byť realizovaná ako spojovaná prostredníctvom logického spojenia medzi dvoma aplikačnými entitami, alebo nespojovaná zaisťovaná výmenou správ. Logické spojenie na aplikačnej vrstve má na starosti prvok ACSE *(Association Control Service Element),* ktorý

patrí medzi CASE prvky. Nespojovaná komunikácia má charakter vzdialeného volania procedúr (*remote procedure call)*. Pre zaistenie takéhoto spôsobu komunikácie je potom potrebný iný prvok CASE, ktorý sa označuje ROSE *(Remote Operations Service Element).*

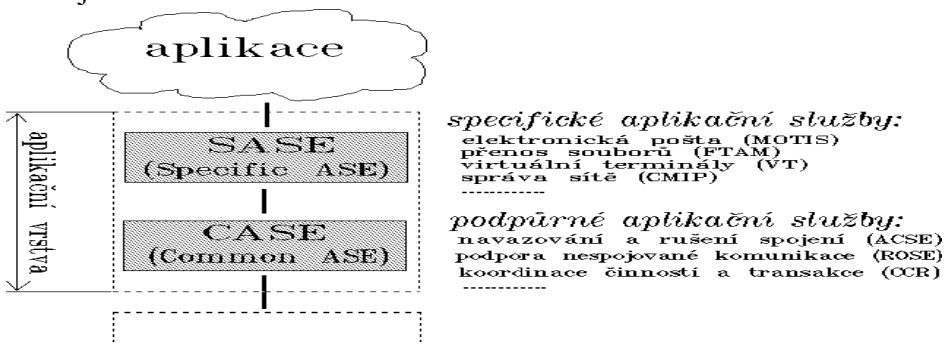
Prvky SASE majú na starosti špecifické aplikačné služby, kde patrí napríklad prenos súborov, elektronická pošta, apod. Referenčný model RM OSI pritom predpokladá, že tieto služby budú implementované tak, aby sa voči vlastným aplikačným procesom chovali vždy rovnako. Tento prístup je zrejmý zo spôsobu, ako sa model RM OSI vyrovnáva s rôznorodosťou používaných terminálov, ktoré sa líšia svojimi parametrami, spôsobom ovládania a pod. Pokiaľ sieťová aplikácia potrebuje iné služby, než aké sú jej ponúkané prvkami CASE a SASE v súvislosti s predstavou virtuálneho zariadení, musí si ich sama podľa svojich konkrétnych potrieb upraviť. V rámci väčšiny aplikácií sa preto ešte vymedzuje vrstva, ktorá zaisťuje potrebné prispôsobenie. V terminológii ISO/OSI modelu sa táto vrstva označuje ako používateľský prvok ***UE (User Element),*** obr. 7.2.

Služby aplikačnej vrstvy

Služby poskytované aplikačnou vrstvou sa tak delia do dvoch skupín:

- **Špecifické aplikačné služby**
- **Podporné aplikačné služby.**

Ich znázornenie ja na obr. 7. 3.



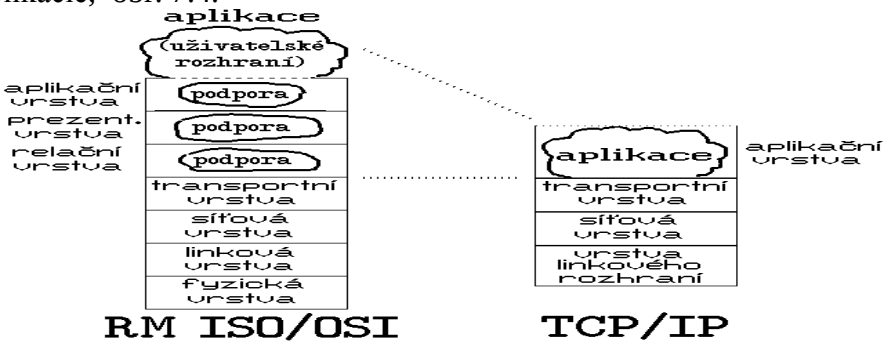
Obr. 7.3 Rozdelenie služieb aplikačnej úrovne

Pre špecifické služby aplikačnej vrstvy, poskytované prvkami SASE, sú vytvárané potrebné protokoly, ktoré špecifikujú procesy príslušnej služby. Väčšina z nich dnes má formu medzinárodných štandardov.
Špecifické služby siete internet sú elektronická pošta, World Wide Web a multimediá.
Podporné služby sú prístup k vzdialenému terminálu, správa domén,..

Porovnanie aplikačnej vrstvy RM OSI a TCP/IP

Referenčný model ISO/OSI bol vytvorený za predpokladu, že jednotlivé aplikácie budú mať mnoho spoločného, a že sa vyplatí realizovať ich spoločné časti samostatne, a implementovať ich len raz. Súvisí to zo spôsobom, akým aplikačné protokoly v rámci referenčného modelu vznikali. Tento prístup možno označiť za maximalistický a príkladom je protokol pre prenos súborov v rámci ISO/OSI označený FTAM - File Access, Transfer and Management, ktorý je tak obsiahly a komplikovaný, že nikdy nebol implementovaný v celom rozsahu.
Naproti tomu sieťový model TCP/IP vznikal viac z praktických skúsenosti a potrieb. Jeho aplikácie začínali ako relatívne jednoduché, a postupom času sa ich funkcie a schopnosti

zväčšovali, a začali sa zavádzať nové, náročnejšie druhy aplikácií. Sieťový model TCP/IP vychádza z predpokladu, že jednotlivé aplikácie nebudú mať veľa spoločného, aby sa tieto ich spoločné časti vyplatilo osamostatniť. Na rozdiel od referenčného modelu ISO/OSI sa preto očakávalo, že každá aplikácia si sama zaistí to, čo potrebuje a čo jej nižšie vrstvy neposkytujú. Až v poslednej dobe sa i v rámci sieťového modelu TCP/IP začínajú niektoré podporné mechanizmy v rámci aplikační vrstvy osamostatňovať, napríklad volanie vzdialených procedúr.
Tu je treba uvedomiť si rozdiel medzi referenčným modelom ISO/OSI a sieťovým modelom TCP/IP, ktorý spočíva v počte ich vrstiev. Referenčný model ISO/OSI totiž zaraďuje medzi transportnú vrstvu a vrstvu aplikačnú ešte dve ďalšie vrstvy, relačnú a prezentačnú, ktoré tiež poskytujú služby vlastným aplikáciám. Sieťový model TCP/IP však nemá žiadnu analógiu relačnej a prezentačnej vrstvy ISO/OSI. Tieto funkcie si v prostredí TCP/IP musia zaistiť jednotlivé aplikácie, obr. 7.4.



Obr. 7.4 Porovnanie aplikácie v RM OSI a TCP/IP

Referenčný model ISO/OSI aj sieťový model TCP/IP boli navrhnuté pre heterogénne prostredie, počítačových sietí, ktorých uzlové počítače sa môžu i dosť výrazne líšiť nielen použitým hardvérom, ale tiež napríklad konvenciami pre znázorňovanie čísiel, kódovaním jednotlivých znakov, konvenciami operačných systémov vo vlastníctve a prístupových právach k súborom apod. V referenčnom modeli OSI sa o odstránenie niektorých odlišností, hlavne vo vnútorných formátoch, stará prezentační vrstva. V modeli TCP/IP je všetko na samotných aplikáciách.
Vývoj aplikačnej vrstvy v RM OSI a TCP/IP je v tabuľke 1.

RM ISO/OSI	**TCP/IP**
• snaha vytvárať „bohaté“ a „dokonalé“ aplikačné protokoly	• postupný vývoj, od jednoduchšieho k zložitejšiemu • aplikácie vznikali ako jednoduché, a až potom sa obohacovali • rozširovalo sa aj spektrum aplikácií
• eletronická pošta – **MOTIS/X.400** *(Message Oriented Text Interchange System)* • adresárové služby – **X.500** • práca so súbormi – **FTAM** *(File Transfer, Access Management)*	• „počiatočná množina“ aplikácií: o vzdialené prihlasovanie (Telnet, rlogin) o prenos súborov (FTP) o elektronická pošta (SMTP, RFC 822) • ďalšie aplikácie o zdieľanie súborov (NFS) o zdieľanie informácií (NNTP)

• vzdialené prihlasovanie – **VT** *(Virtual Terminal)* • správa, management – **CMIP** *(Common Management Information Protocol)*	○ sprístupnenie informácií ▪ Gopher ▪ WWW – (HTTP) ○ vyhľadávanie informácií ▪ Archie, WAIS, Veronica ...
• väčšina z nich sa neujala a nepoužíva sa • u niektorých ISO/OSI protokolov sa došlo k použitiu ○ X.400 – MS Exchange bol založený na X.400 ○ X.500 – na jeho základe vznikol protokol LDAP	• dochádza k vzniku platforiem ○ el. pošta, www nie sú už len službami/aplikáciami, ale stávajú sa platformami, nad ktorými sa vytvárajú nové služby • niektoré pôvodné aplikácie časom zanikajú ○ napr. vyhľadávanie sa stáva nadstavbou WWW

Protokoly aplikačnej vrstvy

Protokoly aplikačnej vrstvy sú štandardizované špecifikácie, ktoré zabezpečujú špecifické komunikačné služby. Komunikačné protokoly aplikačnej vrstvy je možné rozdeliť podľa typu poskytovaných služieb do dvoch základných skupín podľa toho, či poskytujú podporné služby, alebo špecifické služby:
Protokoly podporných služieb aplikačnej vrstvy sú:

- **DNS *(Domain Name System),*** je systém na správu doménových mien počítačov a ich IP adries. Umožňuje preklad doménového mena na IP adresu (priamy preklad) a opačne (reverzný preklad). Pre internet je DNS kľúčovou záležitosťou, ktorú zabezpečujú programy na obsluhu DNS, označované ako DNS servery.
- **LDAP *(Lightweight Directory Access Protocol)*** je adresárový protokol založený na protokole **X.500** a zahrnuje väčšinu z jeho primárnych funkcií.
- **X.500** je model pre adresárové služby *(Directory Services)* v koncepte RM OSI.
- **TELNET (*Telecommunication Network)***
  Vytvára terminálovú prevádzku. Prostredníctvom Telnetu môžeme pracovať zo vzdialeným počítačom rovnako, ako by sme boli pri termináli, ktorý je k nemu bezprostredne pripojený. Pretože komunikácia prebieha nešifrovane predstavuje jeho používanie bezpečnostné riziko. Náhradou za TELNET je SSH SSH *(Secure Shell)* ktorý komunikuje šifrovane.
- **NFS RPC/XDR** Vzdialené volanie procedúr. Používa sa pri požiadavke vykonať výpočet programov na inom počítači než kde sú uložené dáta.

Protokoly špecifických služieb aplikačnej vrstvy, ktoré priamo podporujú používateľské aplikácie možno rozdeliť do troch skupín, ktoré používajú príslušné protokoly podľa potreby príslušnej služby:

1. **Elektronická pošta,** E-mail alebo email, mail prípadne mejl, je skratka pre „elektronickú poštu“ Je to spôsob písania, posielania a prijímania správ v elektronických

komunikačných sieťach. Väčšina dnešných emailových systémov používa internet, a e-mail je jedným z najobľúbenejších použití internetu. Protokoly e-mailu

- **SMTP** *(Simple Mail Transfer Protocol)* pre prenos elektronickej pošty alebo dokumentov z definovaného zdroja do definovaného cieľa.
- **POP3 a IMAP** pre prístup k e-mailovej schránke adresáta.

2. **World Wide Web**

- HTTP (*Hypertext Transfer Protocol)* - slúži k prístupu na www stránky. HTTPS je zabezpečený (šifrovaný) prenos www stránok.
- FTP **FTP** *File Transfer Protokol,* pre prenos súborov alebo viet so stručným určením obsahu a formy od definovaného zdroja k definovanému cieľu. Zdroj i cieľ by mali mať logické mená a byť nezávislé na mieste aktuálnej implementácie. To slúži napríklad k tomu, že si používateľ siete môže na akomkoľvek pracovisku po zadaní svojho loginu a hesla alebo iných kľúčov vyvolať svoje pracovné prostredie TFTP je jednoduchší variant k FTP.
- Cookois RFC 2109
- **WAP *(Wireless Application Protocol)*** je systém pre zaistenie prevádzky elektronických služieb na mobilných telefónoch.

3. **Multimédiá**

- **VoIP** (Voice over Internet Protocol) je protokol na prenos hlasu cez IP siete, označuje sa aj ako IP telefónia.
- **H.323** je doporučenie ITU Telecommunication Standardization Sector (ITU-T), které definuje protokoly pro audio-vizuální relace komunikace v jakékoli paketové síti
- **RTSP *(Real Time Streaming Protocol),*** vyvinutý IETF v roku 1998 ako RFC 2326, je protokol pre používanie streamovaných systémov ktoré umožňujú používateľovi vzdialenú kontrolu na streamingovom media serveri používaním príkazov "play" a "pause" a umožňujú prístup k súborom na serveri..

Popis niektorých protokolov

DNS - Domain Name System

DNS je systém, ktorý ukladá prístup k informácii o názve stroja (hostname) a názve domény v istej distribuovanej databáze v počítačových sieťach ako internet. Najdôležitejšie je, že poskytuje mechanizmus získania IP adresy pre každé meno stroja (lookup) a naopak (reverse), a uvádza poštové servery (MX záznam) akceptujúce poštu pre danú doménu.
DNS vynašiel Paul Mockapetris v roku 1983; originálna špecifikácia sa nachádza v RFC 882 a 883. V roku 1987 aktualizovali špecifikáciu RFC 1034 a RFC 1035, čím RFC 882 a RFC 883 zastarali. Niekoľko ďalších RFC navrhlo do protokolov rôzne zmeny.
DNS poskytuje na internete všeobecne dôležitú službu, pretože kým počítače a sieťový hardvér pracujú s IP adresami, ľudia si vo všeobecnosti ľahšie pamätajú mená strojov a domén pri použití napr. v URL ***(Uniform Resource Locator)*** a e-mailovej adrese. Zložité by to bolo hlavne pri IPv6 adrese.

Využitie DNS

Najzákladnejšie využitie DNS je preklad názvu stroja na IP adresu. Podobá sa to telefónnemu zoznamu. Napríklad ak chcete vedieť IP adresu stránky en.wikipedia.org, tak DNS vám povie, že IP adresa tejto stránky je 66.230.200.100. DNS má však aj ďalšie dôležité typy využitia. DNS umožňuje priradenie internetovej adresy k stránke nejakej organizácie či firme ktorú reprezentuje, nezávisle od fyzickej smerovacej hierarchie, ktorú predstavuje číselná IP adresa. Vďaka tomu internetové odkazy môžu reprezentovať to isté, čo daná IP adresa, a tak môžme použiť ľuďom bližšiu formu (napr. "wikipedia.org"), čo sa celkom určite pamätá ľahšie ako IP adresa (napr. 66.230.200.100). Takto majú ľudia výhodu pri zadávaní URL, resp. e-mailovej adresy, keďže sa nemusia starať o to ako počítač daný odkaz nájde.
Takto DNS poskytuje schopnosť priradenia domény a jej mapovanie v sieti IP adries, napríklad serverom ktorý uchováva pre každú doménu jej vlastný zápis zmien, čím predchádza potrebe hlavného správcu k akejkoľvek aktualizácii.

História DNS

DNS vynašiel Paul Mockapetris v roku 1983; originálna špecifikácia sa nachádza v RFC 882 a 883. V roku 1987 aktualizovali špecifikáciu RFC 1034 a RFC 1035, čím RFC 882 a RFC 883 zastarali. Niekoľko ďalších RFC navrhlo do protokolov rôzne zmeny.

Typy DNS záznamov

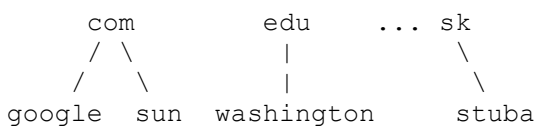
Medzi dôležité kategórie údajov uložené v DNS patria

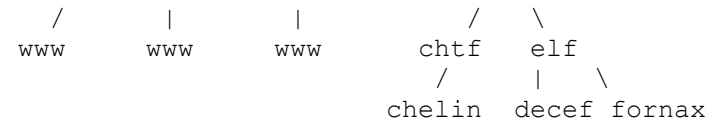
- A záznam alebo záznam adresy mapuje hostname na 32-bitovú IPv4 adresu.
- AAAA záznam alebo záznam IPv6 adresy mapuje hostname na 128-bitovú IPv6 adresu.
- CNAME záznam alebo záznam kanonické meno spôsobuje, že jeden názov domény je aliasom pre iný. Takáto doména má platné všetky subdomény a DNS záznamy originálu.
- MX záznam alebo mail exchange záznam mapuje meno domény na zoznam mail exchange serverov pre danú doménu.
- PTR záznam alebo ukazovateľ mapuje hostname na kanonické meno stroja. Ak je PTR záznam nastavený na doménu `in-addr.arpa`, znamená to, že IP adresa implementuje tzv. en:reverse DNS lookup alebo reverz pre danú adresu. Napríklad, `www.icann.net` má IP adresu 192.0.34.164, ale PTR záznam mapuje `164.34.0.192.in-addr.arpa` na jeho kanonické meno, `referrals.icann.org`.

Iné druhy záznamov slúžia jednoducho na informačné účely (napríklad **LOC** záznam udáva fyzické *umiestnenie* stroja) alebo uloženie experimentálnych údajov (napríklad **WKS** záznam udáva zoznam serverov poskytujúcich v rámci domény niektoré zo *štandardných služieb* ako HTTP alebo POP3).

Doménové meno sa skladá z častí (domén, subdomén) oddelených bodkou. Doména môže obsahovať znaky "A-Z", "a-z", "0-9", "-" a "_".

DNS je vytvárané ako strom domén:





Výhodou stromového riešenia je, že každú časť stromu môže spravovať iný server. Správa systému domén je teda distribuovaná, čo znižuje možnosť výpadku celého systému v prípade výpadku niektorého uzla.
Najvyššiu úroveň stromu domén - domény najvyššej úrovne *(top-level domains, TLD*) spravujú koreňové DNS servery. Tie obsahujú údaje o DNS serveroch pre domény najvyššej úrovne ("`.com`", "`.net`", "`.sk`" atď.). Koreňové DNS servery sú veľmi dôležité, pretože sú nevyhnutné pre správnu činnosť celého internetu. Preto existuje niekoľko koreňových DNS serverov, ktoré sú rozmiestnené na viacerých kontinentoch. Adresy týchto serverov sú verejne známe a nachádzajú sa v konfigurácii každého DNS servera.
Ak DNS server spravuje doménu, môže vytvárať domény nižšej úrovne (subdomény) a buď obsahuje údaje o týchto doménach, alebo odkaz na podriadené DNS servery, ktoré ich spravujú. Napríklad DNS server pre "`stuba.sk`" obsahuje odkazy na DNS servery domén "`chtf.stuba.sk`" a "`elf.stuba.sk`" (a mnoho ďalších). Na DNS serveri pre doménu "`elf.stuba.sk`" nájdete napr. údaje o serveroch "`decef.elf.stuba.sk`" a "`fornax.elf.stuba.sk`".
Časť stromu domén, ktorú spravuje DNS server, sa nazýva **zóna.**
TTL *(Time To Live)* je čas, počas ktorého klient považuje informáciu o doménach/adresách za platnú. Po uplynutí tohto času si opäť obnovuje informácie z DNS.

DNS servery rozdeľujeme na **dva** základné druhy:

- **Primárny DNS server** je server, ktorý obsahuje a obsluhuje údaje o doméne a je pre danú doménu autoritatívny. Odpovede primárneho DNS servera sú považované za vždy aktuálne a platné. Odkazy na DNS servery domény sú uložené v nadradenom DNS serveri. Ukazovatele na DNS servery druhej úrovne ("`mojadomena.sk`") sú uložené v DNS pre doménu najvyššej úrovne ("`.sk`").
- **Sekundárny DNS server** je server, ktorý pomocou pravidelného kopírovania údajov o doménach z primárneho DNS servera vytvára záložný DNS server pre danú doménu. Úlohou primárneho DNS servera je tiež upozorniť svoje sekundárne DNS servery pri zmene záznamov v DNS. Jeden primárny DNS server môže používať niekoľko sekundárnych DNS serverov, vždy však najmenej jeden.

Jeden DNS server môže byť autoritatívny aj pre viacero domén (typicky napr. provider Internetu), ale pre jednu doménu môže byť autoritatívny iba jeden DNS server.

Primárny DNS server sa v terminológii DNS servera BIND označuje aj ako "master", sekundárny server ako "slave".

Telnet[1]

Telnet je protokol pre vzdialenú prácu na počítači cez internet. Umožňuje počítaču používateľa správať sa ako vzdialený terminál na inom počítači hocikde v internete. To znamená, že keď sa Telnetom pripojíte na nejaký vzdialený host a port, vzdialený počítač (ktorý musí mať Telnet server) akceptuje vstup priamo z používateľského počítača, ktorý

musí mať a Telnet klienta. Cez Telnet sa možno dostať k mnohým funkciám vzdialeného počítača.
Telnet bol štandardizovaný ako IETF STD 8 (RFC 854 a RFC 855) a je jeden z prvých internetových štandardov.
K vytvoreniu spojenia z Telnet klienta musia byť vybrané voľby pre spojenie. Typicky sa volí meno hosta a typ terminálu. Meno hosta je IP adresa alebo DNS meno vzdialeného počítača. Typ terminálu popisuje typ emulácie, ktorú by mal Telnet klient vykonávať.
Jeho účelom je poskytovať pomerne všeobecný obojsmerný prostriedok komunikácie s osembitovým slovom. Primárnym cieľom je poskytnúť štandardizované rozhranie prostredníctvom siete pre terminálové zariadenia a terminálovo orientované procesy. Tiež je možné jeho využitie na komunikáciu medzi terminálmi navzájom a medzi procesmi navzájom.
Bežnou aplikáciou bolo vzdialené prihlasovanie k terminálu, telnet však prenáša údaje v čisto textovej forme, preto ho v tejto aplikácii z dôvodov bezpečnosti nahradil protokol SSH. Hoci rozšírenia protokolu už definujú TLS zabezpečenie a SASL autentifikáciu, väčšina implementácií ich nepodporuje a prevažuje používanie SSH.

Telnet je protokol klient-server, využíva TCP štandardne na porte 23. Medzi aplikácie patria prístup k aplikáciám, MUD *Multi-User Dungeon* hrám, talkerom a BBS *(Buletin Board System).*

Telent inak

Potřeba vzdáleného přihlašování (anglicky: remote login) je v rámci TCP/IP řešena protokolem Telnet. Ten se v souladu s celkovou filosofií TCP/IP snaží spíše o jednoduchost, univerzálnost a minimální vazbu na okolní systémové prostředí, tak aby umožnil vzájemnou spolupráci (formou vzdáleného přihlašování) i dosti odlišným platformám. Prostřednictvím Telnetu se například můžete přihlásit k Unixovskému počítači, přičemž váš počítač, vystupující v roli vzdáleného terminálu, může být velmi jednoduchým PC s MS DOSem, výkonnějším PC s MS Windows, nebo znovu Unixovským počítačem či něčím ještě úplně jiným. Stejně tak dobře se ale můžete přihlásit (prostřednictvím Telnetu) třeba k sálovému počítači, k počítači VAX apod. Důležité je to, aby systémové prostředí vzdáleného počítače podporovalo terminálové relace a vzdálené přihlašování prostřednictvím Telnetu (aby zde byl implementován tzv. Telnet démon) - což třeba Unix běžně činí, ale například MS Windows (včetně Windows NT) nikoli.
Podstatným rysem protokolu Telnet je jeho rozšiřitelnost - na schopnosti obou komunikujících stran se zcela záměrně snaží klást co možná nejmenší nároky, tak aby šanci měl i velmi „hloupý" (tj. jednoduchý) klient. Pokud ale proti sobě stojí dva uzly s dokonalejšími schopnostmi, mohou se vzájemně dohodnout na jejich používání. Příkladem může být vztah k přenosu jednotlivých znaků v rámci sedmi či osmi bitů - Telnet standardně počítá s tím, že jednotlivé znaky jsou přenášeny jako sedmibitové (což mj. činí značné problémy české diakritice). Pokud ale obě komunikující strany dokáží pracovat s osmibitovými znaky, mohou se dohodnout na změně, a předávat si osmibitové znaky.

Zdieľanie súborov *(file sharing)*

Zdieľanie súborov je služba na používanie vzdialených a miestnych súborov. Pri zdieľaní súborov nie je nutné poznať umiestnenie vzdialených súborov. So vzdialenými a miestnymi súbormi sa pracuje rovnako. Pre presun súborov z miestneho umiestnenia na vzdialené a naopak nie je treba podnikať žiadne explicitné akcie. Aplikácia to zaisťuje sama. V TCP/IP je najpoužívanejším protokolom pre zdieľanie súborov je protokol NFS *(Network File System*).

Protokol je platformovo nezávislý, to znamená, že klient a server môžu mať rôzne platformy. Napríklad file server môže byť Unixovým počítačom, a jeho klient napríklad počítačom PC s DOS-em, MS Windows atď.
Samotný protokol NFS, realizujúci vlastné zdieľanie súborov je podložený dvoma samostatnými službami - službou pre vzdialené volanie procedúr RPC *(Remote Procedure Call)* a XDR *(eXternal Data Representation).* Zmyslom mechanizmu RPC je skryť pred programátormi existenciu siete a vytvoriť ilúziu toho, že všetko sa odohráva na jednom počítači - programátori volajú procedúry a funkcie, o ktorých si myslia že sú lokálne ale v skutočnosti sú procedúry a funkcie vykonávané na vzdialených počítačoch, odtiaľ názov vzdialené volanie procedúr. Výhodou je, že aplikačný programátor nemusí poznať špecifiká siete a práce v sieti. Mechanizmus XDR potom zaisťuje prípadné konverzie dátových formátov, ak je potrebné. Obidva mechanizmy boli vytvorené takýmto spôsobom preto, aby boli relatívne nezávislé a využiteľné aj inými aplikačnými
službami a ich protokolmi. Znázornenie je na obr.7.6.

Obr. 7.6 Umiestnenie protokolov RPC a XRD

Uvedené umiestnenie protokolov pripomína samostatnú relačnú a prezentačnú vrstvu v referenčnom modelu ISO/OSI, ktorá sa v TCP/IP najskôr javila ako zbytočná. Tento príklad ukazuje, že sa zrejme postupne presadí stredná cesta medzi RM OSI a TCP/IP, aj keď nie v podobe zmeny počtu vrstiev modelov.
Ďalšími protokolmi pre zdieľanie súborov sú v TCP/IP AFS *(Athena File System),* najnovšie CIFS *(Common Internet File System).* V RM ISO/OSI protokol FTAM *(**File** Transfer Access and Management),* pre Microsoft, MS protokol SMB (Server Message Blocks)

Elektronická pošta

Existujú rôzne koncepcie – Mail602, ccMail, MS Mail, X.400... Líšia sa formátom správ, prenosovými mechanizmami,...
SMTP (Simple Mail Transfer Protocol), je jednoduchý protokol umožňujúci prenos e-mailov medzi stanicami. založená na konkrétnej koncepcii (protokoly SMTP a RFC 822)
Protokol zaisťuje doručenie pošty pomocou priameho spojenia medzi adresátom a odosielateľom; správa je doručená do tzv. poštovej schránky adresáta, ku ktorej môže užívateľ pristupovať pomocou protokolov POP3 a IMAP. Jedná sa o jednu z najstarších aplikácií, pôvodná norma RFC 821 bola vydaná v roku 1982 (V roku 2001 ju nahradila novšia s názvom RFC 2821). SMTP funguje nad protokolom TCP, využíva port TCP/25.
Základná koncepcia elektronickej pošty je v rámci protokolov TCP/IP definovaná jednak protokolom SMTP (Simple Mail Transfer Protocol), a jednak štandardom RFC821. Tento štandard definuje formát správ, prenášaných elektronickou poštou, do čoho spadá aj spôsob adresovania a formát adries. Protokol SMTP sa potom tyká konkrétneho spôsobu prenosu jednotlivých správ medzi poštovnými servermi.

Důležitou vlastností elektronické pošty, definované standardem RFC821 a protokolem SMTP (a označované obvykle jako tzv. SMTP pošta) , je orientace na přenos čistě textových zpráv tvořených sedmibitovými znaky (tzv. čistými ASCII znaky). Ačkoli přenosové cesty obvykle dokáží přenášet osmibitové znaky a mnohé implementace SMTP pošty s nimi dokáží pracovat, obecně to zaručeno není. Pak stačí jediné „sedmibitové úzké hrdlo" v celém

přenosovém řetězci, aby z obsahu původně osmibitové zprávy zbylo jen hodně málo jejího původního obsahu.

Lidé ale potřebují přenášet prostřednictvím elektronické pošty v prostředí TCP/IP (tj. prostřednictvím tzv. SMTP pošty) i takové věci, které nemají charakter čistě textových zpráv, tvořených pouze sedmibitovými znaky. Například binární (datové) soubor, programy, ale také formátované texty, texty s národních abecedách apod. Jelikož ale přenosový mechanismus el. pošty garantuje korektní přenos pouze pro sedmibitové znaky, musí být vše ostatní pro potřeby přenosu zakódováno právě do této podoby (tj. do podoby posloupnosti sedmibitových znaků).

Pokud se všechny komunikující strany správně dohodnou, je v zásadě jedno, jaké konkrétní kódování použijí. V praxi se pak nejvíce ujalo tzv. uuencodování, pocházející ještě z doby existence protokolů UUCP (Unix-to-Unix Copy Protocol). To se sice stalo jistým nepsaným standardem, který dokáže vyhovět potřebám přenosu jednotlivých netextových příloh k textovým zprávám, ale stále ještě nejde o systematický přístup, který by věc řešil zásadním způsobem, formou všeobecně uznávaného a akceptovaného standardu. To dělá až novější standard MIME (Multipurpose Internet Mail Extensions), který lze chápat jako rozšíření původní koncepce elektronické pošty. Jak už název tohoto standardu napovídá, počítá s existencí nejrůznějších formátů včetně multimediálních, a činí z elektronické pošty dosti univerzální přenosový kanál.

SMTP - Simple Mail Transfer Protocol

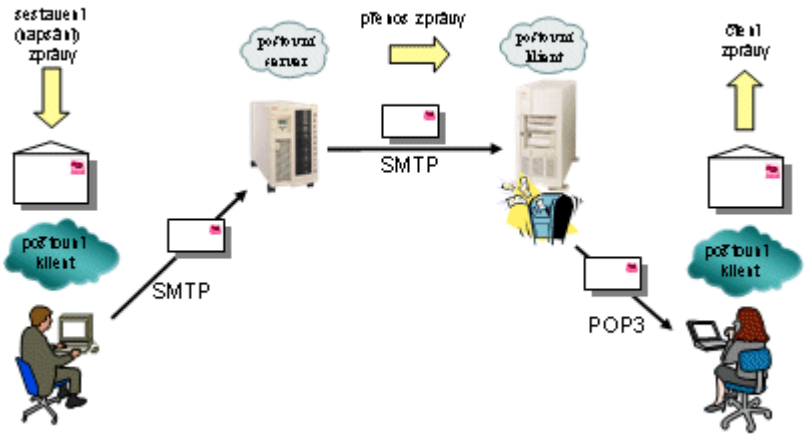
- Začína ako jednoduchý protokol, postupne sa obohacuje
  - pôvodne vznikla ako veľmi jednoduchá služba
  - ako elektronická obdoba „office memo“
  - pôvodne prenášala len krátke texty v čistom ASCII tvare
- ďalšie vlastnosti a schopnosti sa pridávali najprv postupne, pokiaľ sa ukázala ich potreba
  - možnosť formátovania textu, vkladanie obrázkov
  - možnosť prenosu netextových príloh
  - podpora národných abecied
- el. pošta vychádza z modelu klient/server
  - poštovný server (mail server)
    - v RM ISO/OSI: MTA, Message Transfer Agent
    - zaisťuje transport správ
    - zhromažďuje správy pre tých účastníkov, ktorí sú momentálne nedostupní
  - poštovný klient
    - v RM ISO/OSI: UA, User Agent
    - umožňuje čítať, písať a inak spracovávať jednotlivé správy
    - vytvára užívateľské rozhranie
- štandardy el. pošty musia pokrývať
  - prenos správ (medzi servermi)
    - definuje protokol SMTP
  - formát správ a adries
    - definuje odporučenie RFC822
  - download

        - sťahovanie správ zo schránky na poštovnom serveri
        - definuje protokol POP3, IMAP
    - rozšírenie (národné abecedy, prílohy, formátovanie)
        - definuje štandard MIME

POP3

- *Post Office Protocol version 3* (POP3) je internetový protokol aplikačnej vrstvy, ktorý sa využíva na prijatie pošty zo vzdialeného servera prostredníctvom TCP/IP spojenia pomocou protokolu POP3 sa štandardne komunikuje na porte 110.
- skoro všetci, ktorí využívajú emailové účty u niektorého z Internet Service Providerov /ISP/ získavajú prístup k svojim emailom prostredníctvom klientského software, ktorý využíva POP3.

Ako mnoho iných starších internetových protokolov, POP3 pôvodne podporoval iba nešifrované prihlasovacie mechanizmy. I keď POP3 je bežný jednoduchý (nezabezpečený) prenos hesiel, podporuje súčasne niekoľko autentizačných metód overovania na rôznych úrovniach ochrany pred neoprávneným prístupom k cudzej poštovej schránke. Jedna taká metóda, APOP (kde základnou špecifikáciou definuje ako „voliteľný príkaz“), užíva MD5 hash funkciu pre zabezpečený prenos hesla od klienta na server. Klienti podporujúci APOP sú napríklad Mozilla, Thunderbird, Eudora a Novell Evolution. Klienti môžu takisto kódovať celú POP3 komunikáciu použitím SSL alebo modernejšieho TLS.



IMAP ***(Internet Message Access Protocol)***
IMAP je internetový protokol umožňujúci prístup k e-mailovým schránkam.V súčasnosti sa používa verzia **IMAP4** (IMAP version 4 revision 1 - IMAP4rev1) definovaná v RFC 3501. Na rozdiel od protokolu POP3 je optimalizovaný pre prácu v dlhodobo pripojenom režime, keď správy zostávajú uložené na serveri a priebežne sa sťahujú, keď je to potrebné. Rozdiely zahrňujú podporu pre prácu viacerých pripojených klientov zároveň, uchovávánie stavov správ na serveri, podporu viac zložek a prehľadávanie správ na strane servera.

MIME ***(Multipurpose Internet Mail Extensions)***

Standard MIME v zásadě definuje tři věci:

- použitelné způsoby kódování přenášených dat
- způsob vyjádření typu dat, které jsou přenášeny
- způsob „vložení" netextových dat do původní, čistě textové zprávy (formátované dle RFC82).

Jak uvidíme později, některé mechanismy a konvence standardu MIME se používají i jinde, než jen v elektronické poště - například když WWW server posílá svému klientovi (browseru) nějaká data, musí k nim připojit také informaci o typu těchto dat. A právě k tomu používá konvence standardu MIME (tzv. MIME type).

Standard MIME je jedním z novějších přírůstků ve světě TCP/IP, a je motivován především soudobým rozvojem Internetu a potřebami jeho uživatelů. Stejným důvodům vděčí za svůj vznik i další protokoly, které ještě také souvisí s elektronickou poštou. Jde například o celou skupinu protokolů, které dovolují vzdáleným uživatelům (nejčastěji s připojením komutovanými linkami veřejné telefonní sítě) stahovat si jejich elektronickou poštu z poštovních serverů, na které jim jejich pošta dochází. V současné době je k tomuto účelu nejvíce používán protokol POP (Post Office Protocol) verze 3. Původní protokol SMTP není k tomuto účelu použitelný proto, že předpokládá trvalou existenci spojení, a pak také proto, že nedovoluje ověřit identitu uživatele, který by si jeho prostřednictvím stahoval svou poštu.

World Wide Web

Služba World Wide Web, která dnes doslova hýbe celým Internetem, má po technické stránce mnoho společného se sdílením souborů a systémem NFS. Původně totiž vznikla v komunitě fyziků zabývajících se vysokými energiemi, jako řešení jejich potřeby sdílení informací, především textového charakteru (konkrétně ve švýcarském středisku CERN). Časem se ale prosadila i do světa TCP/IP, a postarala se o nebývalý boom Internetu. Po stránce implementační jde opět o řešení, tvoření několika složkami - zejména protokolem HTTP (HyperText Transfer Protocol), který definuje způsob přenosu WWW stránek po síti, mezi WWW serverem a jeho klientem, a pak jazykem HTML (HyperText Markup Language), který definuje formát jednotlivých stránek. V poslední době pak k těmto dvěma „základním" složkám přibývají další, které mají za úkol dále zvyšovat schopnosti a funkční možnosti služby WWW. Jde například o jazyk Java, mechanismy ActiveX, nebo různé zabezpečovací mechanismy a protokoly (jako SSL, S/HTTP, SET apod.), které umožňují provádět prostřednictvím služby WWW bezpečné transakce. Formální standardizace těchto složek, v rámci obvyklé standardizační mašinérie světa TCP/IP, však zatím poněkud pokulhává - není ostatně ani moc divu, vzhledem k neuvěřitelně rychlému vývoji v této oblasti.

Také po stránce svého fungování má služba WWW hodně společného se sdílením souborů á la NFS. Komunikace WWW serveru a jeho klientů je totiž také bezestavová, a WWW server si tedy obecně nepamatuje nic o tom, co po něm chtěl určitý klient někdy dříve. Důsledkem je větší robustnost než jaké by bylo možné dosáhnout při stavovém způsobu komunikace. Výhody přitom pociťujeme skoro všichni: pokud jste k Internetu připojeni po modemu, tj. přes komutované linky veřejné telefonní sítě, pak váš browser dokáže bez problémů přežít i výpadek spojení, a po opětovném „dovolání se" můžete ve svém brouzdání pokračovat, jako kdyby se nic nestalo.

HTTP - *Hypertext Transfer Protocol*

Hypertext Transfer Protocol (HTTP) pracuje s World Wide Web, čo je najrýchlejší rastúca a najpoužívanejšia služba internetu. Jeden z hlavných dôvodov takého záujmu o web je jednoduchý prístup k informáciám pomocou internetového prehliadača. Ten reprezentuje rôzne dáta na internetových stránkach, ktoré sú vo formáte (X) HTML *(eXtended Hypertext Markup Language)*. Prevádzané linky týchto dokumentov umožňujú jednoduchú navigáciu. Cesta k stránkam je daná identifikátorom *Uniform Resource Locator* (URL). Klient si vyžiada požadovanú stránku a pokiaľ tá na serveri existuje, dostane ju.
HTTP (skratka **Hypertext transfer protocol**) je primárna metóda prepravy informácií na world wide webe. Pôvodný účel bol poskytovať prostriedky pre publikáciu a obdržiavanie HTML stránok.
Vývoj HTTP koordinovalo World Wide Web Consortium a pracovné skupiny Internet Engineering Task Force, čím vytvorili sadu dokumentov RFC, predovšetkým RFC 2616 definujúci HTTP/1.1, dnes používanú verziu HTTP.
HTTP je protokol definuje požiadavky a odpovede medzi klientmi a servermi. HTTP klient (označovaný ako *user agent*), ako webový prehliadač zvyčajne začne požiadavku nadviazaním TCP spojenia na určenom porte vzdialeného stroja (štandardne port 80). HTTP server počúvajúci na danom porte čaká, kým klient pošle reťazec s požiadavkou ako "GET / HTTP/1.1" (ktorý žiada o zaslanie štartovacej stránky web servera) nasledovaný sériou hlavičiek podobných MIME opisujúcich detaily požiadavky a nasledovaných ľubovoľných údajov. Po prijatí požiadavky server pošle reťazec s odpoveďou ako "200 OK" nasledované hlavičkami spolu so samotnou správou, ktorej telo tvorí obsah požadovaného súboru, chybové hlásenie alebo iná informácia.

- je to jednoduchý prenosový protokol
  - prenáša dáta v textovom tvare
  - používa transportné služby protokolu TCP
  - funguje bez stavovo
    - dialóg s klientom nemení stav servera
  - nadväzuje samostatné spojenie pre každý objekt v rámci WWW stránky
- komunikácia ma charakter „požiadavka-odpoveď“
    - klient iniciuje zavedenie spojenia
  - klient pošle svoju žiadosť
  - server pošle odpoveď
    - spojenie je ukončené
- odpovede majú číselný charakter
  - tak isto ako u FTP a SMTP
  - súčasť odpovede je i samotný obsah WWW stránky
- HTTP verzia 1.0 – každý objekt na stránke je sťahovaný samostatne
- HTTP verzia 1.1 – ak sú objekty na tom istom serveri, sú získavané spoločne

Druhy žiadostí HTTP [úprava]

Zvyčajne sa nazývajú metódy.

- **GET** Zďaleka najbežnejší typ žiadosti. Žiada o zdroj uvedením jeho URL
- **POST** Podobne ako GET, okrem toho, že je pridané telo správy zvyčajne obsahujúce dvojice kľúč-hodnota z HTML formulára.
- **PUT** Používa sa na upload súborov na špecifikované URI na webserveri.
- **DELETE** Zriedka implementované. Zmazanie zdroja.
- **HEAD** Podobné GET, okrem toho, že sa nepožaduje telo správy, iba hlavičky. Používa sa na získavanie metainformácií o dokumente.

- **TRACE** Odošle kópiu obdržanej požiadavky späť odosielateľovi, takže klient môže zistiť, čo na požiadavke menia alebo pridávajú servery, ktorými táto prechádza.
- **OPTIONS** Vracia HTTP metódy, ktoré daný webserver podporuje. Je možné použiť na otestovanie funkcionality servera.
- **CONNECT** Zriedka implementované, na použitie s proxy serverom, ktorý sa môže zmeniť na SSL tunel.

HTTP sa líši od iných na TCP založených protokolov ako napr. FTP v tom, že spojenia sa zvyčajne ukončia potom, ako sa dokončí vykonávanie požiadavky alebo série požiadaviek. Tento dizajn ho robí ideálnym protokolom pre web, kde stránky často odkazujú na ďalšie stránky na iných serveroch. Príležitostne to spôsobuje problémy webovým návrhárom, keďže chýbajúce perzistentné spojenie si vynucuje alternatívne prístupy udržiavania stavovej informácie o používateľovi. Zvyčajne na to používajú tzv. cookies.

HTTPS je zabezpečená verzia HTTP. Na ochranu dát používa SSL/TLS. Štandardný port služby je TCP port 443. HTTPS je vhodné aj v prípadoch, kedy je autentifikovaný len jeden koniec spojenia -- server. To je typický prípad pri HTTP transakciách cez internet.
Lokáciu dokumentov na webserveri udáva **Uniform Resource Locator** (URL). Táto adresa má syntax vyvinutú pre vytváranie odkazov na webstránky.

Príklad

Dolu je príklad konverzácie medzi HTTP klientom a HTTP serverom bežiacom na www.google.com, porte 80.
Klientská požiadavka:

```
GET / HTTP/1.1
Host: www.google.com
```

(nasledovaná znakom nového riadku, v tvare znaku carriage return nasledovaného znakom line feed.)
Adresa stroja je určená na rozlíšenie rôznych DNS názvov pre jedinú IP adresu. Kým v HTTP/1.0 bola táto hlavička nepovinná, HTTP/1.1 ju vyžaduje.
Odpoveď servera:

```
HTTP/1.1 200 OK
Content-Length: 3059
Server: GWS/2.0
Date: Sat, 11 Jan 2003 02:44:04 GMT
Content-Type: text/html
Cache-control: private
Set-Cookie:
PREF=ID=73d4aef52e57bae9:TM=1042253044:LM=1042253044:S=SMCc_HRPCQiqyX9j;
  expires=Sun, 17-Jan-2038 19:14:07 GMT; path=/; domain=.google.com
Connection: keep-alive
```

(nasledovaná prázdnym riadkom a zdrojovým textom HTML tvoriacim webstránku Google.)

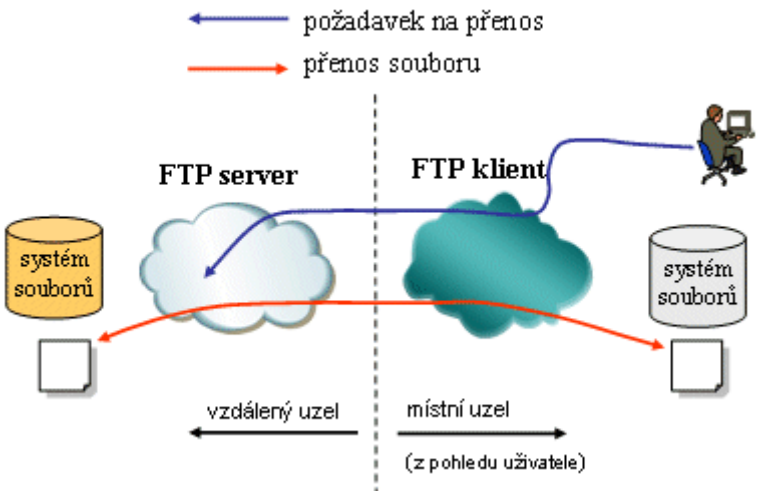
Perzistentnosť spojenia

Pri HTTP/1.0 klient pošle požiadavku serveru, server pošle odpoveď späť klientovi a následne sa spojenie ukončí. HTTP/1.1 však podporuje perzistentné spojenia. To umožňuje klientovi poslať požiadavku a dostať odpoveď a následne tým istým spojením posielať ďalšie požiadavky a prijímať ďalšie odpovede. Tým sa znižuje relatívna réžia TCP. Je tiež možné poslať viacero (zvyčajne dve) požiadavky pred obdržaním odpovede. Táto metóda sa nazýva „pipelining“.

- HTTP proxy

Prenos súborov FTP – *File Transfer Protocol*

Od počiatku internetu sa začali budovať archívy programových a dátových súborov. Prenos súborov z týchto archívov sa riadi protokolom FTP *(File Transfer Protocol*). FTP prenos súborov pracuje na klient – server architektúre. Príklad komunikácie podľa protokolu FTP je na obr. 7.5



Obr. 7.5 FTP služba aplikačnej vrstvy

Postup komunikácie prostredníctvom FTP je nasledovný.
Klient pošle požiadavku o prenos súborov. Túto požiadavku posiela klient cez riadiace spojenie a používa tri typy príkazov

- príkaz na riadenie prístupu *(Access control commands)* pre zadanie užívateľského mena a hesla
- príkaz na nastavenie parametrov prístupu *(Transfer parameter commands)* na nastavenie režimu prenosu
- výkonné príkazy *(FTP service commands)* pre definovanie typu operácie prenosu súborov *(upload, download, delete.)*

Server príjme požiadavku, spracuje ju a pomocou systému súborov odošle súbory cez dátové spojenie klientovi.
Príkazy majú textovú povahu a nadväzujú sa dva typy spojenia:

- riadiace – nadväzuje klient zo svojho portu 21, končí sa až explicitným príkazom
- dátové – nadväzuje server zo svojho portu 20 na port klienta, z ktorého bolo spojenie naviazané

Na prenos FTP súborov môžeme použiť www prehliadač, diskové manažér, špecializovaných FTP klientov. Počítače, na ktorých beží FTP server sa dajú rozdeliť na kategórie:

a) s anonymným prístupom - pri prístupe nám stačí vedieť názov anonymného konta. Ako heslo sa uvádza naša e-poštová adresa.
b) s neanonymným prístupom- musíme mať na počítači na ktorom beží FTP server, zariadené heslo. Pristupujeme naň pomocou používateľského mena a hesla.

Prenos súborov je transparentná služba, ktorá rozlišuje miestne a vzdialené súbory. Preto je potrebné poznať umiestnenie vzdialených súborov. So vzdialenými súbormi sa pracuje inak

ako s miestnymi. Pre presun súborov z miestneho umiestnenia na vzdialené je potrebné podnikať explicitné akcie príkazov typu GET, PUT ...
V TCP/IP najpoužívanejším protokolom pre prenos súborov je protokol FTP a TFTP(TrivialFTP), v RM OSI/ISO protokol FTAM *(File Transfer Access and Management,* ktorý realizuje ako prenos súborov, tak i ich zdieľanie.

Přenos souborů - FTP a TFTP

Pro přenos souborů je v rodině protokolů TCP/IP určen protokol FTP (File Transfer Protocol). Jeho koncepce je poměrně starého data (dokonce starší než samotné TCP/IP), a pamatuje ještě na některé skutečnosti, které jsou dnes již dosti „pasé" - například na rozdílné velikosti bytů na obou stranách přenosu. Přesto se ale protokol FTP s úspěchem používá dodnes, pro přenos celých souborů mezi dvěma uzlovými počítači sítě, například pro „stahování" souborů z nejrůznějších anonymních FTP archivů (které byly podle protokolu FTP dokonce pojmenovány).

Jednou z důležitých vlastností protokolu FTP je jeho povědomí o uživatelích, adresářích a přístupových právech: uživatel, který chce prostřednictvím protokolu FTP odněkud někam přenášet nějaké soubory, se musí vzdálené straně nejprve identifikovat (přihlásit se, pod určitým uživatelským jménem), a svou identitu prokázat (zadáním správného hesla). Vzdálená strana pak má podle čeho posuzovat oprávněnost požadavků na přístup ke konkrétním souborům. Při přenosu souborů prostřednictvím protokolu FTP je tedy možné realizovat nejrůznější přístupové strategie.

Obdobné vlastnosti naopak postrádá další protokol, který je v rodině protokolů TCP/IP určen také přenos souborů. Jde o protokol TFTP, neboli Trivial File Transfer Protocol. Jak již jeho název napovídá, jde o zjednodušenou obdobu protokolu FTP, ochuzenou právě o pojmy uživatele, přístupových práv, a dokonce i o pojem aktuálního adresáře. Chcete-li odněkud někam přenést soubor prostřednictvím protokolu TFTP, musíte vždy explicitně zadat úplnou přístupovou cestu k požadovanému souboru (a nelze například použít přístupovou cestu relativní, vztaženou k aktuálnímu adresáři). Oprávněnost vašeho požadavku navíc není podle čeho posuzovat (jelikož TFTP nezná pojem uživatele), a je proto ponecháno na konkrétní implementaci, jak se k němu druhá strana zachová. Většinou vám vyhoví kladně pouze v případě, kdy požadovaný soubor je běžně přístupný pro všechny uživatele. V praxi je protokol TFTP používán zejména bezdiskovými stanicemi k tomu, aby si z příslušného serveru „natáhly" svůj operační systém (ve formě tzv. bootovacího image

WAP

WAP bol definovaný organizáciou Wap Forum v roku 1998 ako ekvivalent k internetovým protokolom určený pre GSM siete. Jednotlivé protokoly zo štandardu WAP majú svoje ekvivalenty v TCP/IP sieťach a na nich postavených webových aplikáciách.

Multimédiá

VoIP –Voice over Internet Protocol

IP Telefónia

Bežný spôsob telefonovania pozná dôverne každý človek. Či už je to Vaša pevná linka alebo mobilný telefón, vždy sa jedná o prenos ľudského hlasu z jedného miesta na iné. Hlas zmenený na elektrický signál sa prenáša vzduchom alebo káblom.

IP telefónia využíva na prenos hlasu Voice over Internet Protocol (VoIP). Princíp nie je zložitejší, ako pri bežnom telefonovaní. Digitalizovaný hlas sa vo forme paketov prenáša po sieti Internet. Koncové zariadenie ľudský hlas konvertuje a komprimuje na dátové pakety a posiela po sieti ku adresátovi. Na konci dátovej cesty sa spätným procesom z paketov vyrobí pôvodná hlasová stopa. Veľkou výhodou komprimácie je šetrenie šírky pásma a nepomerne nižšie náklady na sieťové zariadenia. Tento pomer je bežne 1:10.

IP telefónia je technológia, ktorá dnes v mnohom prekonáva štandardný spôsob prenosu hlasu. Jednou z nesporných výhod tejto technológie je zníženie prevádzkových nákladov. Disponuje nástrojmi, ktoré bežná telefónna sieť nedokáže poskytnúť. Moderné zariadenia prinášajú úplne nové služby, typické len pre tento spôsob komunikácie (napr. pozdržaný fax, fax do mailu, odkaz do emailu). Všeobecným trendom je konvergencia dát, hlasu, obrazu a internetu na IP protokol. Cieľom je prenášať všetko po jednej sieti.

Pri telefonovaní cez VoIP sa používajú koncové zariadenia, IP telefóny, ktoré sa pripájajú priamo do lokálnej počítačovej siete. Odteraz už nie je nutné používať na prepojenie pobočkových ústrední klasické telefónne káble. Pri prepojení pobočiek WAN sieťou je pásmo optimálne využité. Veľkou výhodou je odbúranie paušálnych poplatkov prevádzkovateľovi verejnej telefónnej siete. IP telefónia je plne integrovateľná s telefonovaním v klasickej telefónnej sieti. Hovory, ktoré smerujú na čísla mimo IP siete, smeruje riadiaci server, alebo ústredňa, na klasické telefónne linky bez toho, aby používateľ postrehol prechod na bežný spôsob komunikácie.

IP Telefón

Pri použití vhodnej telefónnej ústredne je možné telefonovať cez VoIP aj z bežného telefónneho prístroja. Vyžaduje si to však istú réžiu a náklady naviac. Použitie IP telefónov je výhodnejšie.

Princíp

VoIP telefón – je prístroj ktorý mení Váš hlas na dáta, tieto veľmi rýchlo pošle cez internet do miesta, kde má niekto taký istý alebo podobný prístroj, ktorý tieto dáta zase zmení na hlas. Tak isto naopak od neho ku Vám. Na túto službu musíte mať zriadenú k Vášmu pripojeniu verejnú IP adresu

VoIP telefonovanie = Voice over Internet Protocol

- predstavuje alternatívnu hlasovú službu na prenos hovoreného slova prostredníctvom protokolu IP . V praxi môže byt použité VoIP kdekoľvek v prenosovej ceste hlasovej komunikácie.

V určitom prípade môže byť služba VoIP nielen elektronická komunikačná služba, ale aj verejne dostupná telefónna služba, prípadne dokonca univerzálna služba (US) v zmysle zákona o elektronických komunikáciách.

VoIP funguje inak ako tradičné telefónne siete

Na začiatku tradičného telefónneho hovoru sa vytvorí switch medzi účastníkmi spojenie. To umožní obom volajúcim spolu hovoriť, pričom switch spojenie ukončí, resp. uvoľní linku, len

čo jeden z nich položí. Cez linku sa teda prenáša jediný hovor, čo má za následok nevyužitie maximálnej kapacity, pretože počas komunikácie nastávajú stavy, keď jeden volajúci počúva, zatiaľ čo druhý účastník hovorí, a počas hovoru dochádza aj k odmlkám, resp. pauzám.

VoIP funguje na tzv. paketových switchoch – je to podobný proces ako posielanie mailov cez internet. Konverzácia je „rozdrobená“ do balíčkov (paketov) pozostávajúcich z jednotlivých fragmentov rozhovoru. Namiesto toho, aby bolo switchom vytvorené a blokované spojenie iba pre jeden telefonický rozhovor, fragmenty sú zasielané a prijímané podľa aktuálnej potreby, čo umožňuje využiť zvyšnú časť kapacity linky na prenos fragmentov iných rozhovorov, resp. ľubovoľných dátových prenosov. Hneď ako dorazia fragmenty k volanému na druhej strane linky, sú poskladané a prevedené opäť do zvukovej podoby.

SIP – Session Initiation Protocol

SIP je signalizačny protokol pre IP telefóniu

- riešenie pre IP telefóniu
- SIP je iba signalizačný protokol
    - rieši:
        - vytvorenie spojenia medzi dvoma účastníkmi
        - dohľad nad používaním tohto spojenia
        - rušenie spojenia
    - nerieši:
        - vlastný prenos dát
        - riadenie hovoru
- SIP možno použiť aj pre Instant Messaging a ďalšie služby
- je to jednoduchý textový protokol aplikačnej vrstvy
    - blízky protokolu HTTP
    - jeho filozofia je blízka WWW
    - je ho možno dobre integrovať s ďalšími protokolmi TCP/IP

- na SIP nadväzujú ďalšie protokoly, ktoré riešia riadenie hovoru:
    - SDP - Session Description Protocol

Architektúra SIP

- UA – User Agent
    - nachádza sa v každom SIP termináli alebo bráne
    - obsahuje:
        - UAC – User Agent Client
            - žiada o spojenie
        - UAS – User Agent Server
            - prijíma žiadosti o spojenia

- štýl komunikácie medzi UAC a UAS je veľmi podobný komunikácii WWW klienta a WWW serveru pomocou PHP
    - posielajú sa požiadavky formulované ako metódy

        - v textovej forme
        - spresnené hlavičkami
    - odpovede sú číselné
        - ako u FTP, SMTP a HTTP

SIP je primárne určený na zostavovanie a rušenie telefonických a videokonferenčných hovorov, ale dá sa použiť aj pre iné aplikácie požadujúce nadväzovanie spojenia analogické k telefonickému. To by sa mohlo zdať vcelku jednoduchým, v skutočnosti to obsahuje niekoľko problémov - môže ísť napríklad o konferenčný hovor, používateľ sa nemusí nachádzať na tom istom mieste, atď.
Na podporu služieb spojenia popisuje RFC 3261 pre SIP päť aspektov správy multimediálnych spojení:

- umiestnenie používateľa (User location) - určenie, s ktorým koncovým systémom sa komunikuje.
- dostupnosť používateľa (User availability) - určenie, či sa volaný účastník chce zúčastniť komunikácie alebo nie
- možnosti používateľa (User capabilities) - určene média a jeho parametrov, ktoré budú použité pri komunikácii
- zriadenie spojenia (Session setup) - "vyzváňanie", stanovenie parametrov spojenia na oboch jeho stranách
- správa spojenia (Session management) - zahŕňa prenos a ukončenie spojenia, zmenu parametrov spojenia a vyvolanie ďalších služieb

H.323
Je v současnosti implementován v několika Internetových real-timeových aplikacích, například NetMeeting nebo Ekiga, která využívá implementaci OpenH323. Je součástí rodiny protokolů H.32x. H.323 je běžně využíván při komunikaci pomocí VoIP (Internetová telefonie) a videokonferencích založených na IP. Jeho účel je tedy podobný účelu SIP.

RTSP

The sending of streaming data itself is **not** part of the RTSP protocol. Most RTSP servers use the standards-based RTP as the transport protocol for the actual audio/video data, acting somewhat as a metadata channel. The RTSP server from RealNetworks also features Real's proprietary RDT as the transport protocol.

Ďalšie protokoly

- **Virtual Terminal System** alebo prinajmenšom emulátory terminálov pre použitie veľkých počítačov. Všeobecné rozšírenie virtuálnych terminálov ako celkom neutrálnych prostriedkov dnes už úplne ustúpilo
- **Distributed Transaction Processing** umožňuje spolupôsobenie dvoch procesov na rôznych počítačoch. To je logicky veľmi progresívna koncepcia, ktorá môže byť realizovaná v prostredí Unixu alebo OS/2 aj s DOSom. Prvé dva menované systémy totiž obsahujú základné mechanizmy, ktoré túto koncepciu podporujú.
- **Job Transfer** slúži k tomu, aby sme spustili úlohu (job) na inom počítači a potom jej výsledok načítali späť. V prostredí počítačov PC sa využíva len zriedka.

- **Remote Database Access** (prístup do vzdialených databázových systémov) je zrejmí už svojím názvom. Problémom týchto systémov je nedostatočná medzinárodná štandardizácia, ktorá je skôr daná koncepciami jednotlivých výrobcov a prevádzkovateľov.

Organizácia sietí na základe vzťahu medzi počítačmi

Siete typu klient-server

Uzly v sieti klient vykonávajú dve rozdielne funkcie. "Obslužná stanica" *(server)* je vyhradená pre poskytovanie služieb, využívajú ostaté "pracovné stanice" *(workstation*). Správa celej siete spočíva buď v konfigurácii jednotlivých serverov alebo je celá správa centralizovaná do jedného bodu. To napomáha efektívnejšej správe sieťových prostriedkov, Siete typu klient-server môžu byť veľmi rozsiahle. Typickým príkladom klient – server komunikácie prenosu súborov. Jeden používateľ nahrá súbor na FTP server a potom mnoho používateľov ten súbor sťahuje, pričom nie je nutné, aby nahrávajúci a sťahujúci používateľ boli pripojení v rovnakom čase.

Vytvorenia takýchto sietí malo dva dôvody:

- dáta sa budú spracovávať tam, kde sa nachádzajú
- výstupy pre používateľa sa budú generovať tam, kde sa nachádza používateľ.

Aplikácia sa tak rozdelí na dve časti:

- serverová časť, ktorá zaisťuje spracovanie dát
- klientská časť, ktorá zaisťuje užívateľské rozhranie.

Pokiaľ sú klient a server správne vytvorené:

- môžu účinne minimalizovať objem prenášaných dát
- majú výrazne menšie prenosové nároky
- môžu pracovať i v prostredí rozľahlých sieťach
- klient- server môžu pracovať na rôznych platformách.

Komunikácia medzi klientom a serverom sa odohráva štýlom požiadavka/odpoveď a má nasledovné vlastnosti:

- server (pasívne čaká, kým dostane nejakú požiadavku
    - sám sa klientom nevnucuje
- komunikáciu iniciuje klient (browser, poštovný klient) zaslaním požiadavky
- musí byť definovaná vzájomná komunikácia
    - komunikačné protokoly: HTTP, SMTP, POP3, IMAP
- musí byť definovaný formát správ, ktoré si server a klient vymieňajú
    - napr.: HTML, RFC-822, MIME

Typy serverov používaných v sieťach klient server

- www server
- mailový server -
- súborový server - poskytuje diskový priestor
- server tlačiarne- umožňuje používanie tlačiarne pre viac pracovných staníc
- databázový server - poskytuje výpočtový výkon pre spracovanie databázových úloh
- komunikační server - zaisťuje prepojenie siete s ďalšími sieťami.

Zástupcovia technológií

- Novell NetWare- Novell

- Windows NT server- Microsoft
- LAN server- IBM
- Banyan VINEs- Banyan Incorporated

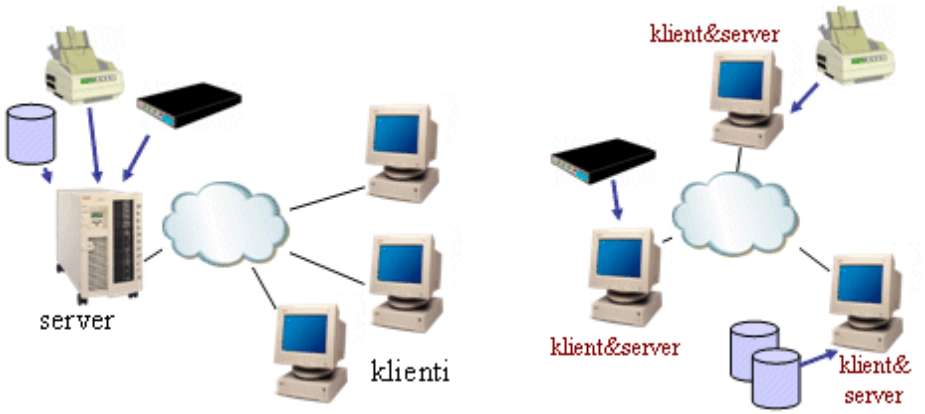
Peer-to-peer

Každý počítač v sieti peer-to- peer môže poskytovať služby ostatným počítačom v sieti. V takejto sieti nie je vyhradený žiadny hlavný počítač. Pojem peer-to-peer možno voľne preložiť ako "rovný s rovným". Čistá peer-to-peer (P2P) sieť neobsahuje ani klientov, ani servery, ale iba rovnocenné sieťové uzly, ktoré voči iným uzlom v sieti plnia súčasne úlohu servera aj klienta. Týmto sa peer to peer komunikácia odlišuje od modelu klient-server, kde komunikácia zvyčajne prebieha cez centrálny server.
Konfigurácia siete spočíva v izolovanom nastavení jednotlivých počítačov. Z toho vyplýva, že správa nie je centralizovaná. Pre prax to prináša menšiu efektivitu pri správe siete. Siete peer-to-peer sa budujú väčšinou v menšom rozsahu. Zriaďovacia cena je relatívne nízka.

Zástupcovia technológií

- Lantastic- Artisoft
- Windows for Workgroups- Microsoft
- Windows 95- Microsoft
- Windows NT Workstation- Microsoft
- Personal NetWare- Novell

Rozdiel medzi sieťami klient –server a peer to peer je na obr. 7.



Obr. 7. Sieť klient-server a peer to peer

Kľúčové slová

1. ***Aplikačná vrstva***
2. ***Aplikácia***
3. ***Aplikačný program***
4. ***Aplikačný proces***
5. ***Základná funkcia L7***
6. ***Application Service Elements***
7. ***CASE - Common Application Service Element***
8. ***SASE, Specific Application Service Element***
9. ***Podporné aplikačné služby***
10. ***Špecifické aplikačné služby***
11. ***DNS (Domain Name System)***
12. ***Koreňové DNS***
13. ***LDAP (Lightweight Directory Access Protocol***
14. ***X.500***
15. ***TELNET (Telecommunication Network)***
16. ***NFS RPC/XDR***
17. ***Elektronická pošta***
18. ***SMTP(Simple Mail Transfer Protocol)***
19. ***POP3 (Post Office Protocol v. 3)***
20. ***IMAP (Internet Message Access Protocol)***
21. ***WWW***
22. ***HTTP (Hypertext Transfer Protocol)***
23. ***HTTPS (HTTP secure)***
24. ***FTP (File Transfer Protokol)***
25. ***WAP (Wireless Application Protocol)***
26. ***Multimédiá***
27. ***VoIP (Voice over Internet Protocol)***
28. ***H.323***
29. ***RTSP (Real Time Streaming Protocol)***
30. ***URL (Uniform Resource Locator)***
31. ***Siete typu klient-server***
32. ***Siete typu peer to peer***

Kontrolné otázky:

1. Nad ktorou úrovňou je definovaná aplikačná vrstva OSI modeli?
2. Nad ktorou úrovňou pracuje aplikačná vrstva v TCP/IP architektúre?
3. Akej úrovni poskytuje aplikačná vrstva svoje služby?
4. Čo je základnou funkciou aplikačnej vrstvy?
5. Aké zariadenia sú používané na úrovni aplikačnej vrstvy?
6. Aké dátové jednotky sú používané na aplikačnej úrovni?
7. Komu sú určené služby aplikačnej úrovne?
8. Čo vyjadruje pojem aplikácia?
9. Aký je rozdiel medzi aplikáciou a aplikačným/používateľským programom?
10. Ktoré z uvedených príkladov sú aplikácie?
11. Ktoré z uvedených príkladov sú služby?
12. Čím je zabezpečená komunikácia s aplikáciami?
13. Aký je rozdiel medzi operačným systémom počítača a sieťovým operačným systémom?
14. Čo zabezpečujú Application Service Elements v aplikačnej vrstve?
15. Aké typy Application Service Elements sú špecifikované na aplikačnej vrstve?
16. Čo znamená označenie CASE - Common Application Service Element?
17. Čo znamená označenie SASE, Specific Application Service Element?
18. Aké skupiny služieb sú poskytované na aplikačnej úrovni?
19. Ktoré sú základné špecifické služby internetu?
20. Ktoré z vymenovaných protokolov sú využívané pre podporné služby aplikačnej vrstvy?
21. Pre aký účel je používaný DNS (*Domain Name System) ?*
22. Akú hierarchiu využíva DNS (*Domain Name System)* pri vytváraní domén?
23. Ako je označovaná najvyššia úroveň v DNS (*Domain Name System)?*
24. K akému účelu je používaný protokol Telnet?
25. Aký je vzťah medzi protokolom Telnet a protokolom SSH *(Secure Shell)?*
26. V čom sa odlišuje protokol Telnet od SSH *(Secure Shell)?*
27. V čom spočíva služba zdieľanie súborov (file sharing)?
28. Aký je rozdiel medzi službou zdieľania súborov a službou prenosu súborov?
29. V čo spočíva využitie protokolu
30. Ktoré z vymenovaných protokolov sú špecifikácie pre elektronickú poštu?
31. Aký je význam protokolu POP3 *(Post Office Protocol version)* v službe elektronickej pošty?
32. Aký je rozdiel protokolov IMAP a POP3?
33. Ktorý je základný protokol komunikácie v *World Wide Web?*
34. Aká je úloha protokolu HTTP (*Hypertext Transfer Protocol?*
35. Akú službu internetu podporuje protokol HTTP?
36. Aký je rozdiel medzi protokolom http a HTTPS?
37. Ktoré z vymenovaných protokolov patria k službe www?
38. Pre aký účel bol vytvorený WAP ***(Wireless Application Protocol)?***
39. Ktoré vymenované protokoly podporujú multimedia v internete?
40. K akému účelu slúži protokol VoIP (Voice over Internet Protocol)?
41. Aký je princíp prenosu hlasu v internete?
42. V čom je odlišnosť prenosu hlasu v internete a v tradičných telefónnych sieťach?
43. Akú službu internetu podporuje SIP *(Session Initiation Protocol)?*
44. Ktorý z vymenovaných protokolov podporuje videokonferencie v internete?
45. Aké je využitie RTSP *(Real Time Streaming Protocol)?*
46. Aký je rozdiel architektúr klieny – server a peer to peer?

47. Ktoré z vlastností patria sieti typu klient – server?
48. Ktoré vlastnosti patria sieti typu peer to peer?