TCP/IP

Z ISO/OSI vychází i množina protokolů TCP/IP. Protokol TCP/IP vznikl původně jako komunikační protokol ministerstva obrany USA pro sjednocení počítačové komunikace v rámci ARPANET. Slouží ke komunikaci především v heterogenních sítích. Dnes je součástí prakticky všech operačních systémů (původně byl navrhován hlavně pro UNIX) a je využit ke komunikaci i v síti Internet. Z těchto důvodů vzrůstá jeho význam jako celosvětového standardu.

Model TCP/IP je nezávislý na přenosovém mediu a je určen jak pro WAN tak i pro LAN, jak pro sériové linky, koaxiální kabely, tak i pro vysokorychlostní optické sítě. Je užíván v heterogenní síti (původně určené pro UNIX) Internet. Je to soustava sítí s IP protokolem tvořená mezisíťovým počítačem. Jednotlivé podsítě mohou být různé (Ethernet, X.25, ..).

TCP/IP (Transmission Control Protocol/Internet Protokol) předpokládá, že na nižších vrstvách jsou pouze nespolehlivé přenosové služby. Zajištění spolehlivosti dělají vyšší vrstvy a to jen při jejich vyžádání.

Rodina protokolů TCP/IP předpokládá existenci čtyř **vrstev:**

Aplikační vrstvy

Transportní vrstvy

Síťové vrstvy

Vrstvy síťového rozraní Přehled architektury TCP/IP

OSI	TCP/IP	Aplikace a protokoly
7. aplikační 6. presentační 5. relační	Aplikační vrstva	telnet FTP TFTP SMTP RIP DNS Ostatní
4. transportní	Transportní vrstva	TCP UDP
3. síťová	Síťová vrstva	IP ICMP ARP RARP
2. linková 1. fyzická	Vrstva síťového rozhraní	token ring ethernet jiné typy protokolů

Aplikační vrstva (Application Layer)

V této vrstvě jsou provozovány základní aplikace v rámci TCP/IP. Aplikační vrstva zajišťuje přenos a srozumitelnost zpráv. (Podle modelu OSI sdružuje tyto vrstvy: Aplikační (7), Prezentační(6), Relační(5)).

Tato vrstva využívá služby

- **TELNET -** což je vlastně emulátor terminálu. Umožňuje pracovat na vzdáleném počítači tak, jako by to byl terminál nebo přímo váš počítač. Využívá služby TCP. - **FTP** File Transport Protokol - umožňuje přenášet soubory ze vzdálených disků (virtuálně je přiřadí k počítači). Využívá TCP. Jeho klonem je TFTP- trivial FTP- u UDP protokolu.
- **SMTP** Simple Mail Transfer Protokol - využívá se pro E-mail je sedmi bitový (ASCII)
- **WWW**
- **RIP** Routing Information Protokol – směrovaí protokol, který předává informace o směrování.
- **DNS** Domain Name Server - konvertuje logické adresy na fyzické. - **a další ….**

Transportní vrstva (Transport Layer)

Obsahuje protokoly: TCP a UDP

TCP protokol zajišťuje **navázání** spojení, zaručení **celistvosti** zprávy a ukončení spojení. Pokud to požaduje aplikace, tato vrstva pro ni zajistí **spolehlivost**, tj. změní nespolehlivý charakter síťové služby na spolehlivý. (komunikuje pomocí portů)

V opačném případě (kdy aplikace nevyžaduje spolehlivost od transportní vrstvy nebo vyžaduje **rychlost** je použit protokol **UDP** (User Datagram protokol), který je jen jednoduchou obálkou nad síťovou vrstvou. UDP nevyžaduje navázání spojení.

Síťová vrstva (Internet Layer)

Na této vrstvě pracují protokoly IP, ICMP a na rozhraní se síťovou vrstvou pracují protokoly ARP, RARP.

IP protokol se snaží co nejrychleji doručit data (datagram) přes případné mezi uzly až k jejímu koncovému adresátovi, proto nabízí pouze *nespolehlivou* přenosovou službu, a to *nespojovaného* charakteru, tzn. IP protokol je nespojovaný nespolehlivý protokol s částečnou detekcí chyb. Tato detekce se týká pouze kontrolního součtu hlavičky protokolu. IP protokol má tyto funkce:

- adresování stanic v internetové (síťové) vrstvě
- definice struktury IP datagramu
- Směrování datagramů
- Propojení internetové a transportní vrsty. Určitým protokolům jsou přiřazeny pevná čísla portů (TCP -6, UDP - 17)
- Fragmentace a sestavení datagramů podle MTU - maximum Transfer Unit - maximální délka datagramu (Ethernet 1500B, seriový port 296B)

ICMP Internet Control Message Protokol přenáší zprávy o **chybách** a řídící zprávy (např. příkaz Ping). Je pevnou částí protokolu IP (využívá služeb IP) a proto je také nespolehlivý a nespojovaný protokol. Nejdůležitější zprávy jsou

- destination unreacheble - nedostupnost cílové stanice nebo služby
- Source Quench - zpráva od příjemce nebo routeru pro zpomalení vysílání dat
- Redirect požadavek brány nebo routeru na přímější cestu k cílové stanici - žádost o přesměrování
- Echo request a echo replay - pro odezvu ping - určuje dostupnost stanice.
- žádost o ozvěnu a odpověď s ozvěnou
- Parametr problem - když je hlavička nečitelná (chybná) - chybný parametr

Pomocí ICMP lze zjišťovat propustnost a dostupnost sítě. Pro ověření dostupnosti slouží utilita **PING** od Packet Internet Grouper. Ta vysílá pomocí servisní protokolu ICMP sérii testovacích paketů, které příjemce okamžitě vrací zpět. Změření doby odezvy se odvozuje dostupnost konkrétního uzlu.. Hodnota je udávána v ms a její hodnoty jsou jednotky až tisíce. Ping se ve Windows spouští z okna DOS, v Unixu z příkazového řádku

Další utilita pro zjištění topologie sítě je **traceroute** (pro Unix, Linux)**,** nebo **Tracert** pro DOS a Windows, který může najít požadovaný uzel i přes 20 meziuzlů. Programy dělají standardně 3 pokusy o ping na jednotlivé uzly. Podle jmen jednotlivých uzlů z odezvy se dá rekonstruovat cesta.

ARP Address Resolution Protokol zabezpečuje pro IP fyzické adresy (MAC – Medium Access Control) podle logické IP adresy. Proto ARP vyšle paket s logickou IP adresou všem uzlům, a ten, který ji u sebe najde předá zpět fyzickou adresu. Komunikace probíhá následovně:

Předpokládejme, že stanice A potřebuje komunikovat se stanicí B. Stanice A ví jakou má stanice B IP adresu, ale neví její MAC adresu, kterou ale vědět musí, aby jí mohla v prostředí Ethernet poslat datové rámce užívající právě MAC adresu. Zde se ujímá své role ARP Stanice se podívá do tzv. ARP cache, což je tabulka IP adres a jim příslušejících MAC adres. Tuto tabulku můžeme zjistit příkazem arp –a jak v prostředí Windows tak i Linux. Pokud zde požadovaný záznam nenalezne, vyšle ARP broadcast. Tento broadcast je přečten všemi stanicemi v síti. Stanice, která zjistí, že IP adresa v ARP broadcastu je právě její, vyšle zpět ARP reply (odpověď) obsahující její hardwarovou adresu. V našem případě tedy stanice B pošle svoji MAC adresu. S touto informací je již stanice A schopna vytvořit patřičný ethernetový rámec. A může probíhat komunikace. Při dalších pokusech o spojení se již nevysílá ARP broadcast, jelikož je MAC adresa již uložena v ARP cache. ARP protokol je protokol 3. vrstvy podle OSI a je tedy na stejné úrovni jako IP protokol, má však svůj vlastní typ rámce.

RARP Reverse ARP - zjišťuje logickou adresu k fyzické (obdobně jako APR). Překlad tímto směrem se využívá podstatně méně časteji. Využívá se například při zpětné kontrole stanice které DHCP server přidělil adresu.

Vrstva síťového rozhraní (Network Interface Layer)

Zajišťuje přenos rámců (frame) mezi dvěma přímo propojenými počítači. V této vrstvě jsou definované metody přístupu na medium (od koaxiálního kabelu až po optiku).

Jelikož zde velmi záleží na konkrétní přenosové technologii (Ethernet, Token Ring, dvoubodový zdroj, telefonní linka apod.), TCP/IP tuto vrstvu nijak blíže nespecifikuje. (Vrstvy 1 - Fyzická a 2 - Spojová).

V souvislosti s protokoly TCP/IP a jednotlivými vrstvami modelu se rozlišují názvy přenášených jednotek podle toho jak se váží na jednotlivé vrstvy.

Rámec - váže se na vrstvu síťového rozhraní a je základní entitou komunikačního media (např. Ethernetu)

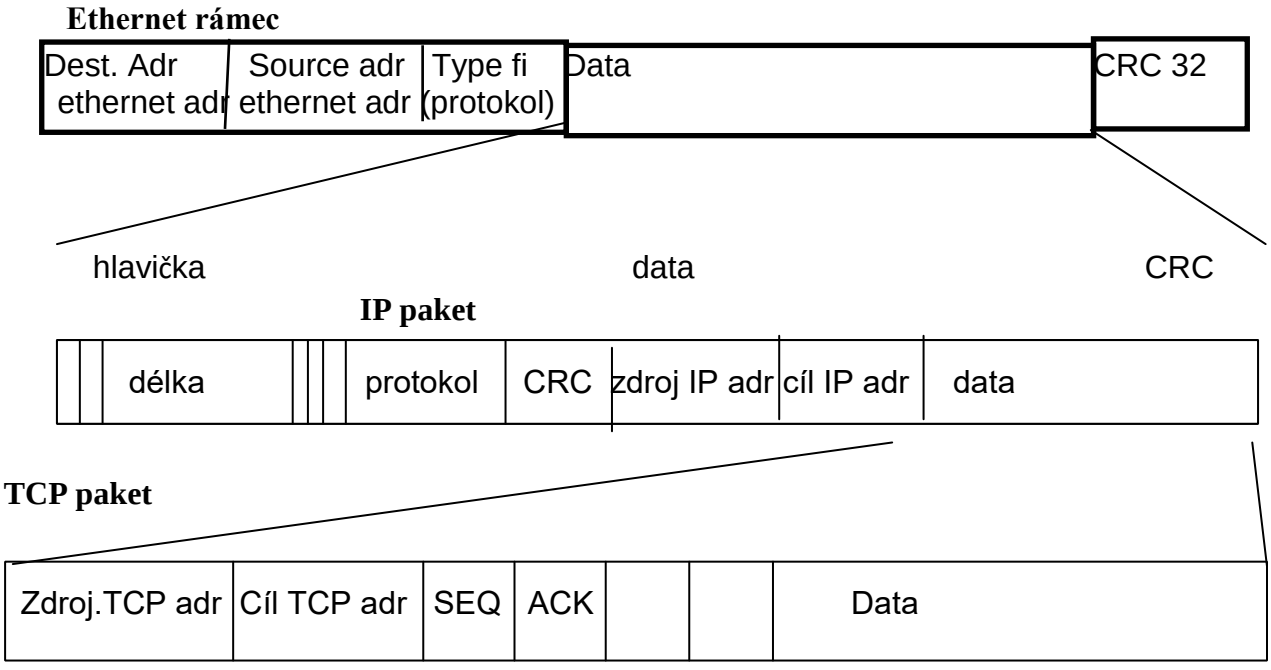
Datagram - internetová vrstva (IP, UDP) - datové kvantum vyměňované mezi stanicemi

Segment - transportní vrstva (TCP) - proud dat, který je dělen na datagramy.

Paket - obecně, bez návaznosti na konkrétní vrstvu

Zpráva - aplikační vrstva

Příklady struktury paketů:



Adresy v TCP packetu zajišťují navázání spojení mezi aplikacemi (URL adresy)

Adresace v sítích TCP/IP

Adresování má 3 úrovně a tedy 3 druhy základních adres.

1. Ethernet adresa (MAC adresa, linková adresa) - 6 Bytů – adresa je pevně vestavěná v adaptéru (síťové kartě, …) a je pro každý adaptér jedinečná a překládá se pomocí protokolů ARP / RARP na IP adesu a zpět. Skládá se z části udávající výrobce adaptéru a z části označující konkrétní adaptér. Např.: 00-14-85-20-F5-D5

2. IP adresa – 32 bitů (podrobněji níže)
3. Adresa v doménovém tvaru. Transformaci zajišťuje Name server BIND (Berkeley Internet Domain Server) nebo DNS (Domain Name Systém/Service), jedná se o stromovou strukturu DNS serverů kdy kořenové uzly jsou replikovány.

IP Adresy

Každá klientská stanice musí mít svou pevně stanovenou identifikaci, tedy IP adresu. IP adresa spolu s číslem portu jednoznačně identifikuje počítač a aplikaci, které mají být předána data. Cílovou IP adresou, zdrojovou IP adresou, zdrojovým a cílovým portem je definováno spojení mezi počítači. Prvních **1024** adres portů je **pevn**ě dáno a nesmí být měněno. Např číslo 21 odpovídá FTP, 23 telnetu, 161 SNMP a pod. IP adresa je napevno přidělena se serverem nebo je přidělována automaticky.

DHCP (Dynamic Host Configuration Protokol) server, který je součástí serverových OS přidělí na požádání připojující se stanici IP adresu ze svého seznamu. Ta může být i dynamicky měněna. DHCP server má svoji vlastní IP adresu a z povoleného rozsahu IP adres je přiděluje na základě klientských požadavků. Celý protokol pracuje systémem DISCOVEROFFER-REQUEST-ACK.

DHCP zjednodušuje manuální nastavení stanic a centralizuje přehled o dostupných IP adresách a připojených počítačích. Je možné jej využít i když je třeba připojit více počítačů k Internetu než je dostupných IP adres a je malá pravděpodobnost, že v jednom okamžiku budou žádat všechny počítače přístup k Internetu, což by v takovém případě znamenalo, že některé počítače budou mít jednoduše smůlu a na Internet se nedostanou.

Takovému stavu se dá předejít použitím proxy serveru, který pod jedinou IP adresu „schová“ celou síť. Počítače v síti pak mají přiřazeny vlastní IP adresy. Když chtějí navázat komunikaci se serverem v Internetu pak mají v konfiguraci nastaveno používat proxy server pro zprostředkování přístupu na Internet. V takovém serveru se příchozí požadavky s určitými IP adresami stanic převádí na IP adresu proxy serveru s číslem portu, který je zaznamenán do tabulky ke zpětnému převodu adresy na stanici, která si komunikaci vyžádala. Server tedy převezme požadavek na sebe a vyřídí jej. Při odezvě od Internetového serveru pak proxy server porovná číslo cílového portu s tabulkou, kterou si udržuje a rozezná tak, na kterou stanici má zpět pakety přeložit a přeposlat a učiní tak.

IP adresa se zapisuje dekadicky po bytech oddělených tečkami (celkem 32bitů) má tvar 255.255.255.255 který označuje jak síť, tak i počítač (Ethernet má 48 bitovou adresu - MAC). Každá adresa může sloužit jen pro jednu fyzickou síť. Proto je nutné interní sítě upravit tak, aby se z venku jevily jako síť jediná. Jednotlivé segmenty sítě se propojit pomocí směrovače (routeru), kde jednomu portu se přidělí IP adresa, nebo pomocí softwareového routeru na serveru.

IP adresy se standardně dělí do několika tříd podle toho jaká část adresy identifikuje síť a jaká počítač.

A:	0nnnnnnn.H.H.H	0.0.0.1 až 127.255.255.255
B:	10nnnnnn.N.H.H	128.0.0.0 až 191.255.255.255
C:	110nnnnn.N.N.H	192.0.0.0 až 223.255.255.255

Další třídy (D, E, F) jsou pro speciální účely např. posílání multipaketů nebo jsou rezervovány pro jiné účely.

V adresaci existují také zvláštní adresy:

0.0.0.0 vlastní adresa . Používá se u startu bezdiskových stanic, kdy ještě není známa IP adresa. Brány ani směrovače ji nepropouští.
255.255.255.255 hromadná - oběžníková- adresa. Paket dostanou všechny počítače lokální sítě.
HostID=0 číslo celé sítě.
127.0.0.1 číslo Loopbacku každého počítače pro spolupráci procesů na jednom počítači. Slouží také pro ping.
ve třídě A 10.x.x.x ve třídě B 172.16.0.0 až 172.31.255.255. ve třídě C 192.168.0.0 až 192.168.255.255 jsou určeny pro vnitřní adresy lokálních sítí, nejsou tedy obsazeny v internetu.

V případech kdy nepotřebujeme celý rozsah nějaké třídy nebo naopak je třeba spojit více adres stejné třídy pro zvětšení rozsahu existují techniky jako:

Podsítě (subneting) - část hostID adresy se používá pro označení podsítě Maska
Maskou rozlišujeme číslo sítě a počítače. 1 – síť, 0 - počítač.

Např. MASK 255.255.0.0 určuje první 2 byty pro číslo sítě.
Ve zbývajících adresách lze určit číslo podsítě, a to podle rozdílu cifer ve třídě adresy a skutečně maskou definovaného počtu bitů.

Př.
Adresa 129.8.23.98 určuje třídu B (10.....) . Pro
masku 255.255.240.0
11111111.11111111.11110000.00000000
určuje adresa 129.8.23.98 adresu ve třídě B, kde je tedy číslo
sítě a podsítě
10000001.00001000.0001hhhh.hhhhhhhh
a srovnáním se třídou B
10nnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh vychází
10000001.00001000 číslo sítě
0001 číslo podsítě
0111.01100010 číslo počítače

CIDR – umožňuje spojování několika menších adres (např. více C dohromady, kdy B je zase příliš velká). CIDR masku musí znát i všechny routery.

IPv6

Klasické IP adresy označované jako IPv4 přestávají svým rozsahem stačit. Dochází tedy k postupnému zavádění IPv6. 128 bitové adresy (nedělí se do tříd) umožňují adresovat 4miliardkrát větší prostor než IPv4. Místo všesměrových zpráv nabízí IPv6 hromadné

(multicast) zprávy a zprávy anycast. IPv6 zjišťuje na vysílacím počítači maximální možnou velikost paketu na celé trase a pak rozdělí data do paketů odpovídající této velikosti, aby se nemusely na trase nikde dále dělit. Dělení paketů způsobuje zpoždění, neboť jejich opětovné složení musí čekat až dojdou všechny části paketu. (Ethernet má 1024 a ATM jen 53 bajtové
pakety). Při zavádění se počítá s paralelním adresováním IPv4 a IPv6 Příklad adresy:

```
3ffe:ffff:1::baf/64
```

Zapisuje se hexadecimálně po dvojicích bytů pokud mezi : chybí znaky byly vynechány nuly. Číslo za lomítkem udává velikost prefixu (zleva) což je adresa sítě.

Směrování v sítích TCP/IP

Přímé směrování – je využito pokud odesílatel může přímo zjistit MAC adresu (pomocí ARP protokolu) v rámci jedné sítě. Pak může přímo poslat paket k cílovému počítači.

Nepřímé směrování – pokud je IP adresa příjemce mimo síť odesílatele je paket odeslán (směrován) na síťový prvek – směrovač (router). Směrovač který má ve své síti patřičnou cílovou IP adresu nalezne pomocí ARP adresu MAC.
Pro směrování se využívá různých technik a protokolů jako jsou RIP, OSPF apod.
RIP (Routing information protocol) – jednoduchý protokol kde jako směrovací metrika slouží pouze počet směšovačů v cestě (hops), snaží se tedy doručit paket přes nejmenší počet přeskoků (maximum je 15 pak se pakety ztrácí). K tomuto slouží směrovací tabulky které jsou opakovaně vysílány RIP na všechny porty. Uzel zná distance vektor a zná tedy ohodnocení cesty sousedních uzlů.
OSPF (Open Shortest Path First) – link state routing, kdy router zná topologii sítě a počítá nejkratší cestu pomocí kostry stromu.
Pro WAN pak slouží další protokoly jako EGP, BGP.

PING a TRACERT

Jde o službu, která nejen ověřuje funkčnost připojení k Internetu, ale umožňuje i otestovat trasy k jednotlivým serverům. To znamená zjistit jaká je např. přenosová rychlost spojení s daným serverem, kudy k němu vede cesta, nebo jak dlouho jsme byli tento měsíc připojeni a kolik to stálo.

*PING adresa_počíta*č*e.doména* Příkaz ohlásí IP adresu cílového počítače a následně mu pošle 4 výzvy. U každé zobrazí, za jakou dorazila odpověď (časy jsou milisekundách). Na závěr shrne, kolik odpovědí dostal, a jaký je nejlepší, nejhorší a průměrný dosažený čas (také se ale dozvíte čtyřikrát jen to, že byl vyčerpán časový limit).

*TRACERT adresa_počíta*č*e.doména* Postupuje se po jednotlivých krocích směrem k cíli. Bere jeden směrovač za druhým a pošle mu vždy 3 výzvy. V každém řádku protokoluje je tedy pořadové číslo směrovače, pak 3 dosažené časy odezvy, a nakonec IP adresa příslušného směrovače.