

Model TCP/IP

- Referenční model ISO/OSI je velmi komplexní, tudíž složitý, a příliš teoretický. Postupně bylo vytvořeno několik zjednodušených variant, z nichž je nejznámější právě síťový model TCP/IP, který je také nazýván DoD model (USA Department of Defense Model, tedy model Ministerstva obrany USA).
- Na této protokolové sadě funguje i největší počítačová síť Internet.

TCP/IP je navržen tak, aby

- byl co nejvíc decentralizovaný (žádná centrální správa),
- byl co nejodolnější vůči různým (i kritickým) podmínkám provozu a co nejodolnější vůči přenosovým chybám,
- nechával co nejvíc práce na koncových zařízeních (jádro sítě musí být rychlé a pružné), a aby byl spravovatelný distribuovaně (každá část si spravuje „to svoje“) ,
- dokázal propojit i sítě s hodně odlišnou síťovou architekturou a technologiemi (aby byl co nejuniverzálnější při zachování předchozích vlastností).
- přednost má nespojovaná a nespolehlivá komunikace, při uplatnění principu „**best effort**“ (maximální snahy).

- Přednost má nespojovaná a nespolehlivá komunikace, při uplatnění principu „**best effort**“ (maximální snahy).
- služba nesplňující podmínky pro spolehlivou službu, i když je vedena nejlepší snahou o doručení. Obvykle se tak označuje služba, která se nepokouší opakovat odeslání dat při selhání komunikace a která neoznamuje uživateli, že došlo k selhání. V souvislosti s Quality of Service to znamená, že uživateli nemusí být poskytnuta určitá kvality služby.
- Internet Protocol (IP) poskytuje pouze best-effort službu doručování datagramů mezi koncovými uzly. Není zaručeno, že se datagram neztratí, neopozdí, nepoškodí nebo nedorazí vícekrát.

Srovnání modelů

	Referenční model ISO/OSI	Síťový model TCP/IP	PDU:	Adresování:
L7	Aplikační vrstva	Aplikační (procesní) vrstva	data, zprávy	
L6	Prezentační vrstva			
L5	Relační vrstva			
L4	Transportní vrstva	Transportní (hostitelská) vrstva	segmenty	porty
L3	Síťová vrstva	Síťová (internetová) vrstva	pakety, datagramy	IP adresy
L2	Linková vrstva	Vrstva síťového rozhraní	rámce	MAC adresy
L1	Fyzická vrstva		bity	

Vrstva síťového rozhraní.

- Tato vrstva v sobě sdružuje funkčnost vrstev L1 a L2 referenčního modelu. Přímě v TCP/IP pro ni nejsou stanoveny žádné protokoly, je jen určeno, jak mají komunikovat se síťovou vrstvou. Komunikuje s hardwarem (síťovým rozhraním), případně její část může být hardwarově implementovaná. Obvykle se do této vrstvy napojují protokolové sady lokálních a rozlehlých sítí, například
IEEE 802.3 (Ethernet),
IEEE 802.11 (Wi-fi),

Síťová vrstva

- na této vrstvě probíhá propojování sítí, včetně směrování mezi sítěmi
- typické zařízení této vrstvy je router (směrovač) nebo switch
- používané protokoly IP (Internet Protocol, verze IPv4 a IPv6, které jsou dnes v praxi používány), ARP, RARP, ICMP, IGMP, IGRP, IPSEC

Transportní vrstva

- je implementována až v koncových zařízeních (počítačích) a umožňuje proto přizpůsobit chování sítě potřebám aplikace
- Poskytuje transportní služby kontrolovaným spojením spolehlivým protokolem TCP (*transmission control protocol*) nebo nekontrolovaným spojením nespolehlivým protokolem UDP (*user datagram protocol*).

Aplikační vrstva

- na této vrstvě najdeme velké množství protokolů, s většinou z nich komunikují aplikace, které potřebují přistupovat na síť
- příklady protokolů: FTP, HTTP, DHCP, DNS, POP3, ...
- pro rozlišení aplikačních protokolů se používají tzv. porty, což jsou domluvená číselná označení aplikací. Každé síťové spojení aplikace je jednoznačně určeno číslem portu a transportním protokolem (a samozřejmě adresou počítače).

Protokol IP

Internet Protocol je základní protokol síťové vrstvy a celého internetu. Provádí vysílání **datagramů** na základě síťových IP adres obsažených v jejich záhlaví.

Poskytuje vyšším vrstvám **síťovou službu bez spojení**.

Každý datagram je samostatná datová jednotka, která obsahuje všechny potřebné údaje o adresátovi i odesilateli a pořadovém čísle datagramu ve zprávě. Datagramy putují sítí nezávisle na sobě a pořadí jejich doručení nemusí odpovídat pořadí ve zprávě. Doručení datagramu není zaručeno, spolehlivost musí zajistit vyšší vrstvy (TCP, aplikace).

IP protokol se dále stará o segmentaci a znovusestavení datagramů do a z rámců podle protokolu nižší vrstvy (např. ethernet).

V současné době je převážně používán protokol IP verze 4.

Nová verze 6, která řeší nedostatek adres v IPv4, bezpečnostní problémy a vylepšuje další vlastnosti protokolu IP, je celosvětově používána jen několika procenty zařízení připojených k internetu, ale jejich počet rychle roste.

Protokoly IPv4 a IPv6

- IPv4:

32 bitové adresy

cca 4 miliardy různých IP adres, dnes nedostačující

- IPv6:

128 bitové adresy

podpora bezpečnosti

podpora pro mobilní zařízení

funkce pro zajištění úrovně služeb (QoS - Quality of Service)

Fragmentace paketů - rozdělování

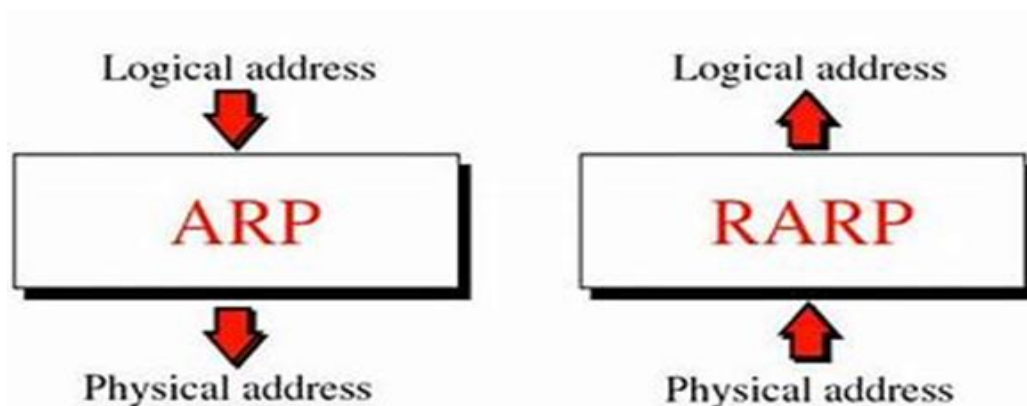
není zpětně kompatibilní s IPv4

snadnější automatická konfigurace

Protokol ARP slouží v rodině TCP/IP k získání linkové adresy síťového rozhraní protistrany ve stejné podsíti pomocí známé IP adresy

Reverse Address Resolution **Protocol (RARP)** se v počítačových sítích s IPprotokolem používá k získání vlastní IP adresy počítače při znalosti MAC adresy (tu každý počítač zná, má ji v trvalé paměti síťové karty)

- fungování protokolu ARP lze obrátit (proto: Reverse ARP)
 - a dosáhnout tak převodu mezi HW a IP adresou
 - uzel zná svou HW adresu, a chce znát svou IP adresu
 - fakticky jde o (nejjednodušší variantu) přidělování IP adres jednotlivým uzlům



Protokol ICMP (anglicky Internet Control Message Protocol) je v informatice jeden z nejdůležitějších protokolů počítačových sítí založených na rodině protokolů TCP/IP (tedy protokolu, který používá Internet). Protokol ICMP používají operační systémy v síti pro odesílání služebních informací, například chybových zpráv pro oznámení, že požadovaná služba není dostupná nebo že potřebný počítač nebo router není dosažitelný. Používá se např. v programu *ping* pro testování dostupnosti počítače, nebo programem *traceroute* pro sledování cesty paketů k jinému uzlu.

IGMP (Internet Group Management Protokol) je protokol, který rozšiřuje požadavky na implementaci protokolu IP (IPv4) o podporu IP multicastu. Využívá se pro dynamické přihlašování a odhlašování ze skupiny u multicastového routeru ve své lokální síti.

IGP (Interior gateway protocol) se používá pro směrovací protokoly sloužící k výměně směrovacích informací mezi směrovači (anglicky router, v názvu je však použit tradiční termín brána, anglicky gateway) v rámci autonomního systému (AS), což může být rozsáhlá firemní lokální síť nebo síť poskytovatele internetového připojení včetně připojených zákazníků.

IPsec (IP security) je v informatice název bezpečnostního rozšíření IP protokolu založené na autentizaci a šifrování každého IP datagramu. IPsec používá kryptografické bezpečnostní služby pro ochranu komunikace prostřednictvím skrze IP protokol. Poskytuje ověřování dat, původ dat, jejich integritu, důvěrnost (šifrování) a ochranu proti útoku pomocí přehrání (viz replay attack).

TCP

- Transmission Control Protocol vytváří virtuální okruh mezi koncovými aplikacemi, tedy **spolehlivý přenos dat**.

Vlastnosti protokolu:

- Spolehlivá transportní služba, doručí adresátovi všechna data bez ztráty a ve správném pořadí.
- Služba se spojením, má fáze navázání spojení, přenos dat a ukončení spojení.
- Transparentní přenos libovolných dat.
- Plně duplexní spojení, současný obousměrný přenos dat.
- Rozlišování aplikací pomocí portů.

UDP

- User Datagram Protocol poskytuje nespolehlivou transportní službu pro takové aplikace, které nepotřebují spolehlivost, jakou má protokol TCP.
- Nemá fázi navazování a ukončení spojení a už první segment UDP obsahuje aplikační data. UDP je používán aplikacemi jako je DHCP, TFTP, SNMP, DNS a BOOTP.
- Protokol používá podobně jako TCP čísla portů pro identifikaci aplikačních protokolů.

SCTP

Spolehlivý protokol pro přenos datagramů ve více proudech. Je využíván zejména v telekomunikacích. Doplnuje některé vlastnosti, které TCP postrádá:

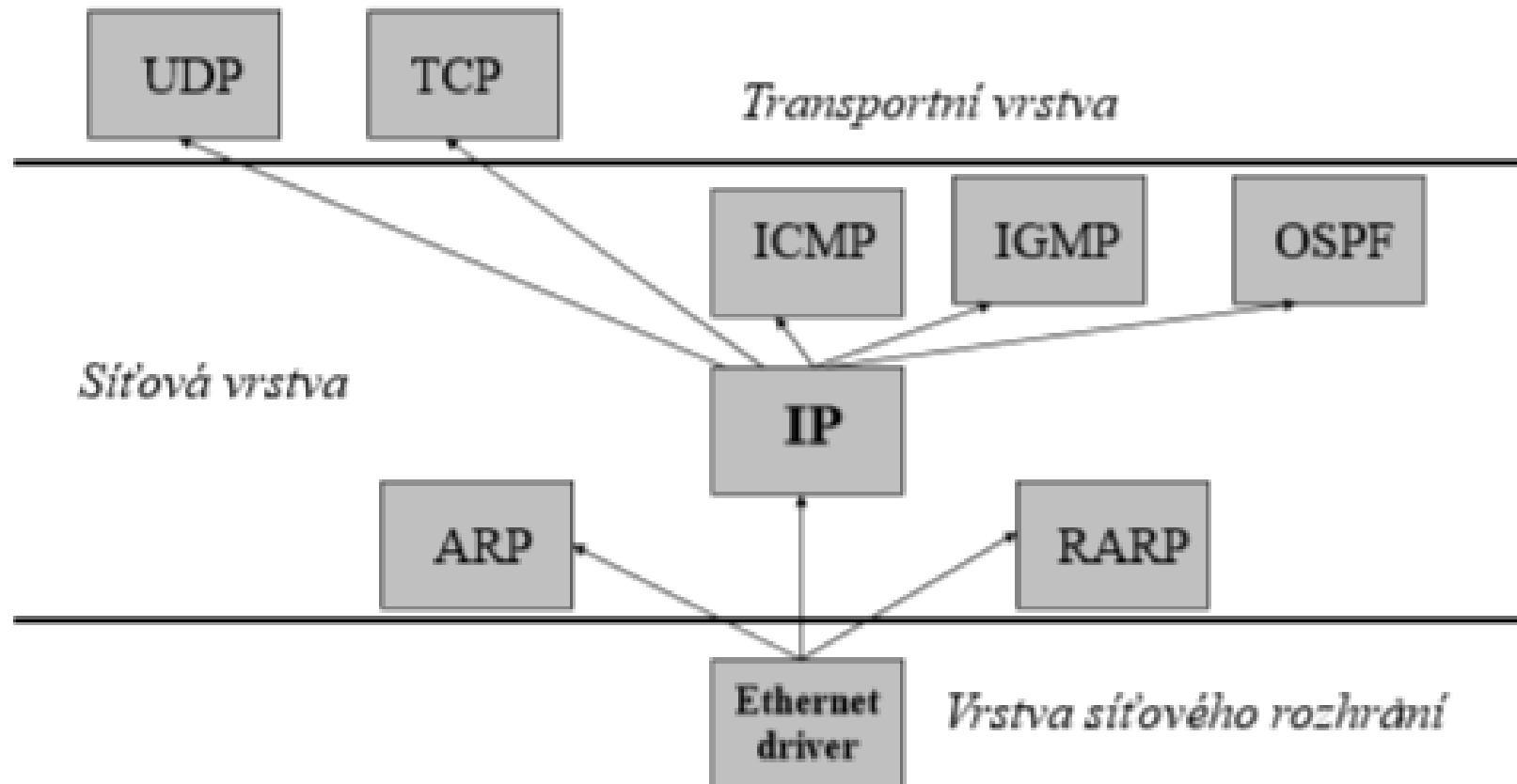
- Multihoming - komunikující uzel může mít několik IP adres.
- Členění datového toku na datagramy.
- Používání více proudů dat - omezuje blokování komunikace způsobené chybějícím blokem dat, ke kterému může dojít v TCP.
- Výběr a sledování cesty - Pokud má primární adresa problémy s dostupností lze používat alternativní.
- Ověřovací a potvrzovací mechanismy - SCTP komplikuje některé útoky směřující k nedostupnosti služeb (DoS). Zajišťuje ověření opakujících se a chybějících balíků.

Stejně jako TCP a UDP rozlišuje aplikační protokoly pomocí portů.

Počítačové síť

IP vrstva

- Protokoly: **IP**, ARP, RARP, ICMP, IGMP, OSPF



Aplikační protokoly (služby)

- DNS – systém doménových jmen
- DHCP – dynamické přidělování síťových informací jako například: výchozí brána, maska sítě, IP adresa
- FTP – přenos souborů po síti
- TFTP - jednoduchý protokol pro přenos souborů
- HTTP – přenos hypertextových dokumentů (WWW)
- WebDAV – rozšíření HTTP o práci se soubory
- IMAP (Internet Message Access Protocol) umožňuje manipulovat s jednotlivými e-mail zprávami na poštovním serveru.

- IRC (Internet Relay Chat) – jednoduchý chat po internetu.
- NNTP (Network News Transfer Protocol) umožňuje číst a umísťovat do sítě zprávy typu *news*.
- NFS (Network File System) – síťový systém souborů, který umožňuje transparentní sdílení vzdálených souborů jakoby byly lokální.
- NTLM Autentizační protokol Windows
- NTP – synchronizace času (šíření přesného času)
- POP3 (Post Office Protocol) – protokol pro získání pošty z poštovního serveru.

- SMB (Server Message Block) - sdílení souborů a tiskáren v sítích Windows
- SMTP – zasílání elektronické pošty
- SNMP Simple Network Management Protokol je určen pro správu síťových uzlů.
- Telnet – protokol virtuálního terminálu.
- SSH – bezpečný shell
- X11 – zobrazování oken grafických programů v Unixových systémech
- XMPP – rozšiřitelný protokol pro zasílání zpráv a sledování přítomnosti