

Balík internetových protokolov

z Wikipédie, slobodnej encyklopédie

Balík internetových protokolov (**Internet protocol suite**) je súbor komunikačných protokolov implementujúcich tzv. protocol stack, na ktorých je postavený systém Internet. Niekedy sa nazýva súbor **TCP/IP** protokolov podľa dvoch najdôležitejších protokolov, ktoré obsahuje: Transmission Control Protocol (TCP) a Internet Protocol (IP), ktoré boli zároveň aj prvé definované.

Balík internetových protokolov je možné opísať analógiou s OSI modelom. Ten opisuje vrstvy protocol stacku, ale nie všetky zodpovedajú internetovej praxi. V protocol stacku rieši každá vrstva množinu problémov spojených s prenosom dát a poskytuje dobre definovanú službu pre vyššie vrstvy. Čím je vrstva vyššia, tým je logicky bližšie používateľovi a zaoberá sa abstraktnejšou množinou dát, pričom sa spolieha na nižšie vrstvy, aby preložili dáta do formy, s ktorou je možné v skutočnosti fyzicky manipulovať.

Internetový model vznikol ako riešenie praktického inžinierskeho problému. Na druhej strane OSI model je výsledkom teoretického prístupu a vznikol tiež v skoršej fáze evolúcie počítačových sietí. Preto je jednoduchšie porozumieť OSI modelu, ale TCP/IP model je v skutočnosti aplikovaný. Je užitočné poznať OSI model pred začiatkom štúdia TCP/IP, keďže platia rovnaké princípy, ale je jednoduchšie pochopiť ich v OSI modeli.

Balík internetových protokolov

Aplikačná vrstva

HTTP · HTTPS · FTP · SSH ·
IMAP · SMTP · NNTP · IRC ·
SNMP · SIP · RTP · NFS a iné

Transportná vrstva

TCP, UDP, SCTP, DCCP a iné

Sieťová vrstva

IPv4, IPv6, ARP a iné

Linková vrstva

Ethernet, Wi-Fi, Token ring, FDDI
a iné

Fyzická vrstva

RS-232, EIA-422, RS-449, EIA-485
a iné

Obsah

- 1 Vrstvy v TCP/IP stacku
 - 1.1 Fyzická vrstva
 - 1.2 Linková vrstva
 - 1.3 Sieťová vrstva
 - 1.4 Transportná vrstva
 - 1.5 Aplikačná vrstva
- 2 Implementácie
- 3 Pozri aj

Vrstvy v TCP/IP stacku

Existuje diskusia o tom, ako mapovať TCP/IP na OSI model. Keďže balíky protokolov TCP/IP a OSI sa presne nezhodujú, neexistuje jediná správna odpoveď.

Navyše OSI model neopisuje dostatočne bohato spodné vrstvy na to, aby vedel opísať skutočné vrstvenie TCP/IP; musí sa pridať vrstva navyše (internetworking layer, medzisieťová) medzi transportnú a sieťovú vrstvu. Protokoly špecifické pre konkrétny typ siete ale bežiacie nad základným hardvérom by mali byť na sieťovej vrstve. Príkladom takých protokolov je ARP a Spanning Tree Protocol (používaný na kontrolu nečinnosti bridgeov zatiaľ, čo sú nečinné). Toto však nie sú lokálne protokoly a patria do funkcionality internetworking vrstvy. Priznávajúc, že umiestnenie oboch skupín do rovnakej vrstvy môže byť mátuce, treba povedať, že OSI model nie je dostatočne komplexný na to, aby to zvládol, nehovoriac o protokoloch, ktoré sú logicky súčasťou internetworking vrstvy, ako ICMP.

Nasledujúci diagram sa pokúša zobrazit', kam by patrili TCP/IP a iné protokoly v pôvodnom OSI modeli:

7	aplikačná	napr. HTTP, SMTP, SNMP, FTP, Telnet, SSH a Scp, NFS, RTSP
6	prezentačná	napr. XDR, ASN.1, SMB, AFP
5	relačná	napr. TLS, SSH, ISO 8327 / CCITT X.225, RPC, NetBIOS, ASP
4	transportná	napr. TCP, UDP, RTP, SCTP, SPX, ATP
3	sieťová	napr. IP, ICMP, IGMP, X.25, CLNP, ARP, RARP, BGP, OSPF, RIP, IPX, DDP
2	linková	napr. Ethernet, Token ring, PPP, HDLC, Frame relay, ISDN, ATM, 802.11 WiFi, FDDI
1	fyzická	napr. elektrina, rádio, laser

Bežne sa v rámci balíka TCP/IP vrchné tri vrstvy OSI modelu (aplikačná, prezentačná a relačná) považujú za jedinú aplikačnú vrstvu. Pretože balík TCP/IP nemá zjednotenú relačnú vrstvu, tieto funkcie zvyčajne vykonávajú (alebo ignorujú) jednotlivé aplikácie. Najvýznamnejší rozdiel medzi modelmi TCP/IP a OSI je aplikačná vrstva, keďže TCP/IP do nej integruje niekoľko vrstiev OSI modelu. Dolu je zobrazená zjednodušená reprezentácia TCP/IP stacku:

	aplikačná "layer 7"	napr. HTTP, FTP, DNS <i>(smerovacie protokoly ako BGP a RIP, ktoré z rôznych dôvodov bežia nad TCP, resp. UDP, môžu byť považované za súčasť sieťovej vrstvy)</i>
4	transportná	napr. TCP, UDP, RTP, SCTP <i>(smerovacie protokoly ako OSPF, ktoré bežia IP, môžu byť považované za súčasť sieťovej vrstvy)</i>
3	sieťová	Pre TCP/IP je toto Internet Protocol (IP) <i>(povinné protokoly ako ICMP a IGMP bežia nad IP, ale stále môžu byť považované za súčasť sieťovej vrstvy; ARP nebeží nad IP)</i>
2	linková	napr. Ethernet, Token ring, atď.
1	fyzická	napr. fyzické médium a kódovacie techniky, T1, E1

Fyzická vrstva

Fyzická vrstva charakterizuje komunikáciu po fyzickej stránke—konvencie o používanom médiu (drôty, optické vlákno, rádiové spojenie) a všetky súvisiace podrobnosti ako konektory, kódy kanálov a modulácia, sila signálu, vlnová dĺžka, nízkoúrovňová synchronizácia a časovanie, maximálne

vzdialenosti. Balík internetových protokolov nepokrýva fyzickú vrstvu žiadnej siete, detaily o špecifických technológiách fyzickej vrstvy nájdete v ich článkoch.

Linková vrstva

Linková vrstva alebo spojová vrstva špecifikuje spôsob prenosu paketov fyzickou vrstvou, vrátane *rámcovania* (t. j. špeciálne bitové vzory označujúce začiatok a koniec paketu). Napríklad Ethernet má polia v hlavičke paketu, ktoré špecifikujú pre ktorý stroj alebo stroje v sieti sú pakety určené. Príkladom protokolov linkovej vrstvy sú Ethernet, Wireless Ethernet, SLIP, Token Ring a ATM.

PPP je o niečo zložitejší, keďže bol pôvodne špecifikovaný ako oddelený protokol bežiaci na vrchu iného protokolu linkovej vrstvy -- HDLC/SDLC.

Táto vrstva sa niekedy rozdeľuje ešte na Logical Link Control (riadenie logického spojenia) a Media Access Control (riadenie prístupu k médiu).

Sieťová vrstva

Sieťová vrstva podľa pôvodnej definície riešila problém transportu paketov v rámci jednej siete. Príkladmi takých protokolov sú X.25 a protokol ARPANETu Host/IMP Protocol.

S príchodom konceptu spájania sietí bola pridaná ďalšia funkcionálna, menovite transport dát z jednej siete do druhej. Sem vo všeobecnosti patrí smerovanie paketu sieťou sietí, známou ako internet.

V balíku internetových protokolov sa o úlohy prenosu paketov zo zdroja do cieľa stará IP. IP je schopný niesť dáta množstva rozličných vysokoúrovňových protokolov; tieto protokoly sú definované jedinečným číslom *IP Protocol Number*. Napr. ICMP a IGMP majú čísla protokolu 1 a 2.

Niektoré protokoly prenášané pomocou IP ako ICMP (používaný na diagnostiku IP prenosu) a IGMP (používaný na správu multicast dát) sú navrstvené nad IP, ale vykonávajú funkcie sieťovej vrstvy, čo ilustruje nekompatibilitu medzi internetovým a OSI modelom. Všetky smerovacie protokoly ako BGP, OSPF a RIP sú vlastne súčasťou sieťovej vrstvy, hoci sa môže zdať, že patria do vyššej vrstvy.

Transportná vrstva

Protokoly transportnej vrstvy riešia problémy ako spoľahlivosť („dorazili dáta do cieľa?“) a zabezpečujú, že dáta prídu v správnom poradí. V balíku protokolov TCP/IP tiež určujú, na akú aplikáciu sú dáta určené.

Protokoly dynamického smerovania, ktoré technicky patria do tejto vrstvy (keďže bežia nad IP) sa vo všeobecnosti považujú za súčasť sieťovej vrstvy; príkladom je OSPF (číslo IP protokolu 89).

TCP (číslo IP protokolu 6) je „spoľahlivý“, spojovo orientovaný transportný mechanizmus poskytujúci spoľahlivý dátový tok, ktorý zabezpečuje, že dáta budú prenesené úplné, nepoškodené a v správnom poradí. TCP sa neustále pokúša merať zaťaženie siete a reguluje rýchlosť odosielania s cieľom vyhnúť sa preťaženiu siete. Toto sú jeho hlavné odlišnosti od UDP a v reálnych streamovacích aplikáciách alebo smerovacích aplikáciách s veľkou stratou informácií pri prenose medzi sieťami sa môžu stať nevýhodou.

Novší SCTP je tiež „spoľahlivý“, spojovo orientovaný transportný mechanizmus. Je orientovaný skôr na záznamy ako na bajty a poskytuje viacero podtokov (substreams) multiplexovaných jedným spojením. Tiež poskytuje podporu multi-homing, kedy je zdroj reprezentovaný viacerými IP adresami

(reprezentujúcimi viaceré fyzické rozhrania), takže keď je jedno z nich neschopné spojenia, spojenie sa nepreruší. Pôvodne bol vyvinutý pre telefónne aplikácie (na prenos SS7 cez IP), ale je ho možné použiť aj inde.

UDP (číslo IP protokolu 17) je nespojový datagramový protokol. Označuje sa ako „nespoľahlivý“ alebo „best effort“ protokol – nie že by bol obzvlášť nespoľahlivý, ale preto, že neoveruje, či pakety prišli do cieľa a neposkytuje záruku, že prídu v poradí. Ak aplikácia tieto záruky požaduje, musí si ich zabezpečiť sama, alebo použiť spojový protokol ako TCP.

UDP sa typicky používa v aplikáciách ako streamovanie multimédií (audio, video atď.), kde je dôležitejšie včasné doručenie ako spoľahlivosť, alebo pre jednoduché aplikácie založené na otázke/odpovedi ako vyhľadávania DNS, kde by predstavovalo nadviazanie spoľahlivého spojenia neúmerne vysoké náklady.

DCCP je v súčasnosti vo fáze vývoja v IETF poskytuje sémantiku riadenia TCP toku, kým si ponecháva z pohľadu používateľa model UDP datagramovej služby.

Množstvo aplikácií vyšších úrovní používa TCP a UDP. Tieto aplikácie sa na jednotlivých sieťových adresách rozlišujú číslom TCP alebo UDP portu. Podľa dohody sú všetkým *známym portom* priradené špecifické aplikácie.

RTP je datagramový protokol určený na prenos dát v reálnom čase, ako audio a video. Hoci RTP používa ako základ UDP formát paketov, poskytuje funkciu, ktorá je na tej istej protokolovej úrovni.

Aplikačná vrstva

Aplikačná vrstva je vrstva bežne používaná väčšinou programov pracujúcich so sieťou na komunikáciu prostredníctvom siete. Procesy na tejto vrstve závisia na konkrétnej aplikácii; dáta prenášané programom v jeho internom formáte sú kódované do štandardného protokolu.

Niektoré programy bežiacie na tejto vrstve poskytujú služby, ktoré priamo podporujú používateľské aplikácie, sem patria programy a ich špecifické protokoly ako HTTP (World Wide Web), FTP (prenos súborov), SMTP (e-mail), SSH (zabezpečené vzdialené prihlasovanie), DNS (vyhľadávania hostname/IP adresy) a mnohé iné.

Po zakódovaní aplikačných dát do protokolu aplikačnej vrstvy sa podajú ďalej nižšej vrstve TCP/IP stacku.

Na transportnej vrstve aplikácie najčastejšie využívajú služby TCP a UDP asociované s číslami známych portov, patria sem napríklad:

- QOTD na porte 17
- File Transfer Protocol (FTP) na porte 21
- Secure Shell (SSH) na porte 22
- Telnet na porte 23
- Simple Mail Transport Protocol (SMTP) for outgoing e-mail na porte 25
- Domain Name System (DNS) lookups on UDP (or sometimes TCP) port 53
- Dynamic Host Configuration Protocol (DHCP) na portoch 67 a 68
- Gopher na porte 70
- Finger na porte 79
- HTTP na TCP porte 80
- POP3 správa emailovej schránky na porte 110
- Network News Transfer Protocol (NNTP) na porte 119

- Network Time Protocol (NTP) na porte 123
- NetBIOS na porte 139
- IMAP správa emailovej schránky na porte 143
- Simple Network Management Protocol (SNMP) na porte 161
- XDMCP na porte 177
- HTTPS zabezpečené HTTP na porte 443
- Routing Information Protocol (RIP) smerovacie aktualizácie na UDP porte 520
- RTSP na porte 554
- IMAPS na porte 993
- Universal Plug and Play (UPnP) na porte 5000
- IRC na porte 6667

Tieto porty pôvodne priradila Internet Assigned Numbers Authority (IANA).

Je možné voľne pridávať do tohto zoznamu: POPS.

Implementácie

- KA9Q

Pozri aj

- Protokol
- Zoznam známych portov
- OSI Model

Zdroj: „https://sk.wikipedia.org/w/index.php?title=Balík_internetov%C3%BDch_protokolov&oldid=6116111“

Kategória: Internetové protokoly

-
- Čas poslednej úpravy tejto stránky je 21:47, 5. september 2015.
 - Text je dostupný za podmienok Creative Commons Attribution/Share-Alike License 3.0 Unported; prípadne za ďalších podmienok. Podrobnejšie informácie nájdete na stránke Podmienky použitia.