Protokoly aplikační vrstvy TCP/IP – přehled; DNS – domény, překlady IP adres, funkčnost DNS serverů a klienta, součinnost

Protokoly aplikační vrstvy TCP/IP

DHCP

Dynamické přidělování síťových informací (např. výchozí brány, masky sítě, IP adresy) DHCP serverem klientovi. Platnost některých údajů (zejména přidělené/zapůjčené IP adresy) je omezená (*lease time*), proto v klientském zařízení běží DHCP klient, který platnost údajů prodlužuje. Klient komunikuje na UDP portu 68, server naslouchá na UDP portu 67.

Po připojení do sítě klient vyšle broadcastem paket DHCPDISCOVER, na který odpoví DHCP server paketem DHCPOFFER s nabídkou IP adresy (nebo více adres, z nichž si jednu klient vybere). O konkrétní IP klient požádá paketem DHCPREQUEST, server odpovídá paketem DHCPACK – od tohoto momentu může klient IP adresu a další nastavení používat. Pokud lhůta zapůjčení uplyne, aniž by bylo požádáno o novou IP (nebo kdyby server nepotvrdil přidělení IP klientovi), musí klient takovou adresu přestat používat.

FTP (file transfer protocol)

Platformě nezávislý protokol podporovaný webovými prohlížeči a specializovanými programy, tzv. FTP klienty. Jde o jeden z nejstarších protokolů, využívá porty TCP/21 a TCP/20. Port 21 slouží k řízení a jsou jím také přenášeny příkazy FTP, port 20 pak slouží k vlastnímu přenosu dat.

Přenos může být binární nebo ascii (textový). Při textovém jsou (v případě, že spolu komunikují různé systémy) konvertovány konce řádků (CR/LF na LF nebo obráceně). Při binárním přenosu není do dat nijak zasahováno. V současné době není protokol již považován za bezpečný, proto pro něj byla definována jistá rozšíření. Je nahrazován protokolem FTPS nebo SFTP.

HTTP (hypertext transfer protocol)

Protokol určený pro výměnu hypertextových dokumentů (zejména ve formátu HTML). Obvykle používá port TCP/80. Společně s elektronickou poštou je http nejvíce používaným protokolem. V současné době je používán i pro přenos dalších informací (díky MIME rozšíření umí přenášet jakýkoliv soubor – podobně jako e-mail).

HTTP používá (jako některé další aplikace) tzv. jednotný lokátor prostředků (URL, Uniform Resource Locator), který specifikuje jednoznačné umístění nějakého zdroje v Internetu. Samotný protokol HTTL neumožňuje šifrování ani zabezpečení integrity dat, pro zabezpečení http se často používá TLS spojení nad TCP, takové použití protokolu je označování jako HTTPS.

Protokol funguje způsobem dotaz-odpověď. Uživatel pošle (obvykle specializovaným protokolem jako je např. webový prohlížeč) serveru dotaz ve formě čistého textu obsahujícího označení požadovaného dokumentu, informace o schopnostech prohlížeče apod., server poté odpoví

pomocí několika řádků textu popisujících výsledek dotazu (zda se dokument podařilo najít, jakého je typu atd.), za kterými následují data samotného požadovaného dokumentu.

Pokud uživatel bude mít po chvíli další dotaz na stejný server, bude se jednat o další, nezávislý dotaz a odpověď. Z hlediska serveru nelze poznat, jestli tento druhý dotaz jakkoli souvisí s předchozím. Kvůli této vlastnosti se http protokolu říká *bezestavový protokol*[1]. K uchovávání stavů slouží rozšíření HTTP cookies, které serveru uchovávání informací o stavu spojení umožňují.

IMAP (Internet Message Access Protocol)

Protokol pro vzdálený přístup k e-mailové schránce. IMAP nabízí oproti jednodušší alternativě POP3 pokročilé možnost vzdálené správy (práce se složkami, přesouvání zpráv mezi nimi, vyhledávání na straně serveru apod.) a práci v tzv. online i offline režimu. V současné době se používá protokol verze IMAP4. Komunikace probíhá na portu TCP/147, výjimečně 993[2].

Umožňuje trvalé (online) připojení ke schránce díky čemuž je možné s celou poštovní schránkou plně pracovat z libovolného místa. Všechny zprávy a složky jsou uloženy na poštovním serveru a na počítač se stahují jen nezbytné informace (při zobrazování složek např. jen záhlaví zpráv, obsah se stáhne až v případě, že chce uživatel zprávu přečíst). Protokol umožňuje současné připojení více klientů zároveň.

NFS (Network File System)

Síťový systém souborů umožňující transparentní sdílení vzdálených souborů jako by byly lokální – prostřednictvím NFS klienta je možné připojit disk ze vzdáleného serveru a pracovat s ním jako s lokálním. V prostředí Linuxu se jedná asi o nejpoužívanější protokol pro tyto účely.

POP (Post Office Protocol)

Protokol pro stahování e-mailů z poštovního serveru na klienta. Ze vzdáleného serveru se stáhnout všechny zprávy včetně těch, které uživatel případně číst nechce nebo spam (pokud není filtrován při přijetí serverem). Byť většina POP serverů umožňuje stáhnout i pouze hlavičky zpráv, chybí podpora v klientech. Tuto nevýhodu může odstranit protokol IMAP, který se zprávami pracuje přímo na serveru. Komunikuje na portu TCP/110. Aktuálně využívaná verze je POP3.

SMTP

Protokol určený pro přenos zpráv elektronické pošty prostřednictvím přepravců elektronické pošty (MTA, Mail Transfer Agent)[3]. Protokol zajišťuje doručení pošty pomocí přímého spojení mezi odesílatelem a adresátem. Zpráva je doručena do poštovní schránky adresáta, ke kterém potom uživatel může kdykoli přistupovat („vybírat zprávy“) pomocí protokolů POP nebo IMAP.

Jedná se o jednu z nejstarších aplikací. SMTP používá pro svoji činnost port TCP/25 (komunikace mezi poštovními servery) a port TCP/587 (příjem e-mailů od e-mailových klientů).

Není-li z důvodu dočasné chyby (např. je cílový server zaneprázdněn, nekomunikuje nebo není dostupný – ale existuje) možné e-mail doručit, bývá uložen do fronty – zpravidla na několik dní –

[1] bezestavový protokol – protokol neumí uchovávat stav komunikace, dotazy spolu nemají souvislost
[2] používá se pro vytvoření zabezpečeného SSL tunelu
[3] MTA běží samostatně na pozadí bez přímého řízení uživatelem na serverech (poštovních uzlech); nejznámější MTA jsou Postfix, Sendmail nebo Microsoft Exchange Server

a jsou činěny opakované pokusy o doručení (typicky po několika málo desítkách minut). Pokud pokusy o doručení jsou po určitou dobu neúspěšné, pošle se odesílateli zpráva o nedoručitelnosti a e-mail je zahozen.

Telnet

Protokol umožňující připojení ke vzdálenému počítači pomocí textového uživatelského rozhraní. Protože komunikace není šifrována, je nahrazován protokolem SSH. Telnet je možné použít pro ruční komunikaci protokoly jako je SMTP, HTTP apod. Serverová část standardně naslouchá na portu TCP/23.

SSH

Protokol navržený (a využívaný) jako náhrada za Telnet, který posílal heslo v nezabezpečené formě, čímž bylo možné jeho odposlechnutí a následné zneužití.

Umožňuje bezpečnou komunikaci mezi dvěma počítači, která se využívá pro zprostředkování přístupu k příkazovému řádku, kopírování souborů a též jakýkoliv obecný přenos dat. Zajišťuje integritu dat a volitelnou bezeztrátovou kompresi. Server standardně naslouchá na portu TCP/22.

DNS (Domain Name System)

Protokol pro výměnu informací mezi DNS servery, které DNS (hierarchický systém doménových jmen) jako takový realizují. **Hlavním úkolem DNS je převod doménových jmen a IP adres.** Později přibral další funkce (např. pro elektronickou poštu) a slouží de facto jako *distribuovaná databáze síťových informací*. Systém je distribuovaný, avšak jednotlivé části jsou spravovány lokálně.

Celé DNS je založeno na principu client-server (server má databázi jmen a dalších informací, klient (resolver) vznáší dotaz k lokálnímu serveru – buď získá odpověď (lokální server ji zná), nebo klient získá odkaz na jiný server, který je blíže k řešení dotazu (lokální server tedy odpověď nemá a musí se zeptat znovu – serveru, jehož adresu obdržel).

Protokol používá porty TCP/53 i UDP/53. Servery DNS jsou organizovány hierarchicky, stejně jako jsou hierarchicky tvořeny názvy domén. Jména domén umožňují lepší orientaci lidem, adresy pro stroje jsou však vyjádřeny pomocí adres 32bitových (IPv4, A záznam) nebo 128bitových (IPv6, AAAA záznam). Systém DNS umožňuje efektivně udržovat decentralizované databáze doménových jmen a jejich překlad na IP adresy. Stejně tak zajišťuje zpětný překlad IP adresy na doménové jméno PTR záznam (*reverzní záznam*).

Pro ověření stavu DNS dříve sloužil nástroj NSlookup, který je již však zastaralý.

Kořenové servery (root servery)

V DNS je 13 kořenových (root) serverů představujících zásadní část technické infrastruktury Internetu, na které závisí spolehlivost, správnost a bezpečnost operací na Internetu. Tyto servery poskytují *kořenový zónový soubor* ostatním DNS serverům. Kořenový zónový soubor popisuje, kde se nacházejí autoritativní servery pro domény nejvyšší úrovně. Tento kořenový zónový soubor je relativně malý a často se nemění – operátoři root serverů ho pouze zpřístupňují, samotný soubor je vytvářen a měněn organizací IANA. Root servery se nacházejí ve 34 zemích světa, na více než 80 místech. Jsou spravovány organizacemi, které vybírá IANA.

Doména

Část jména počítače (jména počítačů jsou složena z částí, které se nazývají domény). Domény jsou uspořádány do stromu, kořenem je fiktivní (neexistující) doména označovaná tečkou (.), tzv. fixní doména. Jejími bezprostředními potomky jsou domény prvního řádu (tematické/generické – gTLD a geografické/národní – ccTLD).

Členění uvnitř domény určují její správci. – každá doména má svého správce (a server určující situaci na doméně). Jednotlivé části (subdomény) mohou mít až 63 znaků a celkově může celé doménové jméno mít až 255 znaků, doména tedy může mít až 127 úrovní. Doménové jméno = doménová adresa = IP adresa „v textovém tvaru". Jednotlivé části jsou odděleny tečkami a seřazeny od nejkonkrétnějšího počítače k nejobecnějšímu. K jedné IP adrese může existovat několik doménových jmen.

Servery se dělí na několik úrovní:

a) **primární server** – určuje obsah domény (soubory, které tam správce umístí, případně je mění, udržováno ručně); pro každou doménu existuje právě jeden primární server, jeho odpovědi jsou brány za správné, takováto odpověď se nazývá *autoritativní*
b) **sekundární server** – slouží jako záloha primárního – nemá právo měnit obsah domény, v podstatě jen v pravidelných intervalech kontroluje stav serveru primárního a pokud nalezne novější data, zkopíruje si je; pro každou doménu musí existovat sekundární server, jeho odpovědi se také považují za autoritativní
c) **pomocný server** – *caching only* – poskytuje neautoritativní odpovědi; činnost spočívá v tom, že si pamatuje dotazy a odpovědi, které přes něj prošly a jestliže se v zápětí vyskytne stejný dotaz, server rovnou posílá odpověď, avšak bez záruky; tuto činnost vykonává každý server bez ohledu, je-li primárním či sekundárním a pro které domény – server je zároveň pomocným serverem pro všechny ostatní domény

Řešení dotazu na DNS server

Koncový počítač pokládá dotaz, v síťové konfiguraci má uloženu adresu lokálního DNS serveru (pokud počítač hledá informaci, obrací se právě na tento lokální server). Každý DNS server má ve své konfiguraci uvedeny IP adresy kořenových serverů. Kořenové servery mají autoritativní informace o kořenové doméně – znají domény nejvyššího řádu a jejich autoritativní servery.

Příklad (hledání IP adresy k doménovému jménu www.wikipedia.org)

1. resolver v PC – program zajišťující překlad – se obrátí na lokální DNS sever s dotazem, jaká je IP adresa k doménovému jménu www.wikipedia.org
2. lokální server odpověď nezná, ale ví, že existuje doména nejvyššího řádu (.org) a ví, jaké jsou její autoritativní servery – nazpět tedy poskytne jejich adresy
3. PC jeden ze serverů vybere a pošle mu znovu dotaz na doménu www.wikipedia.org
4. server ji opět nezná, ale poskytne nazpět IP adresy autoritativních serverů pro doménu wikipedia.org
5. PC z přijatých odpovědí opět jednu vybere a zeptá se znovu na celou doménu
6. server odpověď zná, je vrácena IP adresa domény www.wikipedia.org

Pokud některý z oslovených serverů ve své vyrovnávací paměti odpověď má, odpoví rovnou – taková odpověď je *neautoritativní*.

Rekurzivní a nerekurzivní řešení dotazu

Rekurzivní – server se chopí vyřízení dotazu, najde odpověď a pošle ji tazateli; pokud server dotaz řeší, ukládá si ho potom do své cache (takto se vždy chová lokální server)

Nerekurzivní – server dotaz neřeší, pouze poskytne adresy dalších serverů (takto se vždy chová kořenový server nebo autoritativní server)

Reverzní dotazy

DNS umí převádět také IP adresu na doménové jméno. Při vkládání dat pro zpětné dotazy je však třeba vyřešit problém s opačným uspořádáním IP adresy a doménového jména (IP má na začátku obecné informace – adresu sítě – které se směrem doprava zpřesňují až k adrese PC; doménové jméno má pořadí přesně opačné). Instituce připojená k internetu má typicky přidělen začátek svých IP adres a konec svých doménových jmen.

Tento nesoulad řeší DNS tak, že při reverzních dotazech obrací pořadí bytů v adrese a k obrácené adrese připojí doménu *in-addr.arpa*. Výsledné „jméno" pak vyhledává standardním postupem. Je-li např. hledáno jméno k IP adrese 145.97.39.155, je vytvořen dotaz na 155.39.97.145.in-addr.arpa.

Na data pouze z reverzních domén se nelze zcela spoléhat, do reverzní domény se v principu dají zapsat libovolná jména. Pokud záleží na spolehlivosti údaje z reverzní domény, je údaj ověřen normálním dotazem (pokud reverzní záznam o IP 145.97.39.155 prohlásí, že jde o *www.seznam.cz*, vytvoří se normální dotaz na www.seznam.cz. Pokud odpovědí bude původní IP adresa, jsou data důvěryhodná (správce klasické i reverzní domény tvrdí totiž totéž). Pokud se však liší, znamená to, že data v reverzní doméně jsou nekorektní.

Nastavení serveru

Pro nastavení DNS serveru se používají zónové soubory – obsah zóny (domény nebo několika domén) je uložen v zónovém souboru, soubor tedy slouží pro uložení obsahu určité zóny.

V souboru jsou uloženy tzv. *zdrojové záznamy* (doménové jméno, životnost – jak dlouho bude záznam platit, třída – k jakým protokolům se záznam vztahuje a typ záznamu). Některé typy záznamů:

- **SOA** – zahajující záznam zónového souboru, obsahuje jméno primárního serveru a adresu elektronické pošty jejího správce
- **A** – IPv4 adresa přiřazená danému jménu
- **AAAA** – IPv6 adresa přiřazená danému jménu
- **CAA** – novější typ záznamu oznamující, která certifikační autorita může pro danou doménu vystavit https certifikát
- **CNAME** – alias – jiné jméno pro jméno již zavedené – pokud má např. adresa ww.abc.com sloužit stejně jako www.abc.com, vytvoří se patřičný CNAME záznam
- **MX** – adresa a priorita serveru pro příjem elektronické pošty pro danou doménu
- **NS** – ohlašuje jméno autoritativního DNS serveru pro danou doménu, resp. subdoménu, např. pokud má subdoména sub.abc.com mít DNS server ns.abc.com a příp. sekundární server ns.def.com, bude toto patřičně v NS záznamu uvedeno
- **TXT** – prostý textový záznam, používá se např. pro ověřování vlastnictví domény či jiné specifické účely