# 19. Transportní a aplikační vrstva OSI modelu

## C:\Users\babak\Downloads\osi-model.jpg

4 – Aplikační v.

3 – Transportní v.

2 - Internetová v.

1 - Fyzická v. (síťového rozhraní)

Aplikační v. – L7

Prezentační v. – L6

Relační v. – L5

Transportní v. – L4

Síťová v. – L3

Linková v. – L2

Fyzická v. – L1

## Obecné

* Síť (obecný pojem) – technologické prostředky spojující dva síťové systémy mezi sebou
* Síť (TCP/IP) – Ohraničená oblast v rámci jedné L2 broadcast domény, převedeno do srozumitelné řeči = vymezené území pomocí IP adres, kde se počítače vzájemně vidí pomocí MAC adres. Z praxe: lze přirovnat k městu, nebo státu, které má své hranice a stejně tak i síť má své vymezené území.
* MAC adresa – fyzická identifikace každého síťového zařízení na bázi ethernet standardu (u jiných standardů může být tento identifikátor jiný), důležité je, že to je identifikace na zařízení, tedy hardware (měla by správně zůstat neměnná)
* IP adresa – vyšší typ identifikace jednotlivého síťového zařízení, jedná se o identifikaci na L3, pomocí IP adresy a masky podsítě se vymezuje síť z hlediska TCP/IP standardu. IP adresy dělíme na privátní (pro sítě LAN a privátní WAN) a veřejné (pro Internet)
* L vrstvy – definovány OSI modelem, teoreticky popisují o jaký typ komunikace, resp. o jakou fázi, se aktuálně jedná. Značení L1 – L7. U zjednodušeného praktického modelu TCP/IP se používají pouze vrstvy čtyři. U sítí se rozlišují však běžně vrstvy všechny (především pak L1,L2,L3,L4 a L7)

## Transportní vrstva (3. vrstva TCP/IP modelu, L4 OSI modelu)

* dochází k vymezení a vyhrazení trasy a způsobu přenosu, včetně zajištění její spolehlivosti, nebo nespolehlivosti (např. UDP, TCP)
* úkolem transportní vrstvy je přizpůsobení možností tří nejnižších vrstev (síťové, linkové a fyzické) představám vyšších vrstev
* dalším významným úkolem transportní vrstvy je i rozlišování různých příjemců a odesilatelů v rámci jednotlivých uzlů.
  + až do síťové vrstvy včetně se totiž všechny přenosy týkají jednotlivých uzlů jako celků (a také příslušné adresy identifikují pouze uzly jako celky)
  + teprve transportní vrstva jde dále a rozlišuje jednotlivé příjemce v rámci těchto uzlů
  + již rozlišuje konkrétní entity (jednotlivé procesy, úlohy) v rámci každého uzlu – např. čísla portů v TCP/IP
* na L4 obvykle pracují firewally
* protokoly na L4: TCP, UDP, IP, ICMP, IGMP, GRE, …

### TCP (transport control protocol)

* jeden z dvojice nejpoužívanějších L4 přenosových protokolů
* zajišťuje garantované doručení komunikace z bodu A do bodu B
  + hlídá počet odeslaných a doručených packetů a ověřuje i pořadí, pokud packety nejsou doručeny kompletně, vyžádá si příslušný packet, který doručen nebyl a dle pořadí jej zařadí na správné místo
* používá se tam, kde je striktně vyžadována celistvost a správnost informací
  + konkrétně se využívá např. pro doručování emailů, přenos webových stránek, ale také pro síťovou komunikaci s databázemi, nebo pro přenosové protokoly typu FTP, FTPS atd.
* nevýhodou TCP je jeho relativní pomalost (důvodem je jeho rigidní kontrola celého přenosu)

### UDP (user datagram protocol)

* přesný opak TCP
* UDP neprovádí kontrolu jednotlivých packetů z hlediska pořadí a kompletnosti
* používá se v těch případech, kdy není kompletnost informace podstatná, ale je klíčová rychlost doručení
* výhodou UDP je tedy jeho rychlost
* příkladem aplikací, kde se UDP využívá, je např. DNS, streaming, SIP, IKE atd.

## Aplikační vrstva TCP/IP modelu (L5-L7 OSI modelu)

* vrstva čistě softwarová, pracuje s ní operační systém, ale především jednotlivé aplikace
* obvykle není implementováno do hardware, ač to není vyloučeno

### Relační (L5) vrstva

* smyslem vrstvy je organizovat a synchronizovat dialog mezi spolupracujícími relačnímu vrstvami obou systémů a řídit výměnu dat mezi nimi. Umožňuje vytvoření a ukončení relačního spojení, synchronizace a obnovení spojení, oznamování výjimečných stavů.
* relační vrstva je nejčastěji kritizovanou vrstvou referenčního modelu ISO/OSI, protože právě ona toho má co nejméně na práci v porovnání s ostatními vrstvami.
* především má podporovat vedení relací

### Prezentační (L6) vrstva

* funkcí vrstvy je transformovat data do tvaru, které používají aplikace (šifrování, konvertování, komprimace).
* formát dat (datové struktury) se může lišit na obou komunikujících systémech, navíc dochází k transformaci pro účel přenosu dat nižšímu vrstvami
* mezi funkce patří např. převod kódů a abeced, modifikace grafického uspořádání, přizpůsobení pořadí bajtů apod.
* vrstva se zabývá jen strukturou dat, ale ne jejich významem, který je znám jen vrstvě aplikační.

|  |  |  |  |
| --- | --- | --- | --- |
| Prezentační  vrstva | Data | Prezentace dat a šifrování. Řeší rozdíly v reprezentaci dat mezi aplikací a síťovým formátem – kóduje data pro přenos. | MIDI, MPEG |

### Aplikační (L7) vrstva

* účelem vrstvy je poskytnout aplikacím přístup ke komunikačnímu systému a umožnit tak jejich spolupráci
* některé aplikace jsou globálně definovány ve standardech, mezi takové patří například DHCP, DNS, HTTP, HTTPS, FTP, SMTP apod.
* některé aplikace jsou definovány jen lokálně pro využití například u Client server architektury (příklad: MySQL, HP SIM, AbraG2, Stormware Pohoda, atd…)
* FQDN (neboli DNS jméno) – je nejvyšší způsob identifikace zařízení, běží na L7, je to čitelné jméno označující počítač, nebo jiný síťový objekt. (např. doména, síťový prvek atd.)

#### DNS (UDP53 ; Domain name server)

* nejdůležitější služba pro fungování internetu
* jedná se o databázově orientovanou aplikaci typu Client-Server, která má za úkol provádět překlady z doménových jmen (např. postupicka.cz) na IP adresy
* v databázi jsou uloženy dva základní údaje (IP a domain name) + typ záznamu (A, MX, CNAME, NameServer)
* vy jako uživatel se dotážete předdefinovaného DNS serveru, zda Váš požadavek obsahuje jeho databáze - pokud ano, sdělí Vašemu počítači IP adresu a může proběhnout navázání komunikace, pokud ne, dojde k předání požadavku na vyšší úroveň DNS serveru
* bez DNS serveru se neobejdou některé důležité aplikace (například LDAP, nebo MS Exchange, případně samotné SMTP)
* DNS server je kritický pro fungování většiny WAN i LAN sítí
* DNS se konfiguruje vždy v rámci tzv. domény, tedy logického názvu WAN, či LAN sítě sdružující jeden, nebo více počítačů. Např. doména seznam.cz může obsahovat několik stovek, nebo tisíců počítačů
* DNS servery se dělí na dvě skupiny:
  + Interní – slouží pro LAN, v některých sítích nepovinné
  + Veřejné – veřejné servery, které provozují provideři internetu, mají obvykle velké databáze
* DNS databáze se skládá ze dvou částí:
  + Forward lookup zone (zóna dopředného čtení) – provádí překlad z doménového jména na IP adresu
  + Reverse lookup zone (zóna zpětného čtení) – provádí překlad z IP adresy na doménové jméno
* Jak otestovat DNS? → nejlépe lze otestovat příkazem ping cílová\_adresa, nebo doména
  + Ping postupicka.cz otestuje funkčnost zóny dopředného čtení
  + Ping 195.122.204.32 otestuje funkčnost zóny zpětného čtení (toto funguje pouze za určitých podmínek)
* DNS obsahuje různé typy záznamů
  + A – nejběžnější záznam, prostý překlad z FQDN na IP
  + PTR – překlad z IP na FQDN
  + MX – určení, kde se v dané doméně nachází mail server
  + CNAME – tzv. alias, vytváří se další jméno na existující A záznam (např. CNAME mail.seznam.cz přeloží dopředná zóna na [www.seznam.cz](http://www.seznam.cz/))

#### Další L7 protokoly

* **DHCP server** – kritická aplikace ve větších sítích. Tento program umožňuje dynamickou síťovou konfiguraci jednotlivých síťových prvků. Provádí to na základě DHCP-request packetu, který je vyslán broadcast vysíláním z počítače žádajícího informace o síťové konfiguraci. Na základě MAC adresy je žadateli přiřazena příslušná síťová konfigurace. Data se ukládají do DHCP databáze.
* **DHCP scope** – tzv. obor – je nastavení konfigurace pro tzv. DHCP klienty, tedy žádající počítače. Scope obsahuje informace o rozsahu přidělovaných IP adres (interval od-do), dále informace o tzv. výchozí bráně (default gateway), nebo o DNS serverech. Informací uložených v rámci scope může být velmi mnoho, je možné vkládat jakékoliv dodatečné (custom) konfigurační parametry.
* **HTTP server** – jednoduchá aplikace určená k přenášení souborů, soubory se přenášejí ve formě prostého textu. HTTP se používá k přenášení v rámci internetu a hlavním typem souborů jdoucích přes HTTP jsou soubory HTML. HTTP server používá TCP 80 na vrstvě L4
* **HTTPS server** – jednoduchá aplikace určená k přenášení souborů, soubory se přenášejí v zašifrované podobě. HTTPS server používá TCP 443 na vrstvě L4
* **SMTP server** – je infrastrukturní aplikace určená k přenášení souborů, upravená pro přenos elektronické pošty. Je to kritická aplikace určená pro komunikaci mezi jednotlivými email servery. Data prochází jako prostý text a aplikace používá TCP 25 na vrstvě L4.
* **POP3, IMAP** – on request protokoly používané téměř výlučně pro stahování pošty ze serveru do klientského počítače. Nevýhodou je jejich plaintext varianta. Je tedy vhodné pro přenos důvěrných zpráv používat bezpečnostní klíče (šifrování).
* **FTP server –** protokol určený k přenášení souborů, používá systém autorizace pomocí jména a hesla, využívá ověřovací a řídící kanál. Negativem je fungování v režimu prostého textu (včetně hesel). Používá TCP 21 pro data kanál a UDP 20 pro kontrolní a řídící kanál. Má i šifrované varianty FTPS a dost odlišnou verzi SFTP.
* **TELNET** – protokol určený pro přenášení textu (i souborů), aplikace je upravená tak, aby se jejím prostřednictvím daly řídit různá zařízení (nejčastěji právě síťové prvky). Telnet používá TCP 23 na L4.
* **SSH** – šifrovaný ekvivalent pro telnet, funkce je stejná, pro zabezpečení se používá šifrovací certifikát
* IRC, Jabber, ICQ – instant messaging aplikace
* RDP, VNC – protokoly pro vzdálený přístup k obrazovce cílového počítače
* SQL server, Oracle – databázové protokoly

|  |  |  |  |
| --- | --- | --- | --- |
| Aplikační  vrstva | Data | Síťové procesy pro aplikaci, ověření uživatelů, vše závislé na aplikační vrstvě. | Telnet, FTP |