

Komunikačné protokoly

Základným predpokladom na to, aby mohli dva počítače navzájom komunikovať, je ich vzájomné prepojenie do spoločnej siete, alebo navzájom prepojených sietí. Avšak ani tento fakt nezabezpečí, že počítače budú vedieť medzi sebou komunikovať. Je potrebné aby poznali a používali rovnaký komunikačný protokol. Počítač môže byť schopný komunikovať pomocou niekoľkých, súčasne inštalovaných protokolov. To zabezpečí väčšiu rýchlosť a priepustnosť (alebo bezpečnosť) siete. Ostáva ešte vyriešiť otázku, ako v sieti jednoznačne identifikovať konkrétny počítač, teda ako nadviazať spojenie s konkrétnym počítačom. Každý počítač je možné vzhľadom k použitému protokolu nakonfigurovať tak, aby bol v rámci siete jedinečný a teda identifikovateľný aj pre ostatné počítače. Samozrejme spôsob konfigurácie sa v závislosti od použitého protokolu líši. A to čo býva najlepšie, býva aj najťažšie konfigurovateľné.

Komunikačný protokol – súhrn parametrov a pravidiel, ktorými sa riadi komunikácia. Ide predovšetkým o druh prenosu, jeho rýchlosť, kontrolu apod. Aby mohlo dôjsť k úspešnej komunikácii musia obe strany dodržiavať daný komunikačný protokol.

Základné komunikačné protokoly

Zameriame sa predovšetkým na siete MS (ale nie len na ne).

NetBEUI

Komunikačný protokol NetBEUI (NetBIOS Extended User Interface) bol vyvinutý firmou IBM v polovici 80. rokov 20. storočia.. Stal sa v podstate štandardom v prostredí malých sietí MS Windows. Často sa využíva pri komunikácií medzi pracovnými stanicami s operačným systémom Windows. Inštalácia je pomerne jednoduchá, jediným parametrom je názov počítača a pracovnej skupiny. K výhodám patrí dosahovaná prenosová rýchlosť a minimálne nároky na konfigurovateľnosť. Bohužiaľ tento protokol nie je routovateľný (t.j. komunikáciu v sieti nie je možné požadovaním spôsobom smerovať). Preto sa nedá použiť k pripojeniu lokálnej siete do siete Internet. Často sa teda používa súčasne s iným routovateľným protokolom (napr. TCP/IP).

IPX/SPX

Komunikačný protokol IPX/SPX (Internetwork Packet eXchange/Sequenced Packet Exchange) bol vyvinutý pre potreby operačného systému Novell NetWare. V podstate sa nejedná o jeden protokol, ale o skupinu protokolov. Používa sa pri komunikácii medzi počítačmi s OS Windows a Novell NetWare. Je jednoducho konfigurovateľný. IPX/SPX je routovateľný protokol.

TCP/IP

Komunikačný protokol TCP/IP (Transmission Control Protocol/Internet Protocol) je v súčasnosti najpopulárnejším komunikačným protokolom. Nejedná sa o jediný protokol ale o skupinu protokolov . Protokol TCP/IP je univerzálny v tom zmysle, že je možné ho používať pri komunikácii medzi počítačmi s rôznymi OS. Je routovateľný a vďaka tomu sa stal štandardom pre komunikáciu v sieti Internet. Inštalácia protokolu je jednoduchá. O konfigurácií to už však neplatí.

Protokol TCP/IP obsahuje ďalšie súčasti a protokoly:

DHCP (Dynamic Host Resolution Protocol) – tento protokol sa využíva pre dynamické pridelovanie IP adries (jedinečný identifikátor počítača v sieťach s protokolom TCP/IP). Na niektorom z počítačov v sieti (najčastejšie je to server) je inštalovaná služba DHCP server, ktorá sa stará o dynamické pridelovanie IP adries klientom. Samozrejme IP adresu klientom môžeme prideliť aj staticky, napevno.

DNS (Domain Name Service) – úlohou tejto služby je preklad plného mena domény do číselnej podoby v tvare IP adresy. Keďže pri komunikácii používajú počítače IP adresy a ľudia si skôr zapamätajú doménové meno počítača, bol vytvorený systém DNS na preklad doménového mena na IP adresu, resp. naopak.

SMTP (Simple Mail Transfer Protocol) – poskytuje jednoduchú službu elektronickej pošty. Využíva protokol TCP pre odosielanie a prijímanie správ elektronickej pošty.

FTP (File Transef Protocol) – protokol využívaný na prenos súborov medzi vzdialenými počítačmi. Ak chcem s týmto protokolom pracovať, je nutné aby na počítači ku ktorému sa pripojujeme bola spustená služba FTP server.

Telnet – služba pomocou ktorej sa dokážeme pripojiť na ktorýkoľvek hosťiteľský počítač v rámci Internetu, ak máme na ňom vytvorený účet. Tento počítač potom dokážeme ovládať pomocou textových príkazov.

HTTP (HyperText Transport Protocol) - protokol určený k prenosu hypertextových dokumentov cez internet. K svojej funkcii vyžaduje server - HTTP server a klienta HTTP (napr. internetový prehliadač).

HTTPS (HyperText Transport Protocol Secure) – variant protokolu HTTP pre bezpečný prenos.

Zisťovanie informácií o spojení a o vzdialenom počítači.

Ping – pomocou tejto služby dokáže otestovať dostupnosť ktoréhokoľvek počítača v sieti TCP/IP. Príkazom ping vyšleme požiadavku k cieľovému počítaču a čakáme na potvrdenie prijatia (odozvu). Ak odpoveď nedorazí, počítač sa v sieti nenašiel a je potrebné vyriešiť problém s jeho dostupnosťou.

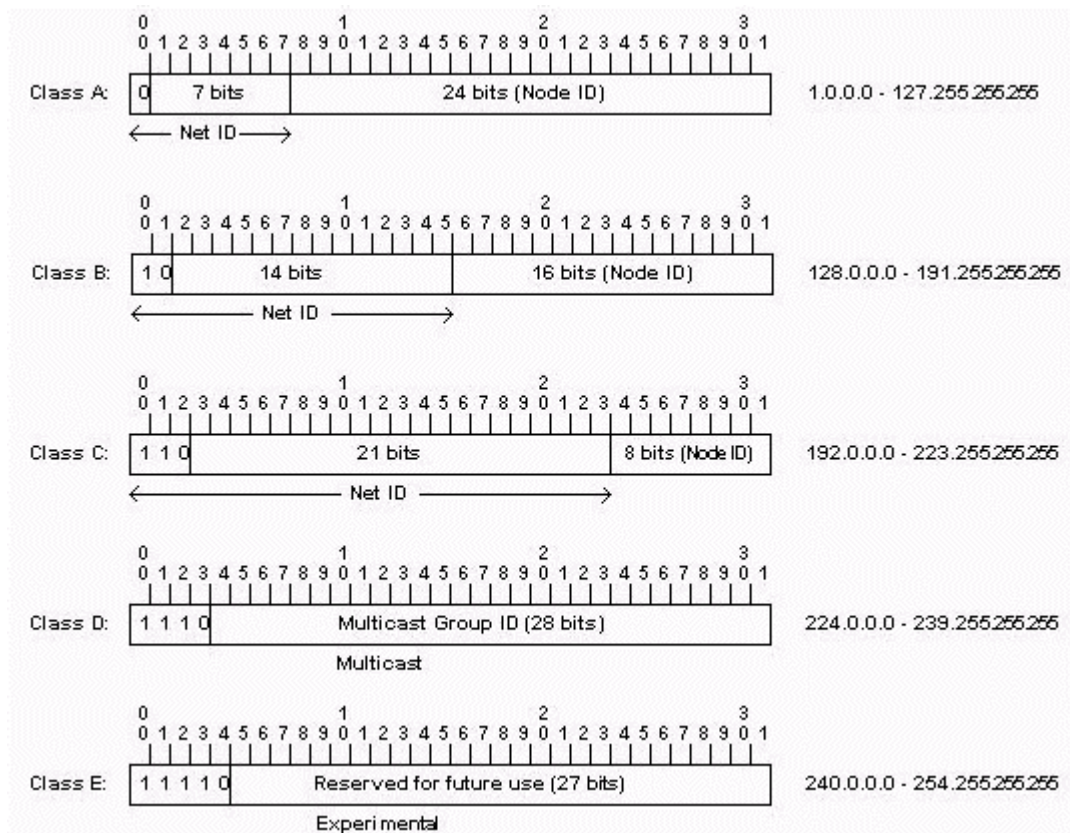
Traceroute – pomocou tejto služby dokážeme zistiť smerovanie blokov dát medzi našim počítačom a zadaným počítačom. Vo výpise vidíme zoznam smerovačov v takom poradí, v akom bloky dát cez ne prechádzajú a štatistické informácie o čase, za ktorý sa tam dostanú..

Nslookup – pomocou tejto služby dokážeme zistiť IP adresu a doménovú adresu nášho a cieľového počítača (resp. môžeme aj utility dig a host)

IP adresa

IP adresa je adresa počítača (ktorá ho jednoznačne identifikuje) v sieťach používajúcich protokol IP. Adresa má špeciálny 32 bitový číselný formát, ktorý je rozdelený na štyri 8 bitové časti (oktety) oddelené bodkami: XXX.XXX.XXX.XXX.. Každá z týchto častí je v praxi tvorená dekadickým číslom z intervalu 0..255. IP adresy teda môžu byť v rozsahu od 0.0.0.0. do 255.255.255.255. V praxi však platia isté obmedzenia, takže tento rozsah sa nikdy nemôže dosiahnuť. IP adresa v celej dostupnej sieti musí byť jedinečná, čo nie je problém v lokálnych sieťach. Používanie IP adries celosvetovo je prísne kontrolované a jednotlivé IP adresy sú pridelené špecializovanými medzinárodnými organizáciami.

Problém zachovanie jedinečnosti IP adries je riešený rozdelením adries do skupín. Bolo definovaných 5 skupín.



zdroj: <http://www.cisco.com/>, 26. 3. 2004

Adresy typu 127.X.X.X sú vyhradené pre špeciálne účely (diagnostika siete).

Adresy triedy D sú vyhradené pre skupinovú adresáciu a adresy typu E pre experimentálne účely.

Časť IP adresy predstavuje adresu siete (Net ID, ľavé oktety) a adresu hostiteľa (Node ID, pravé oktety).

- Trieda A:** prvý bit (0) a ďalších 7 bitov predstavuje adresu siete, zvyšných 24 bitov adresu hostiteľa
prvý byte: 0 – 127
existuje 126 sietí typu A (0 and 127 sú rezervované)
v každej sieti typu A môže byť až 16.777.214 hostiteľov
- Trieda B:** prvé dva bity (10) a ďalších 14 bitov predstavujú adresu siete, zvyšných 16 bitov adresu hostiteľa
prvý byte: 128 – 191
existuje 16 384 sietí typu B
v každej z nich môže byť 65,532 hostiteľov
- Trieda C:** prvé tri bity (110) a ďalších 21 predstavujú adresu siete, zvyšných 8 bitov adresu hostiteľa
prvý byte: 192 – 223
existuje 2 097 152 adries typu C
v každej z nich môže byť 254 hostiteľov

Problém je v tom ako zistiť, ktorá časť IP-adresy je adresou siete a ktorá adresou počítača. Nie je ani celkom jasné čo to znamená slovo sieť, pretože jeho význam sa postupne menil a okrem slova sieť sa zaviedli pojmy subsiet a supersiet. Na siete sa dnes nepozerala cez triedy, ale cez masky. Pomocou masky dokážeme rozlíšiť v IP adrese časť sieťovú a časť hostiteľskú. Maska siete má rovnako ako IP adresa 32 bitový formát. Typická maska v sieti A je 255.0.0.0, v sieti B 255.255.0.0 a v sieti C 255.255.255.0. Pomocou masky môžeme definovať aj podsiete. Princíp masiek vychádza z predpokladu, že tam, kde je v binárnom vyjadrení masky jednotka, tam je sieť. Tam kde je nula, je uzol (hostiteľ).

Ak by sme urobili prepočet jednotlivých bodkou oddelených čísiel napr. IP čísla 192.168.2.10 a IP čísla masky 255.255.255.128 do dvojkovej sústavy vznikli by čísla:

```
11000000.10101000.00000010.00001010 - 192.168.2.10
11111111.11111111.11111111.10000000 - 255.255.255.128
-----
11000000.10101000.00000010.00000000 - 192.168.2.0
```

Ak vykonáme porovnanie týchto čísiel podľa pravidla, že vo výsledku bude 1 len v miestach, kde sú aj v hornom aj v dolnom čísle číslice 1, dostaneme číslo uvedené pod čiarou. Po spätnom prevode do desiatkovej sústavy znamená to IP číslo 192.168.2.0. V našom prípade teda sieť bude mať číslo 192.168.2.0.

Ipv6

V dobe vytvorenia systému tvorby IP čísla sa nepredpokladalo, že veľké siete budú mať taký rozmach ako to je tomu dnes a bude tak akútny nedostatok vhodných adries (zatiaľ sa tento problém rieši napr. pomocou dynamického pridelovania IP adries, NAT (Network Address Translation tzv. maškaráda)), a tak aj tvorba IP čísla bola nedávno inovovaná. Pôvodne 32 bitové číslo (IP verzia 4) bolo nahradené 128 bitovým (IP verzia 6). Nové čísla sú tvorené tak, aby bola zachovaná kompatibilita s doteraz používaným systémom pridelovania čísiel. Pre užívateľa to znamená toľko, že bez zásahu do systému bude jeho zariadenie naďalej korektne pracovať aj v novom systéme, pričom nový systém vytvára dostatočné rezervy pre budúcich užívateľov Internetu a iných veľkých sietí. Pôvodná forma zápisu, štvorica trojmiestnych čísiel oddelených povinne bodkou sa ale mierne mení. Napr. číslo podľa pôvodného zápisu (IP verzia 4) 147.175.68.11 sa zapíše v novej forme (IP verzia 6) tak, že sa doplní dvoma dvojbodkami na začiatku, teda ::147.175.68.11.

Nakoľko nová adresa je šesťnásťbajtová bolo by nepraktické prevziať spôsob zápisu IP adresy z IPv4. Preto sa adresy zapisujú v šesťnásťkovej sústave a jednotlivé dvojice bajtov sa od seba oddeľujú dvojbodkou. Takže IPv6 adresa môže vyzeráť nasledovne:

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

Aby sa zápis ešte skrátil je možné v jednotlivých štvoricach vynechávať počiatočné nuly. Ak by sa vyskytli po sebe idúce nulové skupiny, je možné ich nahradiť dvojicou dvojbodiek. Tá sa však kvôli jednoznačnosti môže v zápise použiť len raz. Napr.: nasledujúce zápisy IPv6 adries sú ekvivalentné.

FF01:0000:0000:0000:0000:0000:0000:0101

FF01:0:0:0:0:0:0:101

FF01::101

Zápis je teda dosť komplikovaný a nepredpokladá sa, že by ho užívatelia písali. Pre nich sú určené mená a adresy, ktoré sa vybavujú prostredníctvom DNS serverov.

Model ISO/OSI

TCP/IP je označenie viacerých protokolov, ktoré sa používajú pri komunikácií prostredníctvom Internetu. Dôvodom pre potrebu viacerých protokolov je komplikovanosť problémov, ktoré treba riešiť. Riešenie prebieha na niekoľkých úrovniach a na každej z nich sa používa iný druh protokolov. Hovoríme o vrstvách.

Pôvodný model prepojovania otvorených systémov (z pohľadu počítačových sietí sa takto nazýva aj sieť Internet) bol štvorvrstvový. Neskoršie bol prepracovaný, doplnený a v roku 1984 prijatý v súčasnosti používaný sedemvrstvový referenčný model, označovaný ako OSI (Open System Interconnection). Vypracovala ho medzinárodná štandardizačná organizácia ISO a obsahuje samozrejme aj štyri vrstvy predošlého modelu.

1.	aplikačná vrstva (application)	Program
2.	prezentačná vrstva (presentation)	prevod do tvaru zrozumiteľného pre príjemcu
3.	relačná vrstva (session)	vytvorenie a údržba spojenia s príjemcom
4.	transportná vrstva (transport)	dozor na spoľahlivý prenos správ a opravy chýb
5.	sieťová vrstva (network)	Vytvorenie paketu s adresami a ostatnými nutnými časťami
6.	spojová vrstva (data-link)	vytvorenie rámcov a ich vysielanie
7.	fyzická vrstva (physical)	prenos rámcov vo forme elektrických signálov

V tomto modeli je najnižšie položená vrstva fyzická, ktorú tvoria hardverové prostriedky (vodiče, sieťové karty atd.) a najvyššie aplikačná vrstva, ktorú tvoria najčastejšie užívateľské programy (napr. Netscape Communicator, Internet Explorer, Word atd.).

Od okamihu, keď užívateľ odošle dáta zo svojej sieťovej aplikácie po ich fyzickú prítomnosť v sieti, prejdú údaje niekoľkými myslenými vrstvami.

Fyzická vrstva

Fyzická vrstva zabezpečuje prenos informácií vo forme elektrických alebo optických signálov. Pomocou nich prebieha komunikácia medzi počítačmi, preto vlastnosti tejto vrstvy sú vopred starostlivo definované. Prepojovacím uzlom na tejto vrstve môže byť opakovač (repeater).

Spojová vrstva

Spojová vrstva zaisťuje v prípade sériových liniek výmenu dát medzi susednými počítačmi a v prípade lokálnych sietí výmenu dát v rámci lokálnej siete. Základnou jednotkou

pre prenos dát je na linkovej vrstve dátový rámec. Dátový rámec sa skladá zo záhlavia (Header), prenášaných dát (Payload) a pätičky (Trailer).

Dátový rámec nesie v záhlaví linkovú adresu príjemcu, linkovú adresu odosielateľa a ďalšie riadiace informácie.

V pätičke nesie okrem iného obvykle kontrolný súčet z prenášaných dát. Pomocou neho je možné zistiť pri prenose chybný prenos (porušenie) dát. V prenášaných dátach je potom spravidla nesený paket sieťovej vrstvy.

Prepojovacím uzlom na tejto vrstve môže byť most (bridge).

Sieťová vrstva

Sieťová vrstva zabezpečuje prenos dát medzi vzdialenými počítačmi WAN (smerovanie). Základnou jednotkou prenosu je sieťový paket, ktorý sa balí do dátového rámca. Sieťový paket sa tiež skladá zo záhlavia a dátového poľa. S pätičkou sa u sieťových protokolov stretávame len zriedka.

V rozsiahlych sieťach (WAN) medzi počítačmi leží spravidla jeden alebo viac smerovačov (router). Medzi susednými smerovačmi je na linkovej vrstve vždy priame spojenie. Smerovač vybalí sieťový paket z dátového rámca (jedného linkového protokolu) a pred odoslaním do inej linky ho opäť zabalí do iného dátového rámca (obecne iného linkového protokolu).

Prepojovacím uzlom na tejto vrstve môže byť smerovač (router).

Transportná vrstva

Sieťová vrstva zabezpečí spojenie medzi vzdialenými počítačmi, takže transportnej vrstve sa javí akoby žiadne modemy, opakovače, mosty či smerovače na ceste neboli. Transportná vrstva sa celkom spolieha na služby nižších vrstiev. Tiež predpokladá, že spojenie medzi počítačmi je zaistené, preto sa bez zbytočných starostí môže venovať spojeniu medzi aplikáciami na vzdialených počítačoch.

Medzi dvoma počítačmi môže byť niekoľko transportných spojení súčasne, jedno napr. pre virtuálny terminál a druhé pre elektronickú poštu. Z hľadiska sieťovej vrstvy sú pakety adresované adresou počítača (resp. jeho sieťového rozhrania). Z hľadiska transportnej vrstvy sú adresované jednotlivé aplikácie. Aplikácie sú jednoznačne adresované v rámci jedného počítača.

Jednotkou prenosu je transportný paket, ktorý sa opäť skladá zo záhlavia a dátovej časti. Transportný paket sa prenáša v dátovej časti sieťového paketu.

Pri vysielaní zabezpečuje segmentáciu dlhých správ do paketov a pri príjme zloženie paketov do pôvodnej správy.

Prepojovacím uzlom na tejto a nadradených vrstvách môže byť brána (gateway).

Relačná vrstva

Relačná vrstva zabezpečuje výmenu dát medzi aplikáciami, tj. prevádza tzv. checkpoint, synchronizáciu transakcií (commit), korektné uzatváranie súborov atd. Dobré predstaviteľnou reláciou je napr. zdieľanie sieťového disku. Disk môže byť zdieľaný po určitú dobu, avšak pracuje sa s ním len zriedka. Vždy, keď je napr. treba pracovať so súborom na sieťovom disku, nadviaže sa na dobu od otvorenia súboru až po jeho uzavretie spojenie na transportnej vrstve. Avšak relácia na relačnej vrstve existuje po celú dobu zdieľania disku.

Nadväzuje, udržiava a ruší logické spojenia - relácie medzi koncovými účastníkmi.

Základnou jednotkou je relačný paket, ktorý sa opäť vkladá do transportného paketu.

Prezentačná vrstva

Prezentačná vrstva je zodpovedná za reprezentáciu a zabezpečenie dát. Reprezentácia dát môže byť na rôznych počítačoch rôzna. Napr. sa jedná o problém či je najvyšší bit v bajte celkom vľavo alebo vpravo a pod. Zabezpečením sa rozumie šifrovanie, zabezpečenie integrity dát, digitálne podpisovanie a pod.

Aplikačná vrstva

Aplikačná vrstva predpisuje v akom formáte a ako majú byť dáta preberané/predávané od aplikačných programov. Napr. protokol Virtuálny terminál popisuje ako majú byť dáta formátované, ale aj dialóg medzi oboma koncami spojenia.

Použitá literatúra:

- § Kostrhoun, A.: Stavíme si malou síť. Praha: Computer Press, 2001. ISBN 80-7226-510-5
- § Hlavenka, J.: Výkladový slovník výpočetní techniky a komunikací. Praha: Computer Press, 1997. ISBN 80-7226-023-5
- § Cisco Systems, Inc. IP Addressing and Subnetting for New Users. [online] Publikované 26. 12. 2003. Dostupné z <<http://www.cisco.com/warp/public/701/3.html>>.
- § HALČIN Pavol. Počítačové siete. [online] Publikované 18.2.2002. Dostupné z <http://www.gymsnv.sk/~x8ahalp/net_web/>.
- § Počítačové siete [online] Dostupné z <<http://www.spsmt.sk/phare/>>.
- § České IPv6. [online] Dostupné z <<http://www.ipv6.cz> >.