INVESTICE DO ROZVOJE VZDĚLÁNÍ
Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky

Sada protokolů TCP/IP

Cílem této kapitoly je popsat jednu z nejpoužívanějších rodin protokolů pro síťovou komunikaci, TCP/IP. Význam TCP/IP spočívá mimo jiné v tom, že jde o sadu komunikačních protokolů používaných v síti Internet.
Kapitola čtenáře seznámí s komunikačními protokoly síťové a transportní vrstvy, protokolům vrstvy aplikační je pro jejich velký počet věnována samostatná kapitola. V samostatné kapitole je také popsán způsob adresace v sítích založených na architektuře TCP/IP (IP adresy).

Klíčové pojmy:
Síťová architektura TCP/IP, RFC, rámec, IP, best effort, MTU, fragmentace paketu, ICMP, ARP, broadcast, proxy ARP, RARP, IGMP, multicasting, TCP, handshake, UDP.

Charakteristika protokolů TCP/IP

Protokoly TCP/IP jsou v současnosti chápány jako standard pro komunikaci v počítačových sítích, používají se např. v nejrozsáhlejší světové síti Internet. Architektura TCP/IP zahrnuje jednak vlastní přenos datových paketů sítí (zajišťuje protokol IP), dále rozhraní pro nespojované, nepotvrzované zasílání datagramů UDP a protokol logického kanálu TCP. Protokol TCP prostřednictvím potvrzování zajišťuje spolehlivost v prostředí sítí, kde přenos dat na nižších úrovních se děje principiálně nespolehlivě, s nezaručeným pořadím doručování paketů, s možností fragmentace a zahození dat na cestě. Protokol TCP je vybaven řízením toku dat a ochranou proti chybám, které mohou vzniknout opakovaným navazováním spojení. Pro aplikace jsou viditelné protokoly IP, TCP a UDP, tyto protokoly jsou dále podporovány služebními protokoly, které mají za úkol překlad síťových adres na adresy hardwarové (ARP) nebo opačně (RARP), řízení a testování sítí a generování chybových hlášení (ICMP) a podporu směrování (RIP, OSPF).

Nejdůležitější principy, na kterých je založena architektura TCP/IP:

- Možnost snadného připojení sítí založených na různých technologiích
- Nespojovaný a bezestavový charakter komunikace
- Důraz na rychlost přenosu dat na úkor spolehlivosti
- Spolehlivost zajišťují až koncové uzly, nikoli přenosová část sítě

Omezení a nedostatky TCP/IP

1. Protokoly TCP/IP nezajišťují dostatečnou míru bezpečnosti (v době vzniku koncepce TCP/IP nebyl tento požadavek důležitý, přednost měla efektivnost

přenosu). Nedostatečná bezpečnost spočívá v nešifrovaném přenosu dat, data mohou být odposlechnuta a případně zneužita. Tato nevýhoda protokolů TCP/IP je v současnosti řešena šifrováním na aplikační úrovni, vytvářením zabezpečených tunelů a dalšími mechanismy. Prvky bezpečnosti již v sobě má obsaženy protokol IPv6.

2. Původní koncepce TCP/IP nepočítala s mobilitou uživatelů (cestovní, přenosná IP adresa). IP adresa je vázána na geografické (topologické) umístění zařízení. IPv6 přináší dílčí řešení této problematiky.
3. Nedostatek IP adres. IPv4 vyhradil pro síťovou adresu pouze 32 bitový adresní prostor, který byl ještě v původní podobě členěn na třídy. Toto rozdělení bylo značně nehospodárné a vedlo k hrozícímu vyčerpání adres. Částečným řešením, které problém nedostatku adres oddálilo jsou mechanismus CIDR, subnetting, zavedení privátních IP adres. Zásadním koncepčním řešením je přechod na novou verzi protokolu IPv6.
4. Vlastní charakter přenosu – protokoly TCP/IP jsou orientovány na blokový přenos dat, což naprosto nevyhovuje např. multimediálním přenosům zvuku a obrazu. Řešením tohoto problému jsou nové protokoly podporující přenos v reálném čase (RTP, RSVP).

Standardy TCP/IP

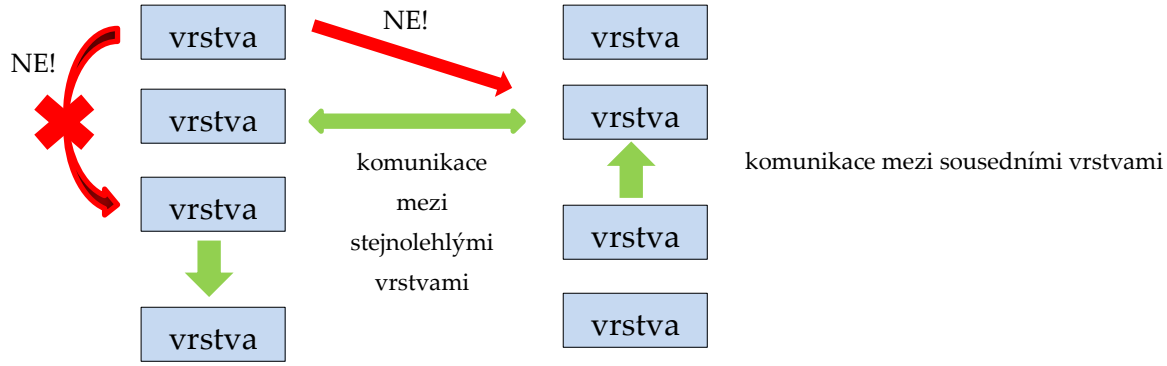
Specifikace jednotlivých protokolů rodiny TCP/IP není proprietární záležitostí (vázanou na konkrétní firmu), je veřejným vlastnictvím. Za využití se tedy neplatí žádné poplatky, specifikace mají podobu veřejně přístupných dokumentů. Každý standard je vydáván jako RFC dokument (Request for Comment), většinou jde o informační materiály, návody a doporučení. Obsah RFC dokumentů je neměnný, dojde-li ke změně ve specifikaci, vydá se nový dokument RFC. Tím pádem mohou existovat různé RFC dokumenty, vztahující se k dané oblasti.

Rozdělení do vrstev

Komunikace v sítích založených na TCP/IP probíhá ve čtyřech vrstvách:

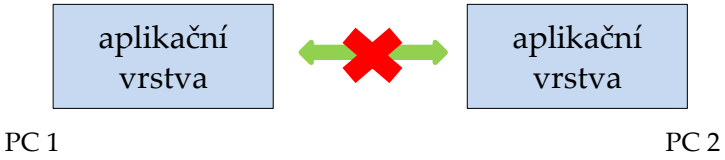
- Vrstva síťového rozhraní
- Síťová vrstva
- Transportní vrstva
- Aplikační vrstva

V koncových uzlech jsou implementovány všechny vrstvy, v přechodových uzlech (směrovače) jsou implementovány pouze spodní dvě vrstvy (vrstva síťového rozhraní a síťová vrstva).
Komunikace probíhá mezi sousedními vrstvami nebo mezi stejnolehlými vrstvami.

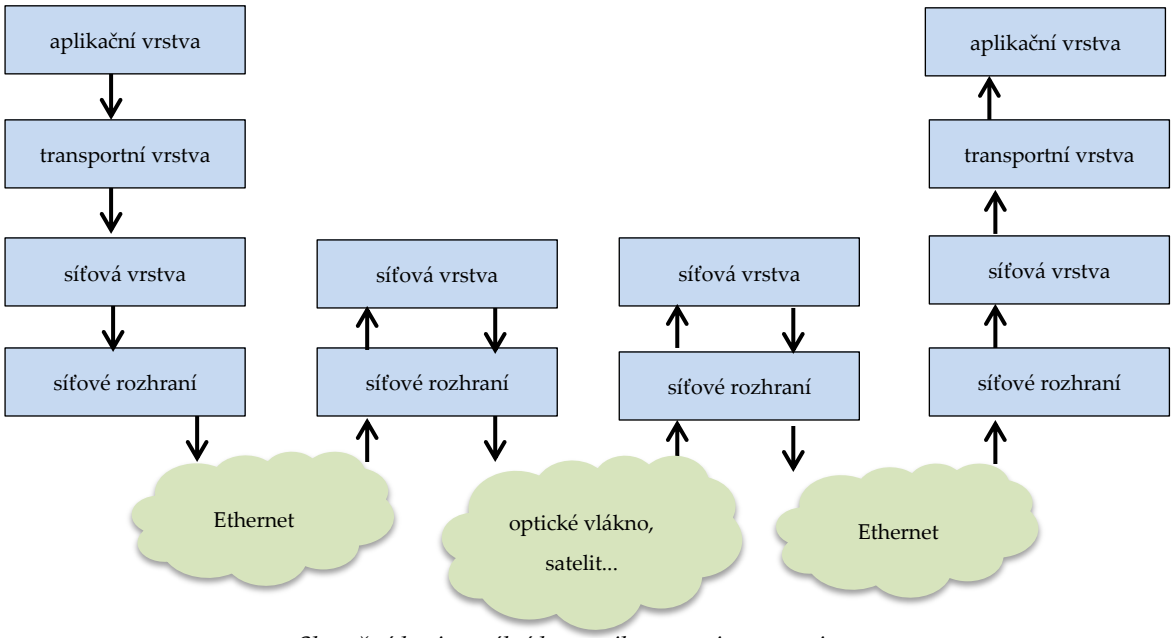


Možné způsoby komunikace v počítačové síti

Horizontální komunikace (mezi stejnolehlými vrstvami) ve skutečnosti neprobíhá na úrovni jiné vrstvy, než vrstvy síťového rozhraní.



Představa horizontální komunikace



Skutečné horizontální komunikace mezi vrstvami

Vrstva síťového rozhraní

Umožňuje přístup k fyzickému přenosovému médiu, je přímo závislá na implementaci, liší se pro jednotlivé přenosové technologie. Tato vrstvu není v rámci TCP/IP blíže specifikována, v rámci TCP/IP pro ni neexistují žádné protokoly.
Přenosové mechanismy používané ve vrstvě síťového rozhraní pochází z použité přenosové technologie.
Přenosové služby používané vrstvou síťového rozhraní slouží k přenosu bloků dat (zvaných v této vrstvě *rámce*) mezi sousedními uzly počítačové sítě.

Síťová vrstva

Primárním úkolem síťové vrstvy je **hledání cesty** pro bloky dat (v této vrstvě zvaných pakety), a to nejen mezi přímými sousedy, ale mezi libovolnými dvěma uzly v síti. Hledá nejvhodnější cestu až k cíli, přitom se nestará o spolehlivost, ale o co nejrychlejší přenos dat. Po nalezení vhodné cesty zajistí postupný přenos paketu přes mezilehlé uzly v cestě, zabalí přenášený paket do rámce a prostřednictvím vrstvy síťového rozhraní předá tento paket přímému sousedovi. V sousedním uzlu rámec přijme opět vrstva síťového rozhraní, ta jej rozbalí a předá získaný paket své síťové vrstvě, která opět najde nejvhodnější cestu k cíli a prostřednictvím své vrstvy síťového rozhraní pošle data k dalšímu sousednímu uzlu (viz. obrázek).
Síťová vrstva zajišťuje pouze nespojovaný, nespolehlivý přenos (co nejrychleji).
Přenosový protokol IP se snaží zakrývat rozdíly v přenosových technologiích nižší vrstvy.
Nejdůležitějším protokolem síťové vrstvy je protokol **IP**, dále jsou na síťové vrstvě k dispozici služební protokoly **ICMP, IGMP, ARP, RARP**.

Transportní vrstva

Tato vrstva a vrstva nadřazená (aplikační) se již nevyskytují na všech síťových uzlech, ale jsou implementovány pouze v koncových uzlech sítě.
Transportní vrstva poskytuje **volitelně** spojovaný a spolehlivý přenos dat, aplikace si může vybrat, zda využije rychlejší, ale nespolehlivý a nespojovaný přenos dat protokolem **UDP** nebo spolehlivý, spojovaný přenos dat protokolem **TCP**.
Transportní vrstva směřuje data přímo aplikacím, které o ně požádaly (nižší vrstvy rozlišují pouze uzel, nikoli jednotlivé aplikace v rámci jednoho uzlu). Kromě protokolů TCP a UDP jsou definovány protokoly DCCP, SCTP, RUDP.

Aplikační vrstva

Je to vrstva aplikací (programů), využívajících síťový přenos dat. Původními službami aplikační vrstvy je elektronická pošta, vzdálené přihlašování a vzdálený přenos dat. Později přibyly další služby, jako je správa sítě, sdílení souborů, sdílení a zpřístupnění informací, identifikace komunikujících partnerů, a další.
K nejdůležitějším protokolům vrstvy patří **FTP, HTTP, HTTPS, www, Telnet, SSH, SMTP, IMAP, POP3, IRC, NFS, SNMP, DNS, DHCP** a další.

Nejdůležitější protokoly architektury TCP/IP

IP protokol

Univerzální přenosový protokol síťové vrstvy, jediný přenosový protokol rodiny TCP/IP. Protokol slouží k nespolehlivému, nespojovanému přenosu dat mezi zdrojovým počítačem a příjemcem. Protokol je implementován v koncových uzlech nb i ve směrovačích. Přenášená data se nazývají IP datagramy neboli IP pakety, každý paket obsahuje hlavičku, ve které nese metadata (řídící informace) a vlastní přenášená data (anglicky payload).
V současnosti jsou paralelně používány dvě verze protokolu, dominuje stále verze IPv4, současně je používána i novější verze IPv6 tam, kde je to možné.

Formát IP datagramu (IPv4):

verze	délka hlavičky	TOS, QoS	celková délka	identifikace	příznaky	offset	TTL	protokol	kontrolní součet hlavičky

adresa odesilatele	adresa příjemce	volby	výplň	data

Hlavička datagramu zabírá 0. až 23. Byte, po hlavičce (od 24. Byte) následuje datová část paketu.

Údaje hlavičky:

- verze — použitá verze (IPv4 nebo IPv6)
- TOS, QoS — třída provozu, požadavky na přenos
- identifikace — jednoznačné určení paketu při fragmentaci (fragmentované pakety mají stejné id)
- příznaky — řízení fragmentace (more fragments, don´t fragment)
- offset — pozice fragmentu v původním paketu

- TTL Time To Live (položka bránící zacyklení paketu, po každém průchodu směrovačem snížena o 1, jakmile klesne na 0 je paket zahozen)
- protokol číslo protokolu podle RFC
- kontrolní součet pokud nesouhlasí, je paket zahozen
- volby doplňující informace a požadavky (obvykle se nepoužívá)

Protokol IP funguje na principu maximální snahy *"best effort"*, pro přenos paketů využívá všech prostředků, které má k dispozici. Jakmile přenosové kapacity přestanou stačit objemu přenášených dat, má protokol IP právo některé pakety zahodit.
Nespojovaný způsob přenosu dat znamená, že není předem vytýčena a vytvořena cesta, po které mají být data přenášena, ale že každý uzel na cestě mezi odesilatelem a příjemcem pro přenášený paket hledá optimální cestu v síti podle momentálního stavu přenosových cest. Dochází tedy k situacím, že je zpráva rozdělená na několik paketů, každý paket putuje k cíli vlastní cestou, přitom pořadí, ve kterém dorazí do cílového uzlu nemusí odpovídat pořadí vysílání paketů.
Nespolehlivost protokolu znamená, že pokud síťová vrstva (IP protokol) obdrží poškozený paket, nestará se o nápravu chyby, ale tento chybný paket zahodí.
Obě tyto vlastnosti umožňují přenášet data s minimální přenosovou režií, maximální rychlostí. Objem dat, která nejsou přenesena (ať už v důsledku nedostatečné přenosové kapacity nebo zahozená poškozená data) je v poměru k přeneseným datům malý.
Požaduje-li aplikace spolehlivý přenos dat, jsou k dispozici protokoly vyšších vrstev, které požadovanou spolehlivost mohou zaručit, síťová vrstva a její přenosový IP protokol fungují principiálně nespolehlivě a nespojovaně.

Adresování a směrování
Každý síťový uzel (síťové rozhraní), používající pro komunikaci protokol IP, má přiřazen jednoznačný síťový identifikátor – IP adresu. Každý přenášený paket v sobě nese informaci o odesilateli a příjemci, tato informace má podobu právě IP adresy odesilatele a příjemce zprávy. Na základě těchto adres provádí směrovače na cestě rozhodnutí o dalším směru pro odeslání paketu – tj. provádí *směrování* (*routing*).

Fragmentace
Protokol IP musí být schopen přenášet datové pakety různými přenosovými cestami. S tím souvisí skutečnost, že maximální velikost datového rámce, kterou je schopna konkrétní vrstva síťového rozhraní přenést může být v různých sítích různá (závisí na velikosti Maximum Transfer Unit *MTU* dané přenosové cesty). Někdy je tedy nutné původní datový paket během přenosu rozdělit (fragmentovat) na menší bloky dat, které je možné přenést. *Fragmentace* paketu probíhá tam, kde je jí zapotřebí, tedy

na směrovači, který zjistí, že takto velký paket není schopný přenést. Fragmentace může být i opakovaná (fragmentace fragmentu). Zpětná defragmentace probíhá až u příjemce (netransparentní fragmentování). Pro určení pořadí jednotlivých fragmentů slouží položka hlavičky *offset*, pro fragmentaci mají dále význam položky *identifikace* (určení, k jakému paketu fragment náleží) a *příznaky* (označení, že se paket nesmí fragmentovat nebo že budou následovat další fragmenty zprávy). Protokol řeší miminální velikost paketu, který by neměl být nikdy fragmentován (576B).

Z principu práce síťové vrstvy vyplývá, že ne všechny fragmenty musí dorazit k cíli, je tedy nutné řešit způsob reakce na ztrátu některého paketu. Sestavení původní zprávy je možné pouze pokud k cíli dorazí všechny pakety, pokud některý nedorazí do určité doby (*timeout*), je celá zpráva zahozena.

ICMP (Internet Control Message Protocol)

Pro generování a zasílání chybových zpráv, diagnostické a testovací účely v sítích byl vyvinut protokol ICMP. Protokol ICMP pracuje nad protokolem IP, takže jsou ICMP pakety pro přenos sítí baleny do IP paketů, ICMP je s IP provázán a musí být povinně s IP implementován. Ztráty paketů nesoucích ICMP zprávy nejsou oznamovány, aby nedošlo k zacyklení.

Formát ICMP paketu

TYPE	CODE	CHECK SUM
ICMP message		

Druhy zpráv, které ICMP generuje (položka TYPE):

- 0 echo reply (odpověď na požadavek, např. ping)
- 3 destination unreachable (další specifikace dle CODE)
- 4 source quench
- 5 redirect
- 6 alternate host address
- 8 echo request
- 9 router advertisement
- 10 router solicitation
- 11 time exceeded (TTL dosáhlo hodnoty 0, např. traceroute)
- 12 parameter problems
- 13/14 time stamp request/reply
- 17/18 adress mask request/reply
- ....

Položka **CODE** dále zpřesňuje význam položky TYPE, např. u time exceeded může jít buď o zacyklení paketu (TTL klesne na 0) nebo vyprší timeout, obě situace spadají do TYPE 11, pomocí CODE rozlišíme, která z těchto situací nastala.

Typické situace, ve kterých dojde k vygenerování ICMP paketu:

- Zacyklení paketu – při směrování datagramů v sítích může dojít k jejich zacyklení. Aby pakety nezůstávaly v sítích donekonečna, mají v hlavičce položku TTL (time to live), která je při každém průchodu směrovačem dekrementována. Jakmile položka TTL klesna na hodnotu 0, má směrovač právo takovýto paket ze sítě odstranit. Při zahození paketu je směrovač povinen o této skutečnosti informovat odesilatele (vyšle ICMP zprávu)
- Vypršení doby odezvy (timeout) – při sestavování paketů u příjemce nejsou do určené doby doručeny všechny pakety zprávy. Celá zpráva je zahozena, o skutečnosti je informován odesilatel, do odesilaného paketu je vložen začátek zahozeného paketu, aby mohl odesilatel zjisti příčinu nedoručení.
- Nedostupný uzel (destination unreachable) – další situace, ve kterých nemohl být paket doručen, tj. nedostupná síť nebo uzel, neexistující adresy nebo porty, překročení maximální velikosti paketu, pokud je zakázána fragmentace, chyby routerů, nesprávné cesty, zakázaný přístup pro daný požadavek apod.
- Testování dostupnosti, počtu směrovačů na cestě, doby přenosu (echo request) – tuto zprávu může poslat kterýkoli směrovač nebo koncový uzel, volbou velikosti paketu lze testovat i fragmentaci.
- Přetížení směrovače (source quench) – např. při souběhu požadavků na směrovač, který překročí kapacitu směrovače, směrovač musí začít zahazovat pakety. Jednoduché směrovače posílají source quench po každém paketu, který dostanou jsou-li přetíženy, dokonalejší směrovače posílají source quench jen těm odesilatelům, od nichž přichází pakety s podstatným vlivem na přetížení, v ideálním případě generuje směrovač source quench ještě dříve, než dojde k zahlcení. Source quench je pouze informační zpráva, neřeší co dělat se zahlcením, je na rozhodnutí adresáta zprávy source quench, jak na situaci bude reagovat.

ARP (Address Resolution Protocol)

Slouží k překladu IP adres na MAC adresy metodou dotaz – odpověď. Je použitelný pouze tam, kde lze použít *broadcast* (všesměrové vysílání).
Funguje tak, že pošle dotaz všem zařízením v dané síti, ten koho se dotaz týká na něj odpoví (uzel, který rozezná svou IP adresu). Dotazy jsou vkládány do linkových rámců a rozesílány broadcastem (v adrese samé 1). Odpověď je již cílená (individuální, nikoli broadcast).

ARP dotazy jsou cacheovány (po dobu cca 20 minut), při dotazu na danou IP se ARP nejprve podívá do cache, teprve není-li adresa v cache nalezena, posílá broadcast.

Formát ARP zprávy:

HW ADDRESS TYPE	PROTOCOL ADDRESS TYPE	HADDR LEN	PADDR LEN	OPERATION
SENDER HW ADDRESS	SENDER PROTOCOL ADDRESS	TARGET HW ADDRESS		TARGET PROTOCOL ADDRESS

- HW ADDRESS TYPE — 1 v případě Ethernetu
- PROTOCOL ADDRES TYPE — 0x800 v případě IP adresy
- HADDR LEN — délka HW adresy v oktetech
- PADDR LEN — délka IP adresy
- OPERATION — 1 dotaz, 2 odpověď
- SENDER HW, PROTOCOL ADD — adresy odesilatele dotazu nebo odpovědi
- TARGET HW ADDRESS — v žádosti nastavená na samé nuly, v odpovědi nese správnou hodnotu

Zpracování ARP dotazu:

- Každý uzel, který přijme broadcast vysílání se žádostí o identifikaci adresy nejprve do své cache uloží (nebo aktualizuje) vazbu mezi HW a protokolovou adresou (IP) odesilatele
- Podívá se, zda jde o dotaz nebo odpověď (pole operation)
- Jde-li o dotaz, zjistí, zda se ho týká (porovná pole target protocol address se svojí adresou)
- Sestaví ARP odpověď
  - Vyplní protocol adresy sender a target
  - Do pole sender hw address doplní svoji HW adresu (MAC)
  - Pole operation nastaví na 2
  - Pošle cíleně tazateli
- Jde-li o odpověď, odpověď použije (předcházel jí dotaz uzlu na adresu)

Zvláštní variantou ARP je tzv. **proxy ARP** – uzel vystupuje jménem jiného uzlu, např. při mobilní IP adrese, v případě uzlu na pomalém jednobodovém spoji apod.

Pro opačný překlad (HW adresy na IP adresu) slouží protokol **RARP**. Tento protokol byl nahrazen BOOTP a DHCP a není používán.

IGMP (Internet Group Management Protocol)

Protokol pro podporu *vícesměrového vysílání* (*multicastingu*) v rámci přenosů protokolem IP. Jde o služební protokol (podmnožinu) protokolu IP, pakety IGMP jsou pro přenos baleny do IP datagramů.
Protokol slouží pro výměnu informací o členství (přihlašování, odhlašování) ve specifických skupinách vícesměrového vysílání, verze 3 umožňuje navíc zadat na straně hostitele, ze kterých zdrojů chtějí přijímat vícesměrové vysílání, respektive zadat, ze kterých zdrojů vícesměrové vysílání nebude přijímáno.

Formát IGMP zprávy:

TYPE	CODE /MAX RESPONSE TIME	CHECKSUM
identifikátor		
adresa multicastové skupiny		
klíč pro přístup do privátních skupin		

Pole TYPE:

- 11 dotaz na členy skupiny
- 12 požadavek na členství ve skupině (IGMPv1)
- 15 sledovací zprávy CISCO
- 16 požadavek na členství ve skupině (IGMPv2)
- 17 opuštění skupiny (IGMPv2)

Pole CODE upřesňuje údaje v poli TYPE, hodnota CODE souvisí s polem TYPE. V poli může být hodnota maximálního času odpovědi užívaná pro timeout, do kterého musí členové opakovat požadavek na členství ve skupině.

TCP (Transmission Control Protocol)

Základní protokol transportní vrstvy. Umožňuje aplikacím vytvořit spojení a přenášet data spolehlivě a spojovaně (nabízí volitelnou nadstavbu se spolehlivým přenosem). Protokol garantuje spolehlivé doručení dat ve správném pořadí, protokol navíc prostřednictvím portů rozlišuje různé aplikace spuštěné na stejném počítači (např. webový server, emailový server, ftp).
TCP využívá pro odesílání paketů nespolehlivý protokol IP, spolehlivost pak zajišťuje kontrolou doručení paketu (pomocí potvrzování), pakety dále na straně příjemce protokol TCP přeuspořádává pro zajištění správného pořadí doručení.

Hlavička protokolu TCP

Zdrojový port	Cílový port	Číslo sekvence	Potvrzovací bajt
offset	příznaky	okénko	Kontrolní součet
Urgent pointer	volby	výplň	

Pro rozlišení komunikujících aplikací používají protokoly transportní vrsty *čísla portů*. Porty jsou rozděleny do tří skupin:

- Dobře známé porty (seznam těchto portů je přiřazován organizací IANA). Př: FTP port 20 a 21, SMTP port 25, HTTP port 80, DNS port 53
- Registrované porty
- Dynamické porty

TCP je spojovaná transportní služba, musí tedy před vlastním odesíláním dat navázat spojení s komunikačním partnerem. Toto navázání spojení má tři fáze (*three-way handshake*). V průběhu potvrzování se obě strany dohodnou na číslu potvrzování a číslu sekvence. Pro navázání spojení se vysílají datagramy s příznaky SYN a ACK.

Třícestný handshake

1. Klient vysílá na server požadavek na komunikaci s příznakem SYN, náhodně vygenerovaným číslem sekvence (x) a číslem potvrzování 0.
2. Server odesílá klientovi datagram s číslem potvrzování x+1 a náhodně vygenerovaným číslem sekvence (y), příznak zprávy nastaví na SYN, ACK.
3. Klient odešle datagram s příznakem ACK, číslem sekvence x+1, číslem odpovědi y+1.

Obě strany si pamatují číslo sekvence své i protistrany. Používají se i pro další komunikaci a určují pořadí paketů.

Ukončení spojení probíhá podobně jako jeho navázání. Používá se k tomu příznaků FIN a ACK:

1. Klient odešle datagram s nastaveným příznakem FIN
2. Server odpoví datagramem s nastaveným příznakem ACK
3. Server odešle datagram s nastaveným příznakem FIN
4. Klient odpoví s nastaveným příznakem ACK

Teprve po těchto čtyřech krocích je spojení ukončeno.

Protokol TCP vytváří při přenosu iluzi proudu (*stream*) jednotlivých bytů. Na straně odesilatele protokol TCP shromažďuje (bufferuje) jednotlivé byty do vyrovnávací paměti a po jejím naplnění odesílá celý takto vytvořený blok, nazývaný segment. Na

straně příjemce je poté přijatý segment uložen do vyrovnávací paměti a aplikaci je poskytován ve formě jednotlivých bytů. Protokol TCP se tímto sdružováním dat do segmentů snaží zefektivnit přenos (snížením režijních nákladů na přenos) a optimalizovat využití přenosových cest. Velikost odesílaného bloku je závislá také na *MTU* přenosových cest (maximální přenosová jednotka). Alternativně protokol nabízí okamžité odeslání dat bez předchozího naplnění vyrovnávací paměti (využívá např. Telnet).

Potvrzování v rámci protokolu TCP
Pro zajištění spolehlivosti přenosu je nutná existence mechanismu, který rozezná chybný blok dat a vynutí opětné odeslání dat. Pro tento účel existuje několik různých metod potvrzování (*acknowledgment*). Protokol TCP využívá *kontinuální pozitivní potvrzování*, tj. potvrzuje úspěšně přijatá data, na chybně přijatá data nijak neupozorňuje. V případě, že klient do daného časového okamžiku (timeout) neobdrží potvrzení o přijetí dat, automaticky znovu odesílá data. Metoda, kterou používá protokol TCP je též zvaná *metoda okénka*, odesilatel může odeslat další data dříve, než obdrží potvrzení o přijetí dat předchozích. Velikost okénka (množství předem odeslaných bloků) je proměnlivá, v případě, že dojde k chybě ve spojení, přechází se na jednotlivé potvrzování a postupně se velikost okénka zvětšuje.

UDP (User Datagram Protocol)

Některé aplikace upřednostňují rychlost doručování paketů před spolehlivým doručením každého jednotlivého paketu (např. internetové rádio, VoiP, real-time online hry apod.). Pro tyto aplikace se více než protokol TCP hodí protokol UDP který nemění kvalitu přenosových služeb, ke službám protokolu IP přidává pouze kontrolní součty a možnost rozlišit pomocí portů konkrétní aplikaci, pro kterou je paket určen. Jeho největšími výhodami jsou rychlost a efektivita.
Zajištění potřebné míry spolehlivosti, detekce a případná náprava chyb jsou plně zajišťovány aplikací, která protokol UDP využívá.

Hlavička protokolu UDP

zdrojovýport	cílový port	délka	kontrolní součet

Protokol UDP je bezestavový, pole zdrojový port nemusí být vyplněno (může být nastaveno na 0), je možné také vynechat kontrolní součet.
UDP je používán řadou služeb, jako je DNS, DHCP, SNMP, RIP.

Shrnutí

Protokoly rodiny TCP/IP jsou standardem komunikace v počítačových sítích. Architektura TCP/IP zahrnuje jednak rozdělení komunikace do jednotlivých vrstev – TCP/IP rozlišuje 4 vrstvy, a to vrstvu síťového rozhraní, vrstvu síťovou, vrstvu transportní a vrstvu aplikační – jednak protokoly definované na jednotlivých vrstvách. V koncových uzlech jsou implementovány všechny uzly, v přechodových uzlech pouze vrstva síťového rozhraní a vrstva síťová. Komunikace probíhá vždy mezi sousedními vrstvami, případně mezi vrstvami stejnolehlými, a to na základě protokolů dané vrstvy.
Vrstva síťového rozhraní umožňuje přístup k přenosovému médiu, její implementace je závislá na konkrétní přenosové technologii a v rámci TCP/IP k ní neexistují žádné protokoly.
Funkcí síťové vrstvy je hledání cesty mezi pro bloky dat (pakety). Síťová vrstva zajišťuje pouze nespolehlivý nespojovaný charakter komunikace tak, aby přenos dat probíhal co nejrychleji. Nejdůležitějším protokolem síťové vrstvy je protokol IP, který je podporován služebními protokoly ICMP, ARP a dalšími.
Transportní vrstva je implementována pouze v koncových uzlech, jejím úkolem je poskytovat volitelně spolehlivý spojovaný přenos dat. Transportní vrstva pomocí portů rozlišuje a směřuje data přímo pro konkétní aplikaci, která o data žádá. Hlavními protokoly transportní vrstvy jsou TCP (pro spolehlivý přenos dat) a UDP (nespolehlivý, nespojovaný přenos).
Aplikační vrstva je vrstva aplikací, využívajících síťový přenos dat. Základní služby, které aplikační vrstva nabízí je elektronická pošta, vzdálený přenos dat, sdílení souborů, správa sítě a další. Protokoly aplikační vrstvy jsou popsány v samostatné kapitole.
Architektura TCP/IP je použitelná v sítích založených na různých technologiích (Ethernet, Wi-fi...) a klade důraz na rychlost přenosu dat na úkor spolehlivosti jejich doručení. Tento princip se nazývá princip nejlepší snahy (best effort).

Kontrolní otázky:

1. Jmenujte principy, na kterých je založena architektura TCP/IP.
2. Jaké jsou nedostatky a omezení TCP/IP a jak se tyto nedostatky dají řešit?
3. Jmenujte základní vrstvy architektury TCP/IP.
4. Jaká je základní úloha vrstvy síťového rozhraní?
5. Jaké protokoly jsou definovány na vrstvě síťového rozhraní?
6. Co je základní úlohou síťové vrstvy?
7. Jaké protokoly jsou definovány na síťové vrstvě?
8. Jaký způsob přenosu dat nabízí transportní vrstva?
9. Jaké protokoly transportní vrstvy znáte?
10. K čemu slouží aplikační vrstva?

11. Popište formát IP datagramu verze 4
12. Jaké jsou největší výhody protokolu IP?
13. Jakým způsobem jsou označeny síťová rozhraní v TCP/IP?
14. Co je to fragmentace?
15. Kdy je nutné paket fragmentovat, kdo tuto fragmentaci provádí?
16. Co je to MTU?
17. Podle kterého údaje jsou identifikovatelné fragmentované pakety, které patří k sobě?
18. Co se děje, nedorazí-li k cíli všechny fragmentované části původního paketu?
19. K čemu slouží protokol ICMP?
20. Jmenujte alespoň 4 situace, při kterých je vygenerován ICMP paket.
21. Která služba (program) využívá protokol ICMP?
22. K čemu slouží protokol ARP?
23. Jakým způsobem ARP pracuje?
24. Jak se jmenuje protokol pro podporu multitaskingu v IPv4?
25. Jaký typ spojení nabízí protokol TCP?
26. Jakým způsobem TCP zajišťuje spolehlivost?
27. Jak vypadá hlavička TCP protokolu?
28. Popište třícestný handshake
29. Jaký typ spojení nabízí UDP?
30. Popište hlavičku UDP.
31. Které služby UDP používají?

Zdroje:

Sochor Tomáš: Počítačové sítě II, skripta pro distanční studium, vydala Ostravská univerzita v Ostravě, Přírodovědecká fakulta, Ostrava 2009

User Datagram Protocol – Wikipedia [online], dostupné z: http://cs.wikipedia.org/wiki/User_Datagram_Protocol, [cit. 03/2012]

Transmission Control Protocol – Wikipedia, [online], dostupné z: http://cs.wikipedia.org/wiki/Transmission_Control_Protocol , [cit. 03/2012]

IGMP Type Numbers [online], poslední update 16.9.2011, dostupné z: http://www.iana.org/assignments/igmp-type-numbers, [cit. 03/2012]