TCP/IP

(Transmission Control Protokol/Internet Protocol)

Obsah :

- Vrstvova architektura TCP/IP
- Protokoly jednotlivých vrstiev
- Transmission Control Protocol (TCP)
- Internet protokol (IP)
- MAC adresa
- Protokoly

V súčasnosti „najpopulárnejší“ komunikačný protokol, resp. sada (skupina) protokolov. Je univerzálnym pre všetky podstatné operačné systémy (Windows, Novell, Unix, Linux), plne smerovateľný jednoducho inštalovateľný ale množstvo nastaviteľných parametrov ho robia nielen široko použiteľným ale aj pomerne náročne konfigurovateľným.

TCP/IP potrebuje k svojej činnosti ešte protokoly na nižších vrstvách o ktorých sa dočítate nižšie. Pri určení TCP/IP nešpecifikuje konkrétne prenosové technológie, používa momentálne dostupné riešenia na úrovni sieťového rozhrania napr. Ethernet, ATP a pod.

Vrstvova architektura TCP/IP :

Prístupová vrstva - je najnizsia vrstva a ako taká, jediná je viazaná na technické prostriedky siete. Zabezpečuje bezkonfliktný obojstranný styk so sieťovým médiom.

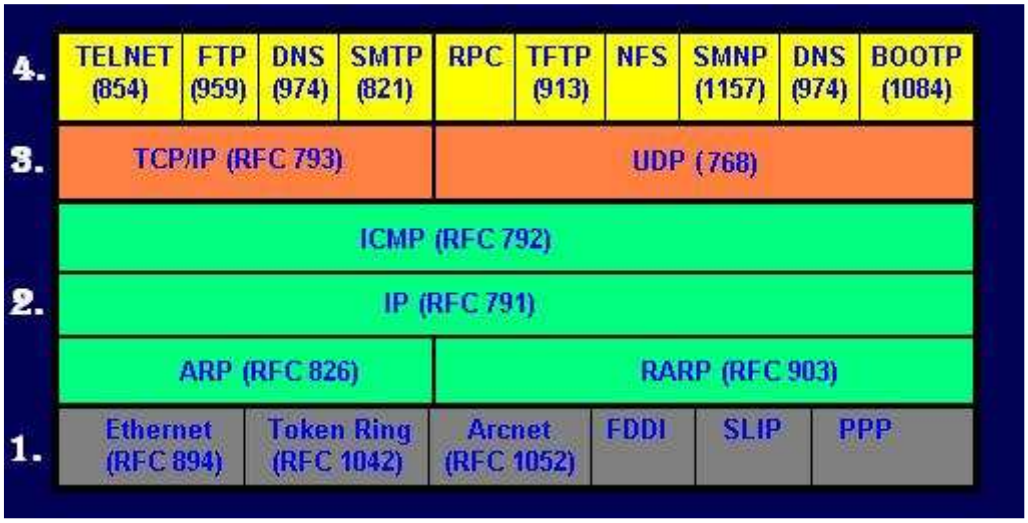
Medzisieťová vrstva - zodpovedá za smerovanie a prepájanie datagramov v komunikačnej podsieti. Datagram - je prepravná jednotka (paket), ktorý má vo svojej hlavičke IP adresu

odosielateľa a príjemcu, poradove číslo paketu v správe a iné informácie.
Smerovanie je založené na systéme IP adries hostiteľských počítačov. Smerová vrstva musí rozpoznať, či datagram je určený do lokálnej siete alebo do siete vzdialenej a podľa toho vybrať lokálny počítač alebo správny router, aby bola cesta k cieľu čo najkratšia. Pri tom používa smerovacie tabuľky (napr. podľa protokolu RIP) a protokol priraďovania fyzických adries k IP adresám (ARP).

Transportná vrstva - zabezpečuje prenos údajov medzi počítačmi protokolom TCP alebo UDP (User Datagram Protocol). TCP vytvára medzi koncovými aplikáciami spoľahlivý prenos dát (t.j. kontrolovaný, s potvrdením o doručení - analógia s telefónom). UDP zabezpečuje prenos dát bez potvrdzovania. Používajú ho tie aplikácie, ktoré nepotrebujú zabezpečenie prenosu v rozsahu TCP. UDP je nespoľahlivá služba (t.j. bez potvrdzovania príjmu, bez zaručenia poradia v cieli - analógia s prepravou listov, telegramov apod.).

Aplikačná vrstva - poskytuje široký rozsah užívateľských služieb. Najrozšírenejšie sú WWW, telnet, FTP, e-mail a news. Každej službe je priradene jedno číslo (t.j. číslo portu), podľa ktorého sa pakety rozdeľujú jednotlivým aplikáciám. Prehľad portov je v systéme UNIX v súbore /etc/services. Prítomnosť služby v tomto súbore neznamená, že odpovedajúca služba je v systéme inštalovaná.

Protokoly jednotlivých vrstiev :



Skratky protokolov znamenajú :

TELNET - je emulácia terminálu. Umožňuje užívateľovi interaktívnu pracú na vzdialenom host počítači.

FTP - umožňuje prenos súborov medzi počítačmi (File Transfer Protocol).

DNS - služba doménových mien (Domain Name Services). Priraďuje k menám počítačov ich IP adresy a naopak.

SMTP - je jednoduchý poštový protokol, ktorý zabezpečuje prenos textových sprav elektronickou cestou (Simple Mail Transfer Protocol).

RPC - je vzdialene volanie procedúr (Remote Procedure Call). Používa sa pre rozdeľovanie aplikácií na niekoľko počítačov.

TFTP - je triviálne FTP.

NFS - je sieťový súborový systém (Network File System) .Umožňuje pracovať so vzdialenými diskami ako s lokálnymi.

SNMP - je jednoduchý protokol riadenia siete (Simple Network Managament Protocol).

BOOTP - umožňuje podľa fyzickej adresy počítača zistiť jeho IP adresu a meno.

ICMP - je medzisieťový riadiaci protokol (Internet Control Message Protocol). Riadi prenos chýb a riadiacich správ medzi host počítačmi a routerami.

ARP - Address Resolution Protocol priraďuje IP adresy k fyzickým adresám.

RARP - Reverse ARP priraďuje fyzickým adresám IP adresy.

Protokoly sady TCP/IP na jednotlivých vrstvách :

Protokoly sieťovej vrstvy :

Transmission Control Protocol (TCP) :

- je jedným z protokolov balíka internetových protokolov, ktoré tvoria jeho jadro. Vďaka TCP môžu programy na počítačoch v sieti vytvárať medzi sebou spojenia (connections), ktorými je možné posielať dáta. Protokol pritom zaručuje, že dáta odoslané z jedného konca spojenia budú prijaté na druhej strane spojenia v rovnakom poradí a bez chýbajúcich častí.

V balíku internetových protokolov tvorí TCP strednú vrstvu medzi IP protokolom pod ním a aplikáciami nad ním. Aplikácie často potrebujú medzi sebou spoľahlivé rúrovité spojenia, ale Internet protokol takéto toky neposkytuje, umožňuje iba nespoľahlivé pakety. Zastáva funkciu transportnej vrstvy v zjednodušenom OSI modeli počítačových sietí.

Aplikácie posielajú sieťou pomocou TCP toky dát s 8-bitovými slabikami a TCP rozdeľuje tok bajtov do segmentov s vhodne zvolenou veľkosťou (zvyčajne ovplyvnenou maximálnou veľkosťou prenosovej jednotky (MTU)). TCP potom podáva výsledné pakety Internet protokolu na doručenie internetom TCP modulu na opačnom konci spojenia. TCP vykonáva kontrolu, aby sa uistil, že sa žiaden paket nestratí tak, že dá každému paketu poradové číslo, ktoré na druhom konci opäť TCP modul kontroluje a zabezpečuje tiež, že dáta sú doručené v správnom poradí. Vzdialený TCP modul zasiela späť potvrdenie (acknowledgement) o úspešne prijatých bajtoch; časovač odosielajúceho TCP spôsobí timeout, ak nedostane potvrdenie vo vhodne zvolenom intervale obehu (round tip time) a dáta o ktorých predpokladá, že sa stratili pošle znova. TCP kontroluje, či dáta neboli poškodené tak, že ráta kontrolný súčet (checksum) pre každý blok odoslaných dát, ktorý sa pri prijímaní kontroluje.

Fungovanie protokolu podrobne :

TCP spojenie má tri fázy: nadviazanie spojenia, prenos dát a ukončenie spojenia. Na nadviazanie spojenia sa používa tzv. 3-way handshake. 4-way handshake sa používa na ukončenie spojenia. Počas vytvárania spojenia sa inicializujú parametre ako poradové čísla paketov, aby sa zabezpečila robustnosť a poradie doručenia.

Nadviazanie spojenia :

Hoci je možné, aby dva stroje nadviazali spojenie zároveň, zvyčajne na jednom stroji beží serverová služba počúvajúca na určitom porte a pasívne počúva, t.j. čaká na prichádzajúce spojenia. Bežne sa to nazýva pasívne otvorenie a určuje stranu spojenia, ktorá funguje ako server. klientská strana spojenia začne aktívne otvorenie tým, že pošle úvodný SYN segment serveru. Server by mal odpovedať platnou požiadavkou SYN so SYN/ACK. Nakoniec by mal klient odpovedať ACK, čím sa 3-way handshake, a teda fáza nadviazania TCP spojenia ukončí.

Prenos dát :

Počas fázy prenosu dát určuje niekoľko kľúčových mechanizmov spoľahlivosť a robustnosť TCP. Patria medzi ne poradové čísla pre určenie poradia TCP segmentov a detekciu duplikátnych dát, kontrolné súčty pre detekciu chýb v segmentoch a potvrdzovanie a časovače pre detekciu a prispôsobenie sa strate alebo oneskoreniu dát.

Počas fázy nadviazania TCP spojenia sa medzi dvoma strojmi vymenia tzv. initial sequence numbers (ISN). Tieto slúžia na idetifikáciu dát v dátovom toku a počítanie dátových bytov. V každom TCP segmente existuje dvojica poradových čísel, ktoré sa nazývajú poradové číslo a potvrdzovacie číslo. Odosielateľ TCP segmentu nazýva poradové číslo jednoducho poradové číslo, zatiaľ, čo odosielateľ považuje poradové číslo segmentu od prijímateľa za potvrdzovacie číslo. Aby bola zabezpečená spoľahlivosť, prijímateľ potvrdzuje dáta v TCP segmente tak, že indikuje obdržané množstvo súvislých bajtov v TCP toku. Rozšírenie TCP nazývané selektívne potvrdzovanie (selective acknowledgement, SACK) umožňuje prijímateľovi potvrdzovať bloky mimo poradia.

Použitím poradových a potvrdzovacích čísel je TCP schopné doručovať obdržané segmenty v správnom poradí v dátovom toku prijímajúcej aplikácii. Poradové čísla sú 32-bitové čísla bez znamienka, ktoré po dosiahnutí čísla 232-1 pokračujú znova od nuly. Kľúčom k udržaniu robustnosti a bezpečnosti TCP spojenia je výber ISN.

16-bitový kontrolný súčet pozostávajúci z doplnkov do jednotky a sumy doplnkov do jednotky obsahu hlavičky TCP segmentu a dát vypočíta odosielateľ a zahrnie ho do prenosu. (Súčet doplnkov do jednotky sa používa preto, lebo je ho možné vypočítať v každom násobku dĺžky -- 16-bitov, 32-bitov, 64-bitov atď. -- a výsledok bude po preložení rovnaký.) TCP prijímač počíta súčet prijatej TCP hlavičky a dát. Doplnok (hore) bol použitý preto, aby prijímač nemusel nulovať súčtové pole po uložení hodnoty inde; namiesto toho prijímač jednoducho vypočíta doplnok do jednotky na mieste kontrolného súčtu a výsledok by mal byť -0. Ak je to tak, segmet prišiel nedotknutý a bez chýb.

Všimnite si, že kontrolný súčet tiež zahŕňa 96 bitovú pseudohlavičku obsahujúcu zdrojovú adresu, cieľovú adresu, protokol a dĺžku segmentu. Tým poskytuje ochranu pred chybne smerovanými segmentami.

Podľa súčasných štandardov je kontrolný súčet pomerne slabou kontrolou. Spojové vrstvy s vysokou pravdepodobnosťou bitových chýb môžu požadovať dodatočné kontroly a opravy chýb. Ak by dnes bolo TCP znova navrhované, pravdepodobne by obsahovalo 32-bitovú cyklickú kontrolu redundancie (CRC, cyclic redundancy check) namiesto súčasného kontrolného súčtu. Slabá kontrola je čiastočne kompenzovaná bežným použitím CRC alebo inej integritnej kontroly na vrstve 2, pod TCP a IP, ako je použité v rámci PPP alebo Ethernetu. To však neznamená, že je kontrolný 16-bitový TCP súčet nadbytočný: výskumy internetovej premávky ukázali, že softvérové a hardvérové chyby produkujúce chybné pakety medzi hopmi premávky chránenej CRC a že 16-bitový TCP kontrolný súčet zachytáva väčšinu týchto chýb. To je princíp end-to-end spojenia v praxi.

Veľmi zjednodušene je možné prenos paketu popísať takto :
Údaje a požiadavky na prenos vznikajú v aplikačnej vrstve. Ta dáta a IP adresu príjemcu odovzdá transportnej vrstve, ktorá vytvorí paket alebo datagram, čo odovzdá medzisieťovej vrstve.

Približná štruktúra paketu v tomto štádiu je takáto :

kde je :
IP-DA - IP adresa cieľového počítača (Destination Address)
IP-SA - IP adresa zdrojového počítača (Source Address)
IP-DATA - dáta uložené v pakete (datagram alebo TCP paket)

Medzisieťová vrstva musí rozlíšiť, či je ide paket do lokálnej siete (t.j. priame doručenie), alebo paket do inej siete. K tomuto rozhodovaniu používa svoju IP adresu, sieťovú masku a routovacie tabuľky. Podľa toho je paket odoslaný priamo príjemcovi alebo na príslušný router, ktorý zabezpečí jeho ďalšiu prepravu.

Pred vyslaním do sieťového média je paket zabalený do prepravného rámca. Pre sieťové médium Ethernet je jeho približná štruktúra takáto :

kde je:
ETH-DA - fyzická adresa príjemcu (t.j. adresa Ethernet karty príjemcu alebo routera; pre jej zistenie sa používa protokol ARP).
ETH-SA - fyzická adresa odosielateľa.
ETH-DATA - IP datagram.

Pri odosielaní sa veľkosť paketu postupne zväčšuje, každá vrstva pridá svoje informácie dopredu a dozadu. Tento proces sa nazýva zapuzdrovanie (encapsulation) IP paketov. Pri doručení v cieľovom počítači sa postupuje opačné.

Internet protokol (IP) :

IP zodpovedá sieťovej vrstve, jeho úlohou je prenášať tzv. IP-datagramy medzi vzdialenými PC. Každý IP-datagram má v záhlaví adresu príjemcu, čo je úplnou smerovacou informáciou k prenosu. Sieť môže každý IP-datagram preniesť samostatne, nemusia teda doraziť k adresátovi v poradí akom boli odoslané. Z toho vyplýva, že každé sieťové rozhranie v Internete musí mať svoju celosvetovo jedinečnú IP-adresu. Pre určenie cieľa prenosu sa nepoužíva iba IP, pri vyslaní dát na prenosové médium (krútená dvojlinka, optický kábel) sa samotné pakety (zákl. prenosová jednotka) doplnia aj o zdrojovú a cieľovú MAC adresu. Tiež sa ešte doplnia o číslo určujúce prenášaný protokol (IP, IPv6, IPX...). Toto spolu s paketom tvorí tzv. rámec. Pri vyslaní rámca na prenosové médium ho príjmu všetky počítače pripojené na toto médium. Ak je ako cieľová adresa uvedená ich MAC adresa, paket sa postúpi na spracovanie vyšším vrstvám. Ak cieľová adresa nie je zhodná s ich MAC adresou, rámec sa "zahodí". Ak chce počítač zaslať mimo lokálnu sieť (na internet) k tomu slúžia zariadenia ako rozbočovače, prepínače alebo najinteligentnejšie z nich smerovač-router. Keď takýto rámec dorazí na router, ten podľa MAC adresy zistí, že je určený práve jemu, ale podľa IP adresy zistí, že je určený niekomu inému a na základe nastavenia smerových tabuliek ho nasmeruje na internet. Pri tomto prenose (tak ako budú putovať po ďalších sieťach) sa menia iba MAC adresy, pričom zdrojová MAC adresa je adresou z ktorej rámec prišiel a cieľová MAC adresa je adresou sieťovej karty ďalšieho počítača (najčastejšie routera) na ktorý ho postúpia. IP adresa ani dáta sa nemenia.

MAC adresa :

MAC adresa (inak povedané hardwarová adresa) je unikátne číslo, ktoré nesie naša sieťová karta od výrobcu. Býva dvanásť miestne a skladá sa z čísel a písmen. Príkladom MAC adresy je napr. 00:0C:2B:DE:3F:25 Za bežných okolností sa táto adresa nedá v operačnom systéme zmeniť - je daná výrobcom sieťovej karty. Vedieť svoju MAC adresu je však dôležité z dôvodu, že Vaše Internetové konto na sieti NITRANET je sprístupnené práve vďaka registrácii MAC adresy Vašej sieťovej karty v našom systéme. Je to z dôvodu bezpečnosti, aby nikto iný nemohol používať vaše pripojenie na Internet. Pri výmene sieťovej karty za inú, prípadne pri výmene celého počítača je preto nutné ohlásiť nám novú MAC adresu Vašej novej sieťovej karty, prostredníctvom ktorej budete pripájať svoj počítač k sieti NITRANET. MAC adresu Vašej sieťovej karty je možné zistiť nasledovne:

Pre Windows 95/98/Me - klikneme na tlačidlo ŠTART - SPUSTIŤ a v uvedenom riadku napíšeme: "winipcfg" Kliknutím na OK sa otvorí nové okno, v ktorom už stačí iba zvoliť svoju sieťovú kartu a systém Windows v tabuľke zobrazí všetky parametre sieťovej karty, vrátane MAC adresy (teda fyzickej, resp. hardwarovej adresy adaptéra).

Pre Windows 2000/XP - klikneme na tlačidlo ŠTART - SPUSTIŤ a v uvedenom riadku napíšeme príkaz: "cmd" Kliknutím na OK sa otvorí nové okno - príkazový riadok systému. Tu napíšeme príkaz "ipconfig /all" a systém windows zobrazí parametre sieťovej karty, vrátane fyzickej adresy.

Protokoly :

Telnet
Vzdialené prihlasovanie – Remote login. Prostredníctvom vášho PC sa prihlásite k vzdialenému PC (vystupujúceho v úlohe vzdialeného terminálu) ktorý môžte ovládať pomocou textových príkazov vpisovaných do príkazového riadku. Prostredníctvom Telnetu sa možno prihlásiť aj na odlišné platformy operačných systémov (z Unixu do Windows a pod.).

FTP
(File Transfer Protocol) – využívaný k prenosu súborov (napr. obrázky, filmy) medzi vzdialenými PC, respektíve ide o službu ktorá umožňuje prenášať súbory. Výhodou je že so súbormi na vzdialenom počítači možno pracovať rovnako ako keby sa nachádzali na vašom lokálnom disku, samozrejme ak k ním máte príslušné administrátorské oprávnenia. Pre prácu je potrebné prevádzkovať na PC ku ktorému sa pripájame aplikáciu s názvom FTP server. FTP počúva na porte 21, ktorý slúži k prenosu príkazov od klienta k serveru nazývané aj ako control connection. Samotný download/upload súborov sa uskutočňuje na porte 20 - dáta connection.
Pred samotným prenosom dát musí server vedieť na ktorý port sa má pripojiť, preto sa klient a server dohodnú na IP adrese aj porte.

DNS
(Domain Name Service) – jeho úlohou je preklad plného mena domény do numerickej podoby IP formátu (napr. irianis.com prevedie na 192.170.2.1) prostredníctvom DNS serverov. Výhodu zapamätania si názvu pred číselným formátom asi netreba spomínať. Systém DNS používa protokol TCP ako aj UDP pričom počúva na porte 53.

SMTP
(Simple Mail Transfer Protocol) - spolu so štandardom RFC821 definuje koncepciu elektronickej pošty. Využíva protokolu TCP pre odosielanie, prijímanie správ a adresovanie el. pošty. Je zameraný na prenos čisto textových správ (tzv. ASCII znaky). v sedembitovom formáte. Národné abecedy používajú aj neštandardné znaky (mäkčene, prehlásky...) tie je nutné zakódovať v osembitovom formáte pomocou sedembitových znakov. Rovnako existuje potreba prenášania netextových správ hudba, video atď.
Prenos najrôznejších formátov, vrátane multimediálnych rieši štandard MIME - Multipurpose Internet Mail Extensions, ktorý v podstate definuje :

- **spôsob kódovania (7 alebo 8 bitové)**
- **spôsob vyjadrenia typu prenášaných dát**
- **spôsob vloženia netextových dát**

MIME našiel uplatnenie aj mimo el. pošty napr.: keď www server posiela svojmu klientovi (browseru – prehliadačovi) nejaké dáta, pripojí k nim informáciu o type týchto dát pomocou konvencie štandardu MIME.

ICMP
(Internet Control Message Protokol) - je tretím najpoužívanejším internetovým protokolom. Slúži na diagnostikovanie siete (napr. ping), tiež na rýchle informovanie o zmene trasy na ktorej prebieha prenos a iné.

ARP
(Address Resolution Protocol) - slúži k prevodu IP adries na Ethernetové adresy. Pracuje na princípe otázka - odpoveď. Najlepší bude príklad: počítač s adresou x.x.x.x vie, že má poslať pakety cez počítač (switch, router) s adresou y.y.y.y . Aby zistil jeho MAC adresu, pošle ARP-otázku (ARP-request) na ktorú čaká odpoveď. Ak chcete vedieť aké MAC adresy sú priradené k jednotlivým IP adresám použite príkaz arp ktorý funguje pod Unix ako aj Windows. Ak chcete ručne zistiť MAC adresu dá sa pod Linux-om poslať ARP otázka príkazom arping.

Pre vzájomnú komunikáciu v sietiach si každý počítač udržiava v pamäti IP adresy a k nim príslušné MAC adresy, takže nabudúce nemusí odosielať ARP pakety, ale priamo začne s ním komunikovať. Samozrejme že sa tieto údaje pravidelne obnovujú. RARP (reverzný ARP) opačný prevod k ARP.

UDP
(User Datagram Protocol) - je vlastne nadstavbou IP schopnou naviac rozlišovať medzi jednotlivými príjemcami a odosielateľmi (napr. rôzne aplikácie, systémové procesy …) v rámci uzlov.
Protokol UDP sa používa na rýchlu výmenu malého objemu dát bez potvrdenia ich doručenia, kde sa nepožaduje nadväzovať na začiatku spojenie. Príkladom je DNS kde pošleme dotaz na IP adresu nejakého PC jedným UDP paketom a ako odpoveď dostaneme tiež jeden UDP paket.

SLIP
(Serial Line IP) a PPP (Point-to-Point Protocol, niekedy označovaný aj ako P2P). Oba slúžia potrebám prenosu protokolu IP po dvojbodových spojoch (sériových linkách), rozšírené vďaka jednotlivým PC pripojených k Internetu. Výnimočnosť z celkovej koncepcie TCP/IP tvorí konkrétna vlastná prenosová technológia, nevyužívajú existujúce sieťové rozhranie.

DHCP
(Dynamic Host Resolution Protocol) – dynamicky prideľuje jednotlivým pc v rámci siete IP adresy. To si vyžaduje prítomnosť DHCP servera.

HTTP
(Hypertext Transfer Protocol) – protocol transferu hypertextových informácií.

Ďalej >>