# 18. Fyzická a internetová vrstva TCP/IP adresa

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

4 – Aplikační v.

3 – Transportní v.

2 - Internetová v.(síťová)

1 - Fyzická v. (síťového rozhraní)

Aplikační v. – L7

Prezentační v. – L6

Relační v. – L5

Transportní v. – L4

Síťová v. – L3

Spojovací 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
* 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)
* ICMP – je soubor diagnostických technologií určených pro zjišťování dostupnosti a kvality sítě, popř. pro zkoušku směrovacích protokolů. Nejdůležitějším zástupcem je funkce PING (zjišťuje v ms časovou odezvu vzdáleného systému)
* ARP – propojovací protokol mezi L2 a L3 vrstvou, provádí překlad z IP adres na MAC adresy a naopak, slouží k tomu tzv. ARP tabulka (dva sloupce, MAC a IP), protokol funguje obousměrně (jako ARP a RARP)

## Vrstva síťového rozhraní TCP/IP modelu (L1 a L2 OSI modelu)

### Fyzická (L1) vrstva

* dochází k navazování spojení mezi dvěma síťovými body (pozor jedná se o navazování bod – bod, čili je to vrstva, která funguje vždycky mezi sousedními síťovými prvky)
* zabývá se výhradně přenosem bitů, nabízí služby typu: přijmi bit, odešli bit
* na L1 se vyjednávají parametry přenosu a to: *(níže uvedené platí pro sítě Ethernet)*
  + rychlost → Mbps / Gbps
    - rychlostní standardy: 10Mbps, 100Mbps, 1000Mbps, 10Gbps, 40Gbps a 100Gbps
  + duplex → Half / Full
    - popisuje směr toku komunikace, zda obousměrně, či jednosměrně (tj. čeká se vždy na dokončení komunikace z jedné strany, aby se mohla zahájit komunikace ze druhé strany)
  + volba typu spojení → MDI / MDI-X
    - MDI – nekřížené tj. rovné; MDI-X křížené
* vyjednávání, neboli negotiation probíhá obvykle automaticky, v určitých případech se musí parametry nastavit ručně
  + parametry musí být na obou stranách vždy shodné, vždy podle nejpomalejšího

|  |  |  |  |
| --- | --- | --- | --- |
| Fyzická  vrstva | Bits (bity) | Fyzické parametry linky – média (kabely, rádio, světlo), signály a binární přenos. Řeší fyzické poslání dat (přenášeným bitům nepřiřazuje žádný význam).; | 100BaseT(ethernet), RS-232(sériový přenos),  802.11g (wi-fi) |

### Linková (L2) vrstva

* dochází ke spojení pomocí fyzických adres (MAC adres), tato komunikace již opouští spojení bod – bod a může prostřednictvím síťových prvků procházet v rámci jedné L3 sítě do libovolného místa
* přenáší celé bloky dat tzv. rámce, využívá k tomu služeb fyzické vrstvy
* na L2 vrstvě pracují switche, provádějí na základě zdrojové a cílové MAC adresy inteligentní přepínání z bodu A do bodu B
* v rámci L2 se provádějí některé speciální funkce závisející na MAC adresách:
  + Linková agregace – logické spojení obvykle dvou až osmi portů dohromady do tzv. agregační skupiny (porty se navenek tváří jako port jeden s rychlostí rovnající se součtu rychlostí agregovaných portů), používá se pro zvýšení výkonu konkrétního spoje a pro zvýšení dostupnosti
  + Spanning-tree – STP protokol se v různých obměnách používá pro spojování sítí do uzavřených okruhů (což standardně nejde), STP udržuje okruh otevřený, v případě výpadku jednoho z páteřních spojení provede STP aktivaci tzv. záložní linky. STP se používá pro zajištění vysoké dostupnosti (má varianty STP, RSTP, MSTP u Cisca pak pod označením PVST, PVST+ atd.)
  + QoS (Quality of Service) – soubor funkcí, které dokáží komunikaci označit podle charakteru a na základě určeného typu nastavit příslušnou prioritu. (umožňuje např. preferovat hlasovou komunikaci proti běžným datům atd.).
* VLAN – je logické oddělení jednotlivých L2 sítí od sebe, pro představu jeden switch můžeme „nakrájet“ na třeba pět, šest menších (na L2 se jednotlivé porty v různých VLAN nevidí). VLAN se používá jednak z bezpečnostních důvodů, jednak pro lepší organizaci síťových prvků v síti (např. jedna VLAN je určena pro vedení firmy, druhá pro ekonomy, třetí pro výrobu a čtvrtá pro návštěvníky přes WIFI). VLAN zajišťují izolaci portů mezi sebou.

|  |  |  |  |
| --- | --- | --- | --- |
| Linková  vrstva | Frames (rámce) | Fyzická adresace, MAC – media access control a LLC – logical link control, datový tok, synchronizace rámců, komunikace 1 hop, používá MAC adresy. Detekce chyb, řízení toku a přístupu na médium. Komunikace mezi dvěma zařízeními v jednom subnetu (nebo na bránu) pomocí MAC adresy. Vytváří rámce (hlavička + data + zápatí). | Ethernet, FDDI, Token Ring, PPP, SLIP |

#### MAC (Media Access Control) 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)
* 48bitové číslo (248 kombinací)
* složena ze dvou částí. První polovina určuje výrobce síťového zařízení, tedy aktivního prvku (viz: <http://standards.ieee.org/regauth/oui/oui.txt>), druhá pak určuje samotné zařízení
* V současnosti je určitým problémem, že hodně síťových prvků umožňuje změnu MAC adresy (u nás třeba nutnost u internetového operátora UPC). MAC proto nemusí vždy garantovat jedinečnost.
* hexadecimální

#### Switching

* Switch – je zařízení pracující na L2 vrstvě, pracuje tedy výlučně s MAC adresami. Switche mohou být kombinovány s jinými funkcemi na vyšších vrstvách, ale switch jako takový je vždy pouze L2 zařízení. Existují v podobách:
  + Unmanaged (neřížené) – jsou bez možnosti cokoliv nastavit, provádí jen a pouze switching (čili přepínání packetů podle MAC adres)
  + Managed (řízené) – jsou prvky s možností konfigurace, tu lze provádět buď pomocí webového rozhraní, nebo příkazové řádky
* A dále dělíme na:
  + Desktop, nebo stolní switche – obvykle unmanaged, jednoduché switche s malým počtem portů
  + Rack-mount switche – určené k montáži do datových rozvaděčů (racků)
  + Modular switche – switche určené pro modulární konfiguraci portů (kombinace gigabit, desetigigabit portů, metalických portů, optických portů), nebo k doplňování funkcionality pomocí speciálních modulů. Pro představu: je to velmi podobné blade serverům)
* Switch má jednu MAC adresu na celé zařízení
* Switching – je kmenovou funkcí switchů, na základě zdrojové a cílové adresy je příslušná komunikace přepnuta na správný cílový port
* Port – jeden připojovací bod, tedy zásuvka, port má vždycky určenu maximální rychlost, duplex a křížení (čili je to L1 konfigurace), porty mohou fungovat na nižších než maximálních rychlostech (např. 100Mbps port umí pracovat na 10Mbps atd.) Počty portů jsou standardně 4,8,16,24,48 u modulárních switchů jsou počty dramaticky odlišné.

## Internetová vrstva TCP/IP modelu (L3 OSI modelu)

* dochází k přechodu hranice jedné L2 domény (aka L3 sítě) do druhé
* hlavním úkolem síťové vrstvy je tzv. směrování, neboli nalezení vhodné cesty vedoucí od odesílatele dat až k jejich koncovému příjemci
  + směrování komunikace z jedné sítě do druhé zajišťují routery (směrovače)
* také síťová vrstva přenáší data po blocích, kterým se říká pakety (anglicky „packets“), zatímco na úrovni linkové vrstvy se jim říká rámce
* Představa fungování je taková, že síťová vrstva v určitém uzlu rozhodne o dalším směru, kterým by měl být konkrétní paket přenesen k některému ze sousedních uzlů. Poté jej předá své linkové vrstvě, která paket vloží do svého rámce a přenese k příslušnému sousednímu uzlu. Zde jej partnerská linková vrstva vybalí a předá datový paket své bezprostředně vyšší síťové vrstvě. Ta rozhodne, kterým směrem by měl být paket dále odeslán… a to vše se opakuje, dokud datový paket nedorazí ke svému konečnému cíli.
* specifickými funkcemi jsou různé routovací (směrovací) protokoly např. OSPF, RIP, BGP, EGP atd.
* na L3 se komunikuje prostřednictvím IP adres

|  |  |  |  |
| --- | --- | --- | --- |
| Síťová  vrstva | Packets (pakety) | Logická adresace – routování – určení cesty paketu, přenos dat z bodu do bodu, používá IP adresy. Komunikace mezi zdrojovým a cílovým zařízením pomocí IP adresy. | IP, ICMP, ARP, RIP |

### IP adresa

* vyšší typ identifikace jednotlivého síťového zařízení, jedná se o identifikaci na L3
* každý síťový prvek musí být definován kromě adresy IP ještě tzv. maskou sítě, která určuje rozsah (velikost) sítě, ve které je daný síťový prvek zapojen. (stanovuje hranice jedné sítě)
* IP adresy dělíme na privátní (pro sítě LAN a privátní WAN) a veřejné (pro Internet)
* musí být v rámci sítě jedinečná (tzn. v rámci skupiny PC, které na sebe „vidí“)
* IPv4 a IPv6 – adresní rozsahy používané v současných sítích TCP/IP, absolutně převažuje IPv4 (232), nastupuje postupně IPv6 (2128)
* Maska sítě – dvě možnosti zápisu
  + Klasický způsob – 255.255.255.0
  + CIDR - /24 (určuje lépe max. počet IP adres v rámci segmentu) – určuje kolik bitů sítě je zamčených (nepoužitelných pro adresaci) – jednodušší
* IPv4 adresování
  + Vyčleněny jsou následující IP rozsahy:
    - 10.0.0.0/8 – 24bit blok (224 adres) = 16,777 mil. adres – adresace vhodná pro firmy s velkou spotřebou IP adres, nejčastěji nadnárodní společnosti. Lze přidělit 10.0.0.0-10.255.255.255
    - 172.16.0.0/12 – 20bit blok (220 adres) = 1,048 mil. adres – adresace vhodná pro virtuální privátní sítě, lze přidělit 172.16.0.0 – 172.31.255.255
    - 192.168.0.0/16 – 16 bit blok (216 adres) = 65536 adres, vhodné pro malé společnosti s malou potřebou IP adres, lze přidělit 192.168.0.0-192.168.255.255
  + Další speciální IP adresní rozsahy a IP adresy:
    - 127.0.0.1 – localhost, loopback – každý počítač s funkčním IP protokolem (netřeba funkční síťovou kartu) má přidělenu tuto IP adresu, tzv. smyčku, přes kterou se za pomocí TCP/IP dostane sám na sebe. Tato adresa je blokována na všech síťových prvcích a nelze běžně přidělit.
    - 224.0.0.0 a výše jsou IP adresy definované pro speciální účely, například pro Multicasting (vysílání many to many)
    - 169.254.0.0/16 – speciální rozsah IP adres určený pro tzv. zeroconf. stavy, tedy pro situace, kdy nedojde k automatickému přiřazení IP adresy ze serveru DHCP. Aby bylo dosaženo alespoň základní konektivity a síť fungovala, síťový adaptér si automaticky přidělí adresu z tohoto rozsahu 169.254.0.0/16. Adrese se také říká APIPA (automatic private IP addressing)

### Routing

* Routing – směrování – je soubor technologií umožňujících komunikaci mezi jednotlivými L3 sítěmi (aka L2 doménami). Dělíme na:
  + Statický routing – jednotlivé cesty musíme určit ručně
  + Dynamický routing – jednotlivé cesty si routery určují podle předem daných pravidel
* Router – směrovač – zařízení umožňující pracovat s routing protokoly (dynamickými a statickými), tedy umožňuje směrovat komunikaci mezi jednotlivými L3 sítěmi. Router jako dedikované zařízení má rovněž jako switch porty avšak každý port má svojí MAC adresu a je nezávislý na portech ostatních. (platí pro ethernet) Routery obvykle kombinují i jiné typy protokolů, než je ethernet (např. ADSL, ISDN, T1, E1 atd.) Routery dělíme na:
  + Fixed port – jsou zařízení s pevným, neměnným počtem portů (obvykle se používají pro domácí použití, nebo pro malé firmy)
  + Modular port – jsou zařízení používaná hlavně pro firemní a infrastrukturní použití, umožňuje podle okolností konfigurovat počty a typy portů používaných pro routing. (obdoba modular switchů
* Routovací tabulka – základní orientační prostředek pro síťová zařízení, kam mají danou komunikaci směrovat. V podstatě se jedná o jakýsi rozcestník co poslat kam. Routovací tabulka používá IP adresy.
* Routing – postup:
  + Router přečte zdrojovou IP adresu, zdrojovou MAC adresu, přečte cílovou IP a MAC adresu.
  + Router odebere zdrojovou IP a MAC adresu a nahradí je svojí a pošle informaci buď na svůj port (pokud je cíl v jeho přímém dosahu), nebo informaci pošle na další router.
* Default gateway – klíčový záznam v routovací tabulce, určuje další router v řadě pro packety, které nemají jiná pravidla. V routovací tabulce se vždy zapisuje:
  + 0.0.0.0 ip\_adresa\_routeru
  + záznam říká, že vše, pro co neexistují další pravidla pošli na ip\_adresa\_routeru
* NAT – network address translation – funkce umožňuje skrýt celou velkou LAN (na privátních adresách) za jednu veřejnou IP adresu dostupnou z internetu. NAT lze provádět dovnitř i ven, standardně se používá tzv. source nat, používaný pro přístup ven z LAN do internetu.