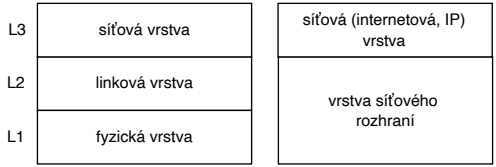
Počítačové sítě 1

síťová vrstva

Martin Trnečka

Katedra informatiky
Univerzita Palackého v Olomouci

TCP/IP architektura



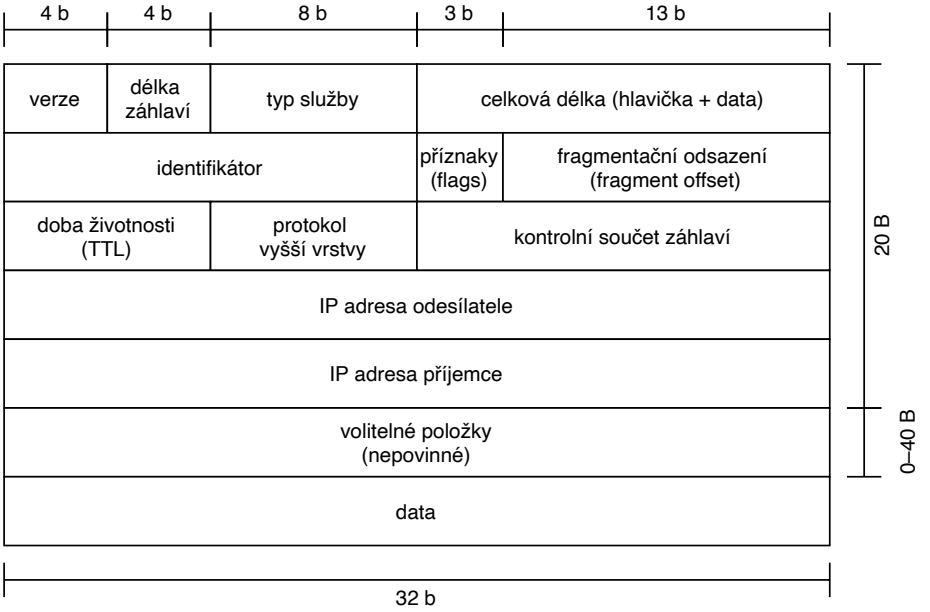
Síťová vrstva

- terminologie: síťová, IP, internetová vrstva
- jedinečná identifikace uzlů v síti → *IP adresa*
- směrování (routing) mezi nesousedními uzly (mimo lokální síť)
- napojení na linkovou vrstvu
- přenos dat ve formě (IP) paketu/datagramu
- balení dat do paketů
- spojová vs. nespojová služba na úrovni síťové vrstvy
- nezajišťuje
  - kontrolu chyb (pozn. může dojít k chybě při zpracování paketu) → zodpovědnost vyšší vrstvy
  - řízení toku dat → zodpovědnost vyšší vrstvy
  - bezpečnost (dodatečné zabezpečení pomocí IPSec)

Struktura IP vrstvy

- Internet Protocol (IP)
  - klíčová část TCP/IP architektury
  - poskytuje nespolehlivou nespojovanou službu
  - umožňuje propojení více sítí
- další protokoly síťové vrstvy
  - ICMP – služební protokol, diagnostika a signalizace
  - IGMP – skupinové adresování (multicast)
  - ARP, RARP – zjištění linkové adresy k IP adrese a opačně

Struktura IP paketu



IP adresa

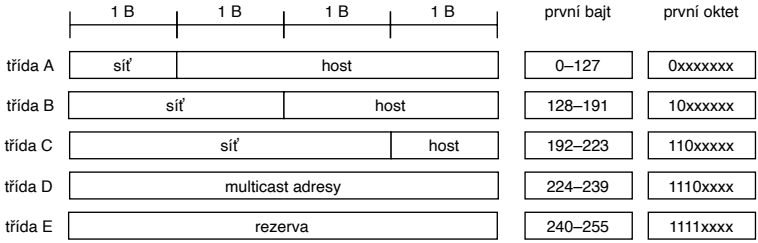
- IPv4 (32 bitů)
- IPv6 (128 bitů)
- IPv6 má jinou strukturu paketu!
- příklad (`phoenix.inf.upol.cz`):
  - `158.194.80.13`
  - `2001:718:1401:50:0:0:0:0d`, zkrácený formát `2001:718:1401:50::0d`

Odbočka: Omezení IPv4

- omezený (teoretický) maximální rozsah ($2^{32} = 4\,294\,967\,296$)
- pro lokální sítě dostatečný
- správa:
  - Internet Assigned Numbers Authority (IANA)
  - Regional Internet registry (RIR)
  - ISP
- IPv4 adresy již došli (na několika úrovních)
- proč stále není IPv6?
  - obtížně zapamatovatelné
  - IP adresy vnitřní a vnější sítě lze oddělit (NAT)
  - ISP neinvestují do infrastruktury

IP adresa

- classfull adresace
  - adresní prostor rozdělen do tříd: A, B, C, D, E
  - pevná část pro adresu sítě a adresu v síti



  - dnes se již (moc) nepoužívá
- classless adresace
  - síť je určena síťovou maskou
  - hierarchická adresace (adresa sítě, adresa podsítě, adresa uzlu)

IP adresa

- *maska sítě* = rozdělení na adresu sítě a adresu v sítí (adresa síťového rozhraní)
- příklad:
  - adresa sítě `192.168.1.0`
  - maska sítě: `255.255.255.0`
  - adresy v sítí: `192.168.1.1`–`192.168.1.254`
  - `192.168.1.255` vyhrazena pro broadcast
- používanější CIDR (Classless Inter-Domain Routing) formát `192.168.1.0/24`

adresa sítě 192.168.1.0/24

192								168								1								0							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0

maska sítě

255								255								255								0							
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0

IP adresa

adresa sítě 192.168.1.0/24

192								168								1								0							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0

první adresa v síti 192.168.1.1/24

192								168								1								1							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1

. . .

poslední adresa v síti 192.168.1.254/24

192								168								1								254							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0

broadcast v síti 192.168.1.255/24

192								168								1								255							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1

IP adresa

adresa sítě 192.168.192.0/18

192								168								192								0							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0

první adresa v síti 192.168.192.1/18

192								168								192								1							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1

poslední adresa v síti 192.168.255.254/18

192								168								255								254							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0

broadcast v síti 192.168.255.255/18

192								168								255								255							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

maska sítě

255								255								192								0							
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0

IP adresa: Poznámky

- první a poslední adresa je vyhrazena z praktických důvodů, nedodržení → problémy
- adresa sítě nemusí končit nulou!
  - `192.168.1.192/26` je adresou sítě
- síť s maskou /32 je adresa uzlu

IP adresa: Matika

- počet adres v síti:

$$2^{32-n}$$

  kde n je délka masky
- adresa sítě: IP_adresa `AND` maska
- broadcast adresa: IP_adresa `OR` (`NOT` maska)

Příklad

`167.199.170.82/27` má $2^{32-27} = 2^5 = 32$ adres. $82_{10} = 01010010_2$, posledních 5 bitů je adresa v síti, adresa sítě je tedy `167.199.170.64/27`. $82_{10} = 01010010_2$ `OR` $00011111_2 = 01011111_2 = 95_{10}$. Broadcast adresa je `167.199.170.95/27`

Speciální IP Adresy

IP adresa	popis
`127.0.0.1/8`	zpětná smyčka (loopback)
`10.0.0.0/8`	adresa lokální sítě (24 bitů na adresu v síti)
`172.16.0.0/12`	adresa lokální sítě (20 bitů na adresu v síti)
`192.168.0.0/16`	adresa lokální sítě (16 bitů na adresu v síti)
`192.168.x.0/24`	adresa lokální sítě (8 bitů na adresu v síti), `x` je 0–255
`0.0.0.0/32`	host, komunikace při které odesílatel nezná svoji IP adresu
`255.255.255.255/32`	omezený broadcast (pouze v lokální síti)

Tvorba podsítí

- sítě lze dále dělit na podsítě → organizace
- sítě lze spojovat do větších sítí
- manipulace (prodlužování, zkracování) s maskou sítě

adresa sítě 192.168.0.0

192								168								0								0							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

původní maska sítě /16

255								255								0								0							
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

nová (prodloužená) maska sítě /18

255								255								192								0							
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0

- znehodnocení adresního prostoru

Tvorba podsítí

- způsoby:
  - konstantní maska $\rightarrow$ stejně velké podsítě
  - variabilní maska $\rightarrow$ různě velké podsítě
  - separátní IP adres $\rightarrow$ reálně nemáme k dispozici
- postup:
  - počet adres N v každé podsíti musí být mocninou 2 (kvůli masce, $N = 2^{32-n} \rightarrow n = log_2(2^{32}/N) = 32 - log_2(N)$)
  - adresa sítě musí být dělitelná $N \rightarrow$ lze zajisti postupným přiřazováním adres dle velikosti podsítě (od největší po nejmenší)
  - délka masky $= n + log_2(N/N_{sub})$

Příklad

Pro tři počítačové učebny se 7, 10 a 40 počítači chceme vytvořit samostatné podsítě. Máme k dispozici síť `192.168.1.0/24`. V síti je $2^{32-24} = 256$ adres.

Tvorba podsítí: Konstantní maska

- síť rozdělíme na stejně velké podsítě
- vybereme největší podsíť → rovnoměrně rozdělíme adresní prostor dle její velikosti

Příklad (řešení – konstantní maska)

Největší podsíť má 40 uzlů, potřebujeme alespoň 6 bitů pro adresaci v síti ($2^5 = 32$, $2^6 = 64$) → maska /26.

podsíť	adresy v podsíti	broadcast
192.168.1.0/26	192.168.1.1/26 ... 192.168.1.62/26	192.168.1.63/26
192.168.1.64/26	192.168.1.65/26 ... 192.168.1.126/26	192.168.1.127/26
192.168.1.128/26	192.168.1.129/26 ... 192.168.1.190/26	192.168.1.191/26
192.168.1.192/26	192.168.1.193/26 ... 192.168.1.254/26	192.168.1.255/26

- nevyužité rozsahy
- zbytečně velké podsítě pokud je velký rozdíl mezi největší a nejmenší sítí

Tvorba podsítí: Variabilní maska

- pro každou podsíť určíme vhodný adresní prostor → menší plýtvání
- seřadíme podsítě dle jejich velikosti a postupně jim přidělujeme adresy

Příklad (řešení, začátek – variabilní maska)

Největší podsíť má 40 uzlů.

podsíť	adresy v podsíti	broadcast
192.168.1.0/26	192.168.1.1/26 ... 192.168.1.62/26	192.168.1.63/26

Další podsíť má 10 uzlů. Potřebujeme alespoň 4 bity pro adresaci ($2^4 = 16$).

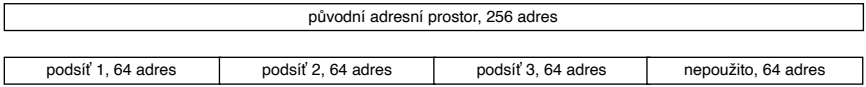
podsíť	adresy v podsíti	broadcast
192.168.1.64/28	192.168.1.65/28 ... 192.168.1.78/28	192.168.1.79/28

Poslední podsíť má 7 uzlů. Potřebujeme opět alespoň 4 bity pro adresaci. Pozor 3 bity nestačí! ($2^3 = 8$, není místo pro broadcast).

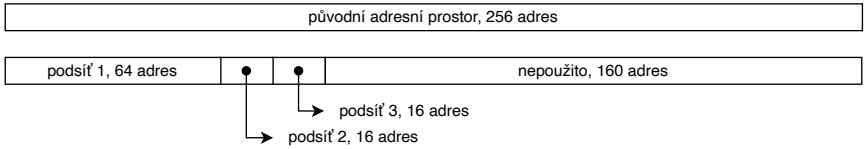
podsíť	adresy v podsíti	broadcast
192.168.1.80/28	192.168.1.81/28 ... 192.168.1.94/28	192.168.1.95/28

Tvorba podsítí: Ilustrace

- rozdělení konstantní maskou



- rozdělení variabilní maskou



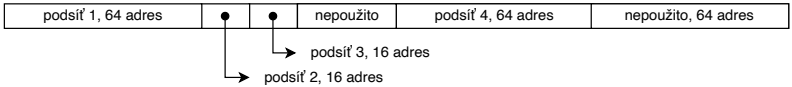
Variabilní maska: Použití zbylého prostoru

- 192.168.1.96/28 má adresní prostor 2^4, zbývá ale 160 adres

poslední oktet								poslední oktet dekadicky
0	0	0	0	0	0	0	0	0
0	0	1	1	1	1	1	1	63
0	1	0	0	0	0	0	0	64
0	1	0	0	1	1	1	1	79
0	1	0	1	0	0	0	0	80
0	1	0	1	1	1	1	1	95
0	1	1	0	0	0	0	0	96

- chceme přidat síť obsahující 50 uzlů (alespoň 6 bitů pro adresaci)

poslední oktet								poslední oktet dekadicky
1	0	0	0	0	0	0	0	128
1	0	1	1	1	1	1	1	191



Variabilní maska: Použití zbylého prostoru

- (nebo) chceme přidat síť obsahující 100 uzlů (alespoň 7 bitů pro adresaci)

poslední oktet								poslední oktet dekadicky
1	0	0	0	0	0	0	0	128
1	1	1	1	1	1	1	1	255

Spojování podsítí

- při tvorbě podsítí zůstává původní adresace nedotčena
- sítě lze opět spojovat = zkrátit masku sítě

Odbočka: Podsítě a Internet

- Internet = síť sítí
- supersíť = síťová maska nepokrývá celou adresu sítě (síť obsahuje podsítě), například `158.194.92.0/24` je součástí supersítě `158.194.0.0/16`.
- Internet se dělí na autonomní systémy (AS) = supersítě
- komunikace uvnitř AS a mezi AS
- informace o AS či adrese v rozsahu AS pomocí `whois`

Odbočka: Přidělení IP adresy

- statické
  - manuální konfigurace
- dynamické
  - DHCP protokol
  - klient-server služba
  - server zašle uzlu nastavení síťového rozhraní

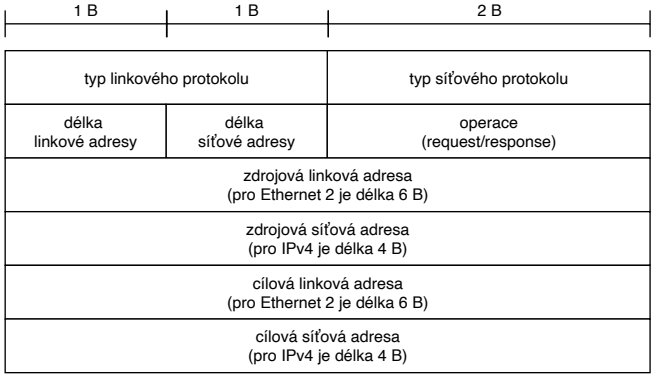
Komunikace v lokální síti

- = doručení mezi uzly v lokální síti
- na úrovni IP vrstvy máme pouze IP adresu
- komunikace v lokální síti → záležitost linkové (L2) vrstvy!
  - komunikaci v lokální síti lze snadno rozpoznat → zjistíme adresy sítí
- pro komunikaci je třeba adresa fyzického rozhraní (MAC adresa)
  - MAC adresa příjemce musí být vložena do linkového rámce
  - MAC adresu odesílatele známe
- je třeba zajistit překlad IP adresy na MAC adresu → protokol ARP
  - ARP se vkládá do linkového rámce
- poznámka: L2 zařízení se během výměny ARP zpráv „naučí“ MAC adresy na daných portech

Protokol ARP (Address Resolution Protocol)

- předpokládejme, že `192.168.1.1/24` (`A`) zná IP adresu se kterou chce komunikovat `192.168.1.2/24` (`B`)
- `A` nejprve pošle ARP paket (request) pomocí broadcastu
  - ptá se: „Kdo má v lokální síti IP adresu `192.168.1.2/24` pošli svoji MAC adresu.“
  - broadcast zpráva je rozeslána na úrovni L2 (switch)
  - `A` přiloží svoji IP adresu a MAC adresu
- pokud `B` obdrží request od `A`, odpoví mu pomocí ARP paketu (response)
  - odpověď je posílána jako unicast
- pokud `A` obdrží response od `B`, získá MAC adresu PC a může zahájit komunikaci

Protokol ARP: Ilustrace struktury



- pro Ethernet II a IPv4 je obrázek nepřesný!

ARP cache

- posílání ARP zpráv při odesílání každého linkového rámce je velmi neefektivní
- ARP cache = tabulka s dočasně uloženými MAC adresami (a jejich mapování na IP adresy)
- po čase dochází k zneplatnění informace v ARP cache
  - na klientech záležitost OS
- s ARP tabulkou je možné pracovat (vypsat, vymazat, změnit)
- nové ARP response přepisují staré hodnoty

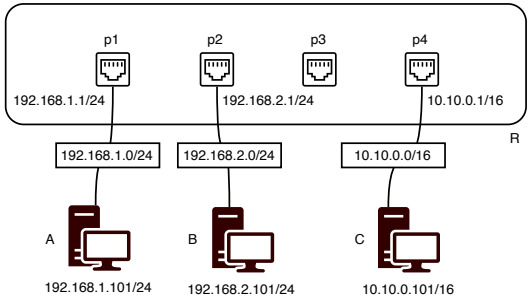
ARP: Poznámky

- ARP proxy
  - možnost propojení dvou nesousedních sítí
  - proxy zajistí přeposlání ARP paketu do jiné sítě
  - je třeba si uvědomit, že ARP samotný nemůže odejít do jiné sítě (je na úrovni L2)
- RARP (Reverse ARP)
  - dnes se již nepoužívá $\rightarrow$ DHCP
- útoky pomocí ARP
- statické ARP
  - zabránění automatické výměně zpráv
  - ARP cache je statická a neměnná $\rightarrow$ zvýšení bezpečnosti, ale snížení flexibility

Směrování mimo lokální síť

- paket je směrován mimo lokální síť
- záležitost L3 vrstvy!
  - komunikaci mimo lokální síť lze snadno rozpoznat → zjistíme adresy sítí
- řešeno pomocí *forwardingu* (předávání) paketů na síťových rozhraních jednoho zařízení
  - router (L3)
  - lze povolit v OS
- rozhodování o cestě paketu na základě *směrovací tabulky*

Směrování: Směrovací tabulka



cílová síť	gateway (next hop)	interface	metrika
192.168.1.0/24	0.0.0.0	p1	0
192.168.2.0/24	0.0.0.0	p2	0
0.0.0.0/0	10.10.0.101	p4	0

Směrování: Rozhodování

- postupný průchod směrovací tabulkou shora dolů
  1. vynásobení cílové adresy paketu s maskou sítě
  2. pokud je výsledek roven adrese sítě, paket se odešle skrze dané rozhraní na následující router nebo cílový uzel
     - odeslání do lokální sítě, next hop `0.0.0.0` → přímé směrování
  3. cílová síť `0.0.0.0/0` výchozí (implicitní) směr pro paket nevyhovující žádnému z předchozích záznamů (typicky směr do sítě Internet)
     - běžné označení: default gateway (výchozí brána)
- pokud router nedokáže rozhodnou kam má paket poslat, je zahozen (je odeslána informativní zpráva, protokol ICMP)
- záznamy v tabulce uloženy dle délky masky (od největší po nejmenší)
- agregace podsítí
- metrika = cena cesty, pokud existují dva záznamy pro daný cíl → menší hodnota metriky

Směrování: Naplnění směrovací tabulky

- tabulky jsou udržovány na každém uzlu v síti (včetně koncových)
- statické plnění
  - pracné/nemožné pro velké sítě
- dynamické plnění $\rightarrow$ pokryto v kurzu KMI/POS2
  - pomocí aplikačních protokolů
  - dělení podle použití
    - IGP – uvnitř AS, např. RIP, OSFP
    - EGP – mezi AS, např. BGP
  - dělení podle použitého algoritmu
    - lik-state, globální informace, např. Dijkskrův algoritmus hledání nejkratší cesty v grafu (OSPF)
    - distance-vektor, lokální informace, distribuovaný Bellman-Fordův algoritmus, (RIP)
    - path-vector, jako distance-vektor, ale využívá informace o cestě (BGP)

Doba životnosti paketu (TTL)

- zamezení nekonečného oběhu paketu
- každý směrovač snižuje o alespoň 1 $\rightarrow$ nutné přepočítat kontrolní součet záhlaví IP paketu
- dosažení hodnoty 0 je signalizováno služebním protokolem

Odbočka: Virtuální okruhy

- TCP/IP $\rightarrow$ nespojová služba
- síťová vrstva (obecně) může být řešena jako spojová (výhody vs nevýhody) $\rightarrow$ virtuální okruhy
- obvykle využito na úrovni velkých ISP
- směrování na základě popisku (labelu) paketu určující okruh
- MPLS (MultiProtocol Label Switching)
  - obaluje IP pakety
  - transparentnost $\rightarrow$ nižší a vyšší vrstvy nic netuší

Odbočka: Nástroje `ping` a `traceroute`

Překlad síťových adres

- NAT (Network Address Translation)
- oddělení IP adres v intranetové (lokální) síti od internetové (venkovní) sítě
- praktické důvody
- na úrovni L3
- překlad:
  - odchozímu (do venkovní sítě) IP paketu je změněna IP adresa odesílatele (adresa v lokální sítí) na venkovní adresu routeru
  - analogicky je měněna adresa příjemce v příchozím (do lokální sítě) IP paketu
  - řešeno pomocí překladové tabulky

Překlad síťových adres

- při odchozí komunikaci je vytvořen v překladové tabulce záznam (odkud, kam)
- při příchozí komunikaci je na základě tohoto záznamu změněna hlavička paketu
- komunikace musí být zahájena ve vnitřní síti! $\rightarrow$ má své výhody i nevýhody
  - NAT traversal techniky
- problém: více hostů nemůže komunikovat současně s jedním příjemcem $\rightarrow$ lze omezeně řešit použitím více tabulek
- plnohodnotné řešení vyžaduje informace z L4 (port)
- poznámka: dnes nutnost, ale má řadu negativ
  - narušuje nezávislost L4 a L3 vrstev
  - narušuje end-to-end komunikaci

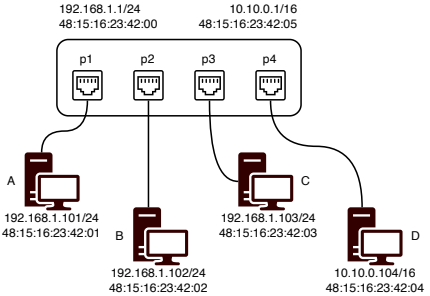
Překlad síťových adres: Praktické poznámky

- běžná funkce
- Dynamic NAT – více veřejných IP adres rozděleny uzlům v intranetu → omezené řešení → lépe porty (L4)
- Static NAT – mapování veřejné (internetové) IP adresy na adresu ve vnitřní síti → lze přistoupit z internetu do intranetu
- source NAT – překlad adresy odesílatele
- destination NAT – překlad adresy příjemce
- maškaráda = automatický source NAT (není třeba uvádět veřejnou adresu, problémy při reinicializaci)

Filtrace

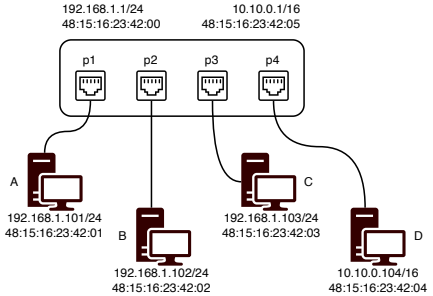
- pakety mohou být v průběhu směrování filtrovány
  - směrování je složeno z více částí (různá zařízení, různé postupy zpracování paketů, tzv. *packet flow*)
  - např. přijetí, odeslání, forwardování, ...
- významný bezpečností prvek $\rightarrow$ firewall
- podrobněji popíšeme v kontextu L4 vrstvy

Směrování na L3: Shrnutí



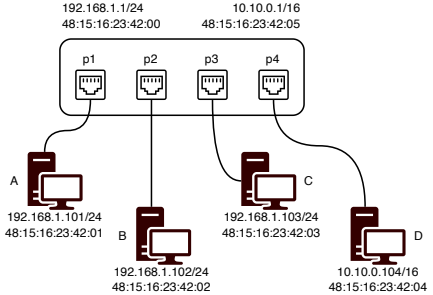
- komunikace v lokální síti `192.168.1.101` (`A`) → `192.168.1.103` (`C`), přes `R`
  - `A` zjistí, že je adresována lokální síť (z masky)
  - `A` použije směrovací tabulku pro zjištění cesty (přes `R`) k lokální síti
  - výměna ARP zpráv mezi `A` a `C` (`R` zařízení se naučí MAC adresy na `p1` a `p3`)
  - `A` pošle data (linkový rámec + IP paket + další)
  - `R` zařízení zná MAC příjemce → nepotřebuje data z IP a data doručí

Směrování na L3: Shrnutí



- komunikace mimo lokální síti `192.168.1.101` (`A`) → `10.10.0.104` (`D`), přes `R`
  - `A` zjistí, že je adresována adresa mimo lokální síť (z masky)
  - `A` použije směrovací tabulku pro zjištění cesty (přes `R`) k této síti
  - výměna ARP zpráv mezi `A` a `R` zařízením (`R` se naučí MAC adresu na `p1`)
  - `A` pošle data (linkový rámec + IP paket + další)
  - `R` identifikuje, že je příjemcem → potřebuje data z IP pro doručení dat
  - ...

Směrování na L3: Shrnutí



- komunikace mimo lokální síti `192.168.1.101` (`A`) → `10.10.0.104` (`D`), přes `R`
  - . . . pokračování
  - `R` použije směrovací tabulku pro zjištění cesty k síti příjemce (v našem případě triviální přímé směrování, obecně může být další router)
  - `R` vytvoří nový linkový rámec (potřebuje MAC adresu, buď zná nebo zjistí pomocí ARP)
  - pokud je použit NAT je vytvořen nový IP paket
  - `R` předá data (skrze `p4`) . . .

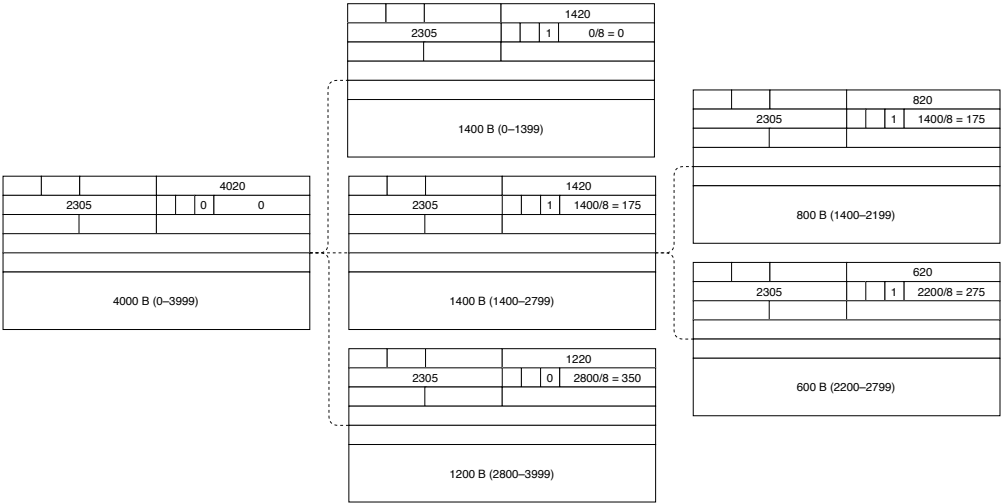
Fragmentace paketu

- paket může cestovat přes různé sítě, vždy dochází k vybalení z linkového rámce a následnému zabalení do nového
- různé (fyzické) technologie → různé linkové rámce (zejména velikost)
- MTU (Maximum Transfer Unit) – maximální velikost dat, které lze přenést v jednom linkovém rámci
- IP paket je omezen na 65535 B
- ideálně velikost IP paketu = MTU
- pokud se IP paket nevejde do linkového rámce → fragmentace
  - data jsou rozdělena do několika paketů (fragmentů), každý je posílán samostatným rámcem
  - každý fragment obsahuje část dat (část IP paketu) + data z původní hlavičky + režijní informaci
  - sestavení fragmentů je na příjemci
  - o fragmentaci může požádat odesílatel nebo jakýkoliv router na cestě

Fragmentace paketu

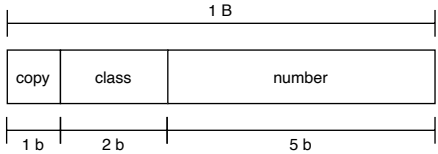
- režijní informace je uložena v hlavičce IP
- identifikátor (16 b)
  - identifikátor + IP odesílatele = jedinečný identifikátor paketu
  - při fragmentaci je identifikátor kopírován do každého fragmentu
- příznaky (3 b)
  - první bit je nepoužit
  - druhý indikuje „do not fragment“ (pokud je nastaven na 1, je zakázána fragmentace → paket nemusí být možné doručit)
  - třetí bit indikuje „more fragment“ (pokud je nastaven na 1, nejedná se o poslední fragment), pokud paket není fragmentován → poslední fragment
- fragmentační odsazení (13 b)
  - data dělena do 8 B bloků dat
  - relativní pozice bloku vzhledem k původním datům

Fragmentace paketu: Ilustrace



Volitelné položky v záhlaví IP paketu

- až 40 B
- zapisovány ve tvaru typ (8 b), délka hodnoty (8 b), hodnota (proměnlivá) → type-length-value (TLV)
  - typ má strukturu



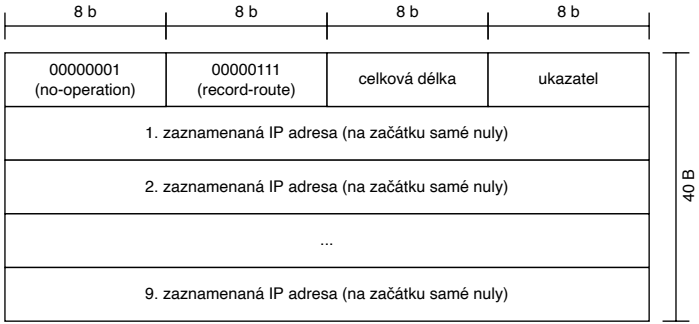
  - copy – určuje zda kopírovat volitelné položky při fragmentaci
  - class – obecné určení paketu (00 – řízení paketu, 10 – správa a ladění), ostatní jsou nedefinované)
  - number – určení konkrétní typu položky (používá se pouze 6)

Volitelné položky v záhlaví IP paketu

- značně zjednodušeno (uloženi režijní informace je nad rámec kurzu)

kód	název	popis
00001	no-operation	žádná operace, slouží pro zarovnání, má pouze 1 B
00000	end-of-option	konec položky, slouží pro zarovnání, má pouze 1 B
00111	record-route	zaznamenávání IP adres routerů, například `ping -r`
01001	strict-route	seznam IP adres routerů přes které paket musí jít (pokud jde přes jiné, je zahozen)
00011	loose-source-route	seznam IP adres routerů přes které paket musí jít (může jít i přes jiné, pokud nenavštíví všechny, je zahozen)
00100	timestamp	zaznamenávání času zpracování paketu routerem

Příklad: record-route

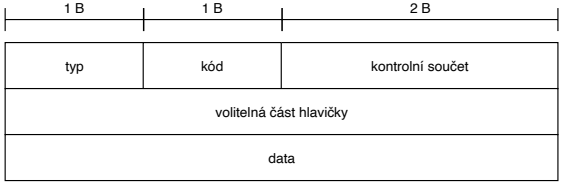


Kontrolní součet hlavičky IP paketu

- pouze hlavička IP paketu (integritu dat řeší L4 vrstva)
- idea výpočtu
  - hlavička se rozdělí na části po 16 bitech
  - provede se logický součet položek
  - v položkách je i položka pro samotný kontrolní součet $\rightarrow$ nastavena na 0
  - do položky kontrolní součet se uloží (bitová) negace výsledku
- příjemce provede stejný součet, pokud je nenulový paket je zahozen
- obecně považováno za nespolehlivé

ICMP protokol

- Internet Control Message Protocol, RFC 777, vkládá se do IP protokolu



- služební protokol pro diagnostiku a signalizaci (chybových) stavů
  - echo – ping
  - time exceeded – vypršel TTL
  - destination unreacheble – nedoručitelný paket
  - mnoho další
- v datové části je hlavička IP paketu + prvních 8 bajtů datové části IP paketu (důležitá data)
- kontrolní součet jako u IP, ale z celých dat
- některých situacích není generována ICMP zpráva: ztráta ICMP zprávy, ztráta fragmentu, který není prvním fragmentem, ztráta IP paketu v rámci multicast komunikace

Odbočka: Multicast

- výrazné snížení zátěže odesílatele
- router může předat paket na více rozhraní
- rozdělení do (multicast) skupin (uzly se hlásí do skupiny, mohou být členy více skupin)
- vyhrazeny adresy třídy D (různé účely)
- např. `224.0.0.0/24` lokální multicast (TTL=1)
- protokol IGMP (Internet Group Membership Protocol), různé verze
- problém: ARP neřeší mapování multicast adres na MAC

Odbočka: Multicast

- řešení:
  - pro multicast MAC adresy vyhrazena polovina rozsahu daného prefixem `01:00:5e`
  - v nejvyšším bitu 4. bajtu MAC adresy musí být `0` → pro mapování zbývá 23 bitů MAC adresy
  - multicast IP adresy (třída D) vždy začínají `1110` → musí se mapovat 28 bitů
  - posledních 23 bitů multicast IP adresy se přímo zkopíruje do posledních 23 bitů MAC adresy (5 bitů je tedy nevyužito)
  - 32 IP multicast skupin se vždy mapuje na jednu multicast MAC adresu (mapování není jednoznačné) → filtrace na úrovni IP vrstvy
- multicast mimo lokální síť → poměrně složitá záležitost

Bezpečnost protokolu IP

- bezpečnostní problémy
  - odposlouchávání paketů → nelze zabránit → data musí být šifrována (obvykle ponecháno na vyšší vrstvě)
  - úprava obsahu (dat) paketu → integritu dat (obvykle ponecháno na vyšší vrstvě)
  - podvržení IP adresy → data musí být ověřena (autentifikace, obvykle ponecháno na vyšší vrstvě)
- IPSec (IP Security) řeší bezpečnost na úrovni IP vrstvy
  - (transparentní) šifrování dat, integrita a autentifikace
  - transportní režim (chráněna pouze data z L4 vrstvy)
  - tunelový režim (chráněn celý IP paket) → je vytvořen nový paket
  - dva bezpečnostní protokoly: protokol AH pouze integrita a autentifikace (data nejsou šifrována), nebo protokol ESP integrita, autentifikace, šifrování

Virtuální privátní sítě (VPN)

- přístup do privátní (bezpečné) sítě skrze veřejnou (nebezpečnou) síť
- vzdálený počítat se chová jako počítač připojený do lokální sítě
- služba klient-server
- klient vytváří zabezpečený tunel s VPN serverem (například pomocí IPSec $\rightarrow$ překonáno)
- VPN server je zodpovědný za dešifrování dat $\rightarrow$ bezpečnostní důsledky