INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Tato publikace je spolufinancována Evropským sociálním fondem a státním rozpočtem České republiky

Registrační číslo projektu: CZ.1.07/1.1.12/01.0004

Studijní materiál

CCNA Exploration – Základy sítí

(Semestr 1)

VOŠ a SPŠE Plzeň

2011

Tato publikace je spolufinancována Evropským sociálním fondem a státním rozpočtem České republiky v rámci projektu „Výuka počítačových sítí v mezinárodním programu Síťová akademie Cisco na střední průmyslové škole elektrotechnické“.

Registrační číslo projektu: CZ.1.07/1.1.12/01.0004.

Vydala VOŠ a SPŠE Plzeň, Koterovská 85, 326 00 Plzeň v roce 2011.

Kolektiv autorů (řešitelé projektu):

- ***Koncepce a text:*** ***Ing. Miroslav Páv***
- ***Vektorová grafika:*** ***Mgr. Jan Syřínek***
- ***Konzultace angličtiny:*** ***Mgr. Jana Hošková***

- *Tato publikace je určena jako doplňkový studijní materiál ke kurzu **CCNA Exploration – Network Fundamentals**. Nejedná se o doslovný překlad celého kurikula ale o nově vytvořené vlastní výklady podporující představivost žáků a komentované upravené překlady vybraných částí jednotlivých kapitol anglického kurikula určené pro usnadnění výuky i studia originálního kurzu v prostředí české odborné střední školy.*
- *Obsah kurzu je integrován v rámci ŠVP naší školy.*
- *Tento dokument je zpracovaný v kancelářském balíku OpenOffice.org a jeho vektorová grafika v grafickém editoru Dia.*
- *Protože se jedná o materiál podléhající v rámci projektu průběžné aktualizaci, používejte vždy poslední dostupnou verzi.*
- *Pro zachování vazby na původní učební materiály (kurikula) jsou u českých termínů uváděny i jejich anglické originály.*
- *Aktuální verze originálních materiálů v angličtině (pro registrované účastníky programu NetAcad): http://www.cisco.com/web/learning/netacad/index.html (http://cisco.netacad.net, www.cisco.com/go/netacad , http://www.cisco.com/edu)*

*Pokud tuto publikaci používáte při své výuce, prosím Vás o informaci o této skutečnosti. Na tuto publikaci navazuje obdobně zpracovaný materiál pro druhý semestr (Směrování, koncepce a protokoly). Věcné a konstruktivní připomínky, náměty i popřípadě nalezené chyby mi zasílejte, prosím, na adresu: pav@spse.pilsedu.cz, věc: **CCNA_Exploration_1_TISK.PDF (verze: 3.04)**.*

Vaší spolupráce si vážím a děkuji Vám za ni!

Za kolektiv autorů

Miroslav Páv, CCNA CCAI

Obsah

CCNA Exploration – Základy sítí

Upozornění: Tento materiál v žádném případě nenahrazuje samotné kurikulum ani Vaše vlastní školní poznámky.

- *Pro procvičování jednotlivých příkazů a celých konfigurací sítí používejte **simulátor Packet Tracer** (v poslední dostupné verzi).*
- *Pro analýzu síťového provozu na stanici používejte **analyzátor síťových protokolů WireShark** v režimu **s právy lokálního administrátora na stanici**.*
- *Samostatně si odpovídejte na kontrolní otázky v souhrnu a kvízu pro každou kapitolu v kurikulu.*
- *Postupujte podle pravidla: **pochopit – naučit se – procvičit – otestovat znalosti i dovednosti**.*
- *Při nastavování na reálných zařízeních v učebně i pro PacketTracer používejte stále stejná následující hesla:*
  - *pro privilegovaný režim enable: **cisco***
  - *pro linku vty - telnet a také pro linku konzole: **class***

CCNA Exploration – představení programu

NetAcad - Cisco Networking Academy (CNA, CNAP) – Program **Síťová akademie Cisco** je komplexní e-learningová iniciativa firmy Cisco, která studentům umožní, aby si vybudovali hodnotné dovednosti z informačních a komunikačních technologií (ICT), které zvýší jejich možnosti přístupu k příležitostem globální ekonomiky.

CCNA[1] Exploration[2] je srozumitelný a zevrubný úvodní kurz do počítačových sítí od základů až k pokročilým aplikacím založený na dekompozičním přístupu výkladu shora dolů tak, aby se při výuce zdůraznily jak teoretické koncepce tak i jejich praktické aplikace.

Kurz CCNA Exploration se skládá ze čtyř semestrů:

1. Základy sítí (*Network Fundamentals*),
2. Směrovací protokoly a základy směrování (*Routing Protocols and Concepts*),
3. Přepínání v lokálních sítích LAN a bezdrátové sítě (*LAN Switching and Wireless*),
4. Připojování k rozsáhlé síti typu WAN (*Accessing the WAN*).

Přehled kvalifikačních stupňů a požadavky na ně kladené

1. Technik PC (*PC Technician*) – studenti aktuálně zapsaní v kurzech IT Essentials nebo absol-

1 CCNA = Cisco Certified Network Associate = název mezinárodní průmyslové certifikace pro síťové pracovníky (640-802 CCNA EXAM).

2 Souběžný kurz **CCNA Discovery** (objevná cesta) je určen pro uživatele zaměřené více prakticky a méně teoreticky, pro správu malých sítí. Výuka probíhá na základě používání síťových aplikací. Kurz **CCNA Exploration** (výzkumná cesta) je určen pro ty, kdo se chtějí počítačovými sítěmi později zabývat i na vysoké škole, pro správu velkých podnikových sítí. Výuka probíhá na základě pochopení a schopnosti použití jednotlivých technologií a protokolů.

venti (*alumni*), kteří mají dokončené pouze tyto kurzy v Cisco Networking Academy, by mohli zvolit tuto kategorii.

2. Technik sítě (*Network Technician*) - studenti aktuálně zapsaní v kurzech CCNA 1, CCNA 2, CCNA Exploration 1 nebo 2, CCNA Discovery 1 nebo 2 nebo absolventi, jejichž nejvyšší stupeň dokončených kurzů v Cisco Networking Academy byl kterýkoliv z výše uvedených, by mohli zvolit tuto kategorii. Na této úrovni lze složit zkoušku 640-822 ICND1 pro získání průmyslové certifikace CCENT (*Cisco Certified Entry Networking Technician*).
3. Síťový pracovník na vstupní úrovni znalostí (*Network Associate*) - studenti aktuálně zapsaní v kurzech CCNA 3, CCNA 4, CCNA Exploration 3 nebo 4, CCNA Discovery 3 nebo 4, nebo absolventi, jejichž nejvyšší stupeň dokončených kurzů v Cisco Networking Academy, byl kterýkoliv z výše uvedených by mohli zvolit tuto kategorii. (Předpokládá se úplná středoškolská kvalifikace.) Na této úrovni lze složit zkoušky 640-822 ICND1 a 640-816 ICND2 popřípadě jednu kompozitní zkoušku 640-802 CCNA pro získání průmyslové certifikace CCNA (*Cisco Certified Network Associate*).
4. Síťový profesionál (*Network Professional*) - studenti aktuálně zapsaní v kurzech CCNP, Network Security, nebo Fundamentals of Wireless LANs nebo absolventi, jejichž nejvyšší stupeň dokončených kurzů v Cisco Networking Academy byl kterýkoliv z výše uvedených, by mohli zvolit tuto kategorii. (Předpokládá se úplná vysokoškolská kvalifikace.) Na této úrovni lze složit zkoušky 642-902 ROUTE, 642-813 SWITCH a 642-832 TSHOOT pro získání průmyslové certifikace CCNP (*Cisco Certified Network Professional*).
5. Instruktor Síťové Akademie prokazuje certifikací CCAI (*Cisco Certified Academy Instructor*) ke své průmyslové certifikaci (CCNA nebo CCNP) svoji profesionalitu při poskytování potřebné podpory žáků při výuce ve třídě.

Kurz CCNA Exploration - Základy sítí

Základní dovednosti a kompetence absolventa kurzu ***CCNA Exploration Network Fundamentals*:**

- Používá síťové protokolové modely k vysvětlení jednotlivých vrstev komunikací v datových sítích
- Navrhuje, vypočítává a používá masky podsítí a jejich adresy
- Navrhuje a sestavuje jednoduché sítě Ethernet s použitím přepínačů a směrovačů
- Využívá základní struktury sítě a znalost budování síťové kabeláže k propojování jednotlivých síťových zařízení
- Používá příkazovou řádku a konzolové příkazy k základnímu nastavení směrovače a přepínače a k ověření jejich správného chodu
- Analyzuje činnost i funkci protokolů a služeb transportní a síťové vrstvy

Obsah kursu **CCNA Exploration Network Fundamentals:**

1 Úvod do předmětu - život a komunikace v zasíťovaném světě
1.1 Síť jako platforma (části počítačové sítě, konvergované sítě)

Úvod ke kurzu

Kurz se skládá z následujících částí:

- Prezentace, diskuse a cvičení ve třídě s vaším instruktorem
- Praktická cvičení v laboratoři síťové akademie
- Online testování vašich znalostí (pro sebehodnocení (*self-assesment*): kvízy, pro externí (= školní) hodnocení (*assesment*): testy *(**minimálně** je potřeba získat 60% bodů ze 100% možných)*).
- Výukový SW pro simulaci a virtualizaci sítě (**Packet Tracer** v poslední dostupné verzi)
- Další SW pro aktivity ve třídě (např. analyzátor síťových protokolů - **Wireshark**)

Online materiály pro kurz:

- http://www.cisco.com/web/learning/netacad/index.html
- http://cisco.netacad.net
- https://cisco.netacad.net/cnams/dispatch

Potřebné vybavení: prohlížeč (*Web Browser*) s pluginem Adobe (Macromedia) Flash Player a povolená vyskakovací okna.

Nové motto NetAcad programu „*Mysl široce otevřená*“ (*Mind Wide Open*™) vás má motivovat k samostatné vlastní činnosti, instruktor vás v tom *„jenom“* podporuje. Ale vy sami si musíte dát svůj vlastní osobní závazek, že se opravdu budete učit nové znalosti a dovednosti. K tomu vám pomůže několik následujících **doporučení**:

1. Dělejte si své **vlastní poznámky**,
2. **Přemýšlejte** o tom,
3. **Procvičujte** své dovednosti v praxi,
4. A ještě jednou je procvičujte,
5. Zkuste **své znalosti naučit spolužáka** (to, co nejste schopni vysvětlit druhému, to neumíte[3]),
6. **Prohlubujte své znalosti** na základě zpětné vazby kvízů a testů.

Orientace - určení aktuální detailní polohy - v systému on-line kurzů:

- Kurz (*Course*) (*CCNA Exploration*),
- Kurikulum (*Curriculum*) (*Network Fundamentals*),
- Kapitola (*Chapter*), v předchozích verzích modul (formát čísla kapitoly: 9)
- Sekce (*Section*) (9.9),
- Téma (*Topic*) (9.9.9),
- Aktuální stránka v tématu (pouze číslo v zeleném kruhu - bez názvu) (*Location Box*) (9.9.9.9).

3 Lucius Annaeus Seneca: “Když lidé vyučují, sami se učí.“ (*Homines dum docent, discunt.*)
"If you can't explain it, you don't know it."

Kapitola 1 – Život ve světě soustředěném kolem sítě

V této kapitole se naučíme:

- Popsat, jaký vliv mají sítě na náš běžný život
- Popsat roli datových sítí na společenské sítě lidí
- Identifikovat klíčové komponenty každé datové sítě
- Identifikovat příležitosti a problémy použití konvergovaných sítí
- Popsat charakteristiky moderní síťové architektury: odolnost vůči chybovým stavům, škálovatelnost, kvalita služby a bezpečnost

Základní termíny

- **Informace** (*information*) - laická definice informace = zpráva (*message*) o reálném prostředí a o (nových) skutečnostech. Informace je to, jakým způsobem člověk interpretuje data.
- **Počítač** (*computer*) – stroj na zpracování informací.
- **Data** (*data*) - části informace uložené v počítači jako jsou soubory, audio, telefonní hovory a video sdílené přes síť (reprezentace informace v počítači).
- **Jednotky pro data** (*data units*) (informace uložené v počítači): **bit** (*binary digit*), **byte** (=1 oktet = 8 bitů, slabika), word (16 bitů, slovo).
- **Komunikace** (*communication*) – sdělování informací - výměna dat (síťového provozu) mezi síťovými zařízeními během jedné transakce.
- **Transakce** – neboli **úkol aplikace** je základní jednotka uživatelovi aktivity v kontextu aplikace. (Například čtení e-mailu, zápis do kalendáře jsou všechno úkoly.)
- **Datová síť** – digitální síť[4] podporující přenos zpráv (dat) (= komunikaci) mezi jednotlivými počítači (někdy se též nazývá informační či komunikační síť). (V dalším textu bude pod pojmem síť míněna právě datová síť.)
- **Síťová infrastruktura** (*network infrastructure*) – všechny navzájem spojené součásti sítě, které zajišťují její správnou činnost v nějaké geografické oblasti.
- **Internet** – veřejně přístupná globální (datová) **síť vzájemně propojených (datových) sítí** („síť sítí“, *network of networks*), které přenášejí data pomocí protokolu IP (*Internet Protocol*) (**protokolové sady TCP/IP**) a metody **přepínaných paketů**[5].
- **ISP** – *Internet Service Provider* – poskytovatel internetového připojení, od něho máte v domácnosti i ve firmě přiveden Internet.

Pravidla (nazývající se **protokoly[6])** pro úspěšnou **komunikaci** (= předávání zpráv, sdělování) v datové síti i u mezilidské komunikace musí obsahovat:

- jednoznačnou identifikaci odesílatele a příjemce,
- dohodnutou metodu komunikace,
- společný jazyk a gramatiku,
- rychlost a časování doručení,

4 Síť – obecně - jde o soubor zařízení nebo skupinu osob určených pro rozvod nebo svod nějakých médií nebo informací (sociální síť, železniční síť, telefonní síť, ...). My se budeme zabývat datovou informační sítí.

5 Internetworking znamená v angličtině propojování sítí. Zkrácením vznikl název Internet. Autorem uvedené definice Internetu je Vint Cerf - „otec Internetu“ (http://en.wikipedia.org/wiki/Vint_Cerf).

6 Protokol = soubor (syntaktických a sémantických) pravidel (předpisů) pro výměnu informací prostřednictvím datové sítě. Protokoly jsou veřejné (public) nebo neveřejné (soukromé, proprietary).

- požadavky na potvrzování doručení dat.

Kvalita komunikace (*QoS – Quality of Service*) (ohodnocení dat z jednotlivých aplikací, nastavení priorit, vytváření front (*queue*) dle priorit, přednostní vyřizování prioritních úloh (například hlasové služby, kontinuální streamové video atp.)) – nový přístup k Internetu ve srovnání s původním přístupem (*Best Effort* – tj. „Dělám co můžu“), kdy nikdo nemá (neměl) prioritu.

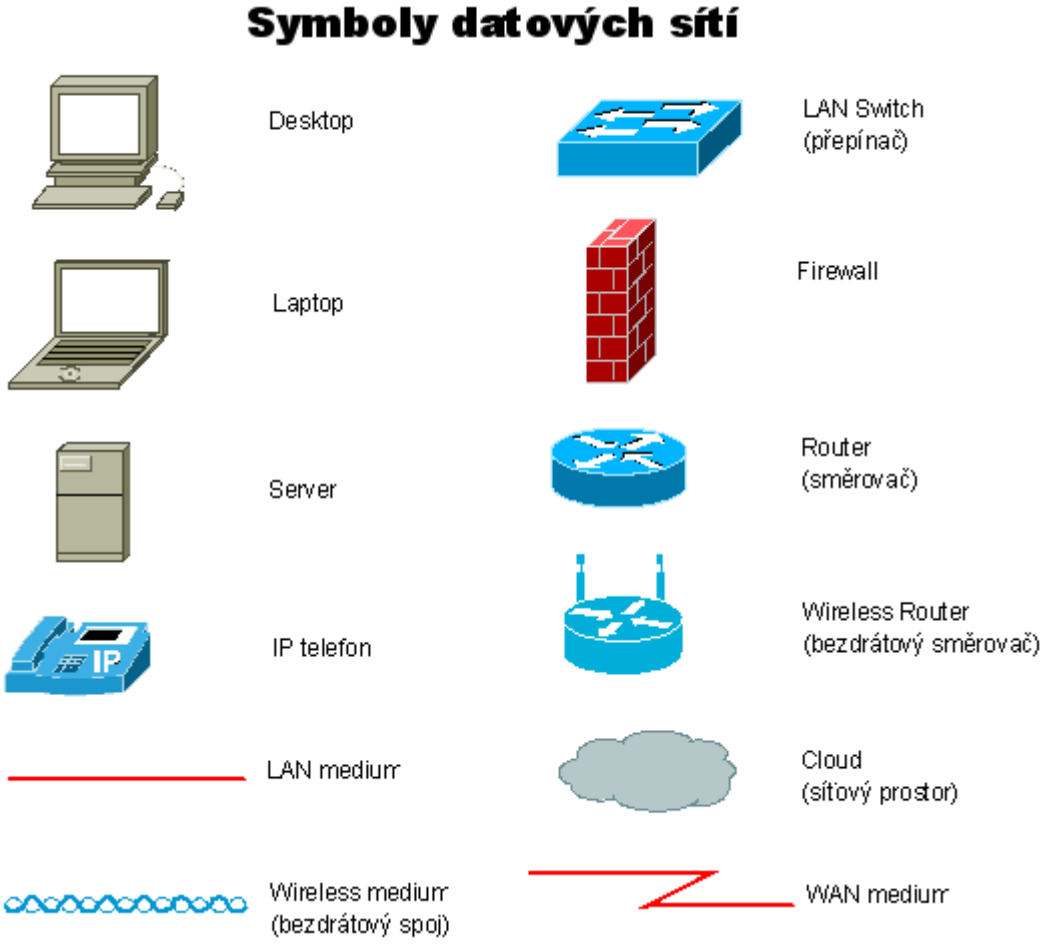
- **Interní faktory** (vlastnosti samotné přenášené zprávy) které mají vliv na **kvalitu (mezilidské i síťové) komunikace:**
  - velikost zprávy,
  - komplexnost zprávy (jednodušší zpráva se snáze pochopí),
  - důležitost zprávy.
- **Externí faktory**, které mají vliv na kvalitu (mezilidské i síťové) komunikace:
  - určení odesílatele a příjemce,
  - jestli bylo přijetí zprávy potvrzeno příjemcem odesílateli,
  - kvalita přenosové cesty mezi odesílatelem a příjemcem,
  - kolikrát zpráva měnila svoji formu,
  - množství jiných zpráv v komunikační síti,
  - kolikrát byla zpráva přeformátovávána,
  - množství vyhrazeného času pro úspěšnou komunikaci.

Základní součásti (komponenty) datové sítě:

- **pravidla a standardy** *(rules and standards)*
  - **protokoly a normy –** *protocols and standards* (IPv4, TCP, TIA/EIA 568A, ...),
  - **služby sítě** – *network services* (Instant Messaging, e-mail, sdílení souborů, WWW, IP telefonie, IPTV, ...) - síťové služby jsou realizovány právě pomocí jednotlivých protokolů,
- **přenosové médium** *(medium)* (drátové: metalické a světlovodné, bezdrátové: ...),
- **síťová zařízení** *(devices)*
  - propojovací zařízení (*Intermediary Devices*):
    - přístupová zařízení k síti (*Network Access Devices*) uvnitř jedné sítě: switch, hub, AP (*Wireless Access Point*), ... ,
    - propojovací zařízení mezi sítěmi (*Internetworking Devices*): router,
    - komunikační servery, modemy
    - bezpečnostní zařízení: firewall
      - účelem těchto propojovacích zařízení je:
        - obnova a znovu odvysílání datových signálů,
        - správa informací o existujících cestách v síti a a mezi sítěmi,
        - oznamování vzniku chyb a selhání ostatním zařízením,
        - nalezení alternativní cesty při selhání linky,
        - klasifikace a obsluha zpráv ve frontách dle priorit QoS
        - povolení nebo zákaz toku dat v závislosti na nastavení zabezpečení.
  - koncová zařízení *(end devices)*:
    - počítač, IP telefon, PDA, ... ,
      - účelem koncových zařízení je vytvářet a přijímat zprávy *(message)*,
  - **přenášené zprávy** *(messages)* (v binárně zakódované podobě).

Pravidla, média a síťová zařízení se také nazývají **síťová infrastruktura** *(network infrastructure)*.

Síťová architektura popisuje fyzickou infrastrukturu sítě a použité služby a protokoly.

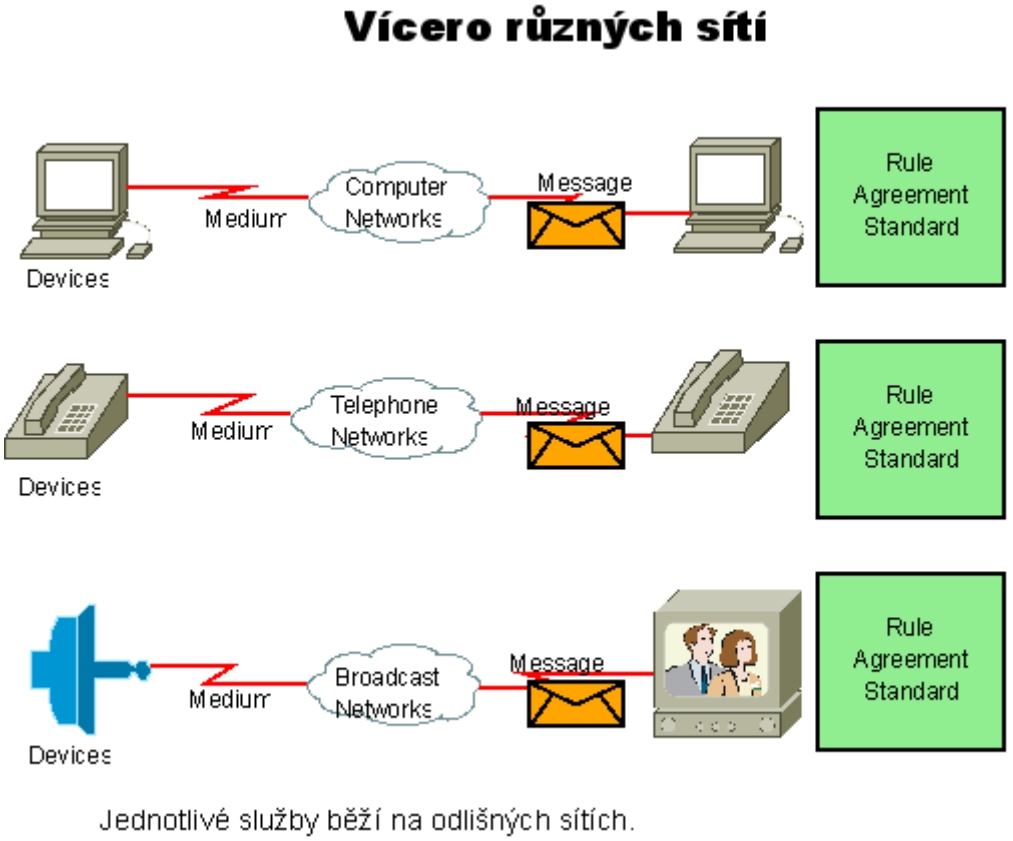


Oblíbené soudobé komunikační nástroje (příklady):

- *Instant Messaging (IM)* – okamžitá komunikace (v reálném čase) mezi lidmi po síti obvykle v textovém tvaru,
- Blogy (*Weblogs*) – umožňují komukoliv globálně publikovat v podstatě bez technických znalostí,
- Wiki – webové stránky, které může současně editovat a číst celá skupina lidí, některé firmy používají Wiki jako prostředek pro vzájemnou spolupráci zaměstnanců,
- Podcasting – médium založené na stahování zvukových záznamů do přenosných přehrávacích zařízení (iPod) a jejich přehrávání,
- nástroje pro týmovou spolupráci a komunikaci - nástroje podporující spolupráci lidí (*collaboration tool*) jsou nástroje umožňující současnou spolupráci více lidí nad jedněmi daty (například WebEx – pro videokonference, vzdálenou podporu a webináře), sociální sítě (Facebook, ...).

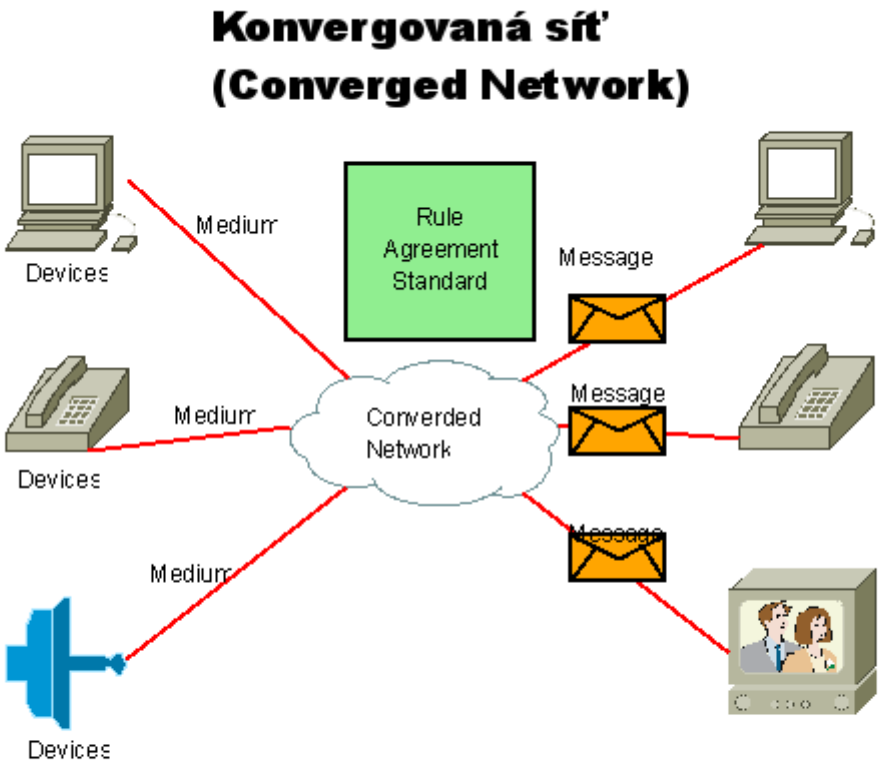
Koncový uživatel používá **služby sítě** (**síťové služby,** *network services*) prostřednictvím **síťových aplikací**. Příklady služeb (tyto **služby** jsou bezprostředně používány síťovými **aplikacemi**) a **protokolů** realizujících příslušnou službu na aplikační vrstvě (vrstvového síťového modelu):

Služba sítě	***Protokol***
World Wide Web (WWW)	HTTP (Hypertext Transport Protocol), HTTPS (HTTP over Secure Socket Layer)
E-mail	SMTP (Simple Mail Transport Protocol) POP (Post Office Protocol) IMAP (Internet Message Access Protocol)
Instant Message (IRC[7], ICQ, Jabber, AIM)	XMPP (Extensible Messaging and Presence Protocol) OSCAR (Open System for Communication in Realtime)
IP Telefonie (VoIP)	SIP (Session Initiation Protocol)
Přenos souborů	FTP (File Transfer Protocol), SFTP, scp
Vzdálené přihlášení (virtuální terminál)	Telnet, ssh



Přechod od (staré, zastaralé) struktury paralelních sítí pro jednotlivé paralelní síťové služby k moderní **konvergované síti** (=> jedna síť = jedna platforma pro všechny datové služby (aplikace v reálném čase, web, transakční provoz, *streaming* (kontinuální zpracování - například videa nebo audia), hromadný přenos dat (*bulk copy*)) (nebo též text, grafika, audio, video přes mobilní datovou síť)).

7 IRC - Internet Relay Chat, jeden z prvních systémů pro internetové „chatování“.



Konvergované datové sítě přenášejí jednotlivé odlišné služby po jedné síti.

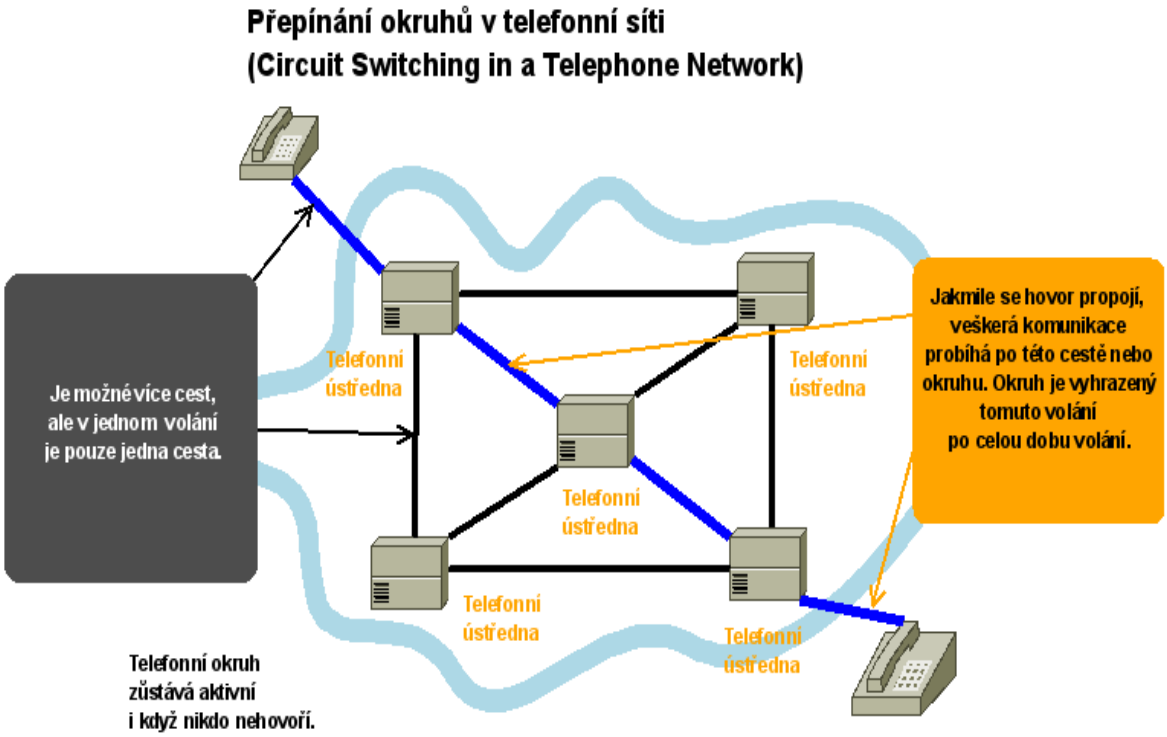
Požadavky na (moderní) síťovou architekturu:

- **odolnost vůči chybovým stavům** (např kolapsu jedné přenosové trasy – přechod od přepínání okruhů (přepojování okruhů) (klasický telefon) k **přepínání paketů** (zpráva rozdělena na malé kousky (pakety), každý putuje „svojí“ cestou).
- **škálovatelnost** (*scalability*) snadná **rozšiřitelnost** v nějakém předem daném rámci, rozsahu),
- **kvalita služby (QoS)** (mechanismy front a priorit dat) – udržuje v rovnováze zprávy dle jejich důležitosti a charakteru za účelem obratného zacházení s nimi („důležitější“ komunikace má prioritu),
- **zabezpečení dat (*security*)**:
  - **důvěrnost** (*confidentiality*, *privacy*) - utajení dat a jejich zpřístupnění pouze oprávněným uživatelům - zajištěno pomocí:
    - **autentizace** (*Authentication*) - ověření přihlášení oprávněného uživatele,
    - **autorizace** (*Authorization*) – povolení konkrétních přístupových práv,
    - **audit** (*Accounting*) – evidence jednotlivých transakcí v síti (transakční logy)[8],
    - šifrování (*encryption*) (proti neoprávněnému zachycování zpráv),
    - firewall,
  - **integrita** (*integrity*) – ověření nepozměněnosti dat - zajištěno pomocí:

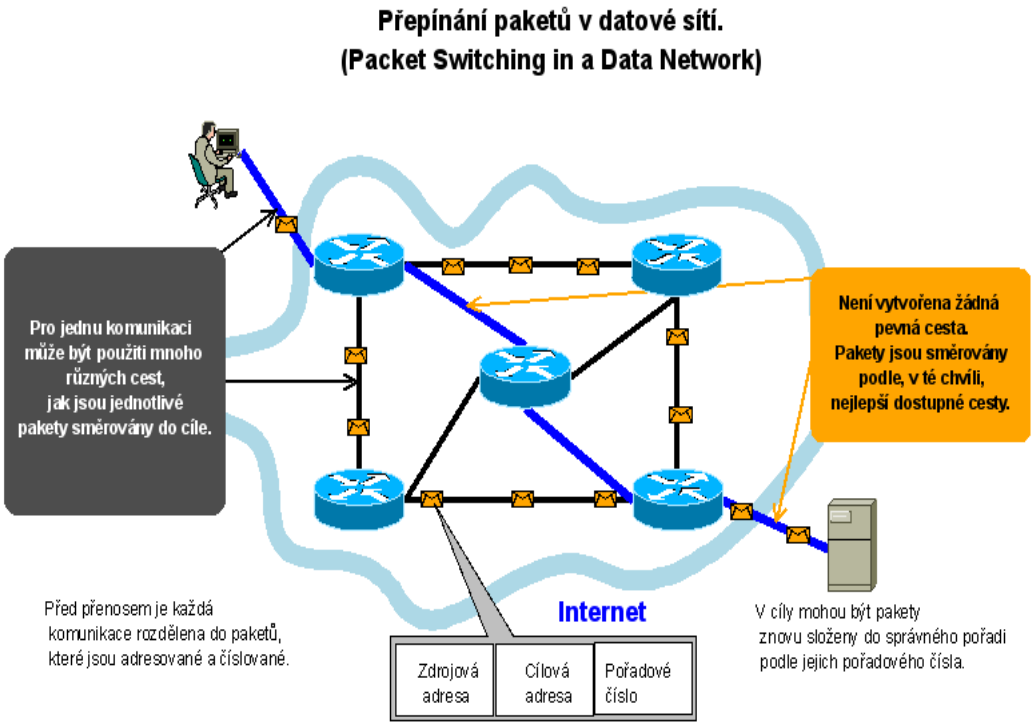
8 Zajišťují AAA protokoly např. RADIUS, TACACS.

- uložené kontrolní součty (*hash*, *CRC*, *fingerprints*),
- zajištění nepopiratelnosti odesílatele - digitální podpis (*digital signatures*),

- **dostupnost** (*availability, accessability*) - zajištěno pomocí:
  - omezení rychlostí a objemů datových přenosů,
  - pravidelné záplaty a aktualizace (*patch, update*) na známá zranitelná místa operačního systému viz www.sans.org a http://nvd.nist.gov/ ,
  - antiviry.



- přechod **sítě s přepínanými okruhy** (*switched circuits*) (= klasické analogové telefony) na **síť s přepínanými pakety** (*switched packets*) (= Internet) (nevýhodou zastaralých sítí s přepínanými okruhy je obvykle definitivní ztráta spojení při výpadku jedné linky, naproti tomu sítě používající přepínané pakety při ztrátě jedné cesty automaticky směrují pakety jinou dostupnou cestou a případně znovu odešlou chybějící nebo poškozená data),**použití paketů** (komunikace je rozdělena do menších datových balíčků, které se snáze přenášejí – při výpadku linky se ztratí pouze několik paketů nikoliv celá komunikace, celá zpráva),



- **nespojově orientované sítě** (Internet) versus spojově orientované sítě (klasická analogová telefonie) – efektivnější přenos dat (případné ztráty dat se eventuálně řeší až na koncových systémech, nikoli během přenosu na jednotlivých směrovačích na trase).

Hlavní **vývojové trendy** v datových sítích v blízké budoucnosti:
- zvětšení počtu mobilních uživatelů (*mobility*),
- rozšíření výkonných zařízení (s velkým tokem dat),
- expanze řady různých nových služeb.

Bezpečná síť musí:
- zamezit neoprávněnému rozšiřování nebo ukradení informací tzn. porušení důvěrnosti informací (*Confidentiality*) a neautorizovanému přístupu do sítě => autentizace (*authentication*) uživatelů, fyzická bezpečnost sítě, eliminace zachytávání datové komunikace => šifrování,
- zamezit neoprávněné modifikaci dat (*Data Integrity*) = digitální podpisy (*digital signatures*), hašovací algoritmy (*hashing algorithms*) a kontrolní součty (*check sums*),
- trvalá dostupnost služeb = zamezit odepření služeb vlivem útoku (*DoS attack*), firewall, antiviry, antispyware, eliminovat jediné kritické místo selhání (*single point of failure*).

Bezpečnost v síti rozlišujeme na:
- **bezpečnost síťové infrastruktury** (příklady narušení: školník odpojí a odnese přepínač, stavební dělníci překopnou kabel páteřní sítě, hacker se vzdáleně přihlásí a změní konfiguraci směrovače),

- **bezpečnost dat** (příklady narušení: naštvaný zaměstnanec pozmění objednávky odběratelů, konkurence ukradne citlivá firemní data, sekretářka odešle citlivá data jako odpověď na zfalšovaný e-mail, který se tváří jako odeslaný jejím šéfem).

Prvky sítě:
naučte se ikonky (používané firmou Cisco – viz obrázek symboly datových sítí) následujících prvků sítě: desktop, laptop, server, IP telefon, LAN (L2) switch, router, bezdrátový router, firewall, síťový mrak (= síťový prostor), přenosová média (LAN (přímý a překřížený UTP, WAN (sériová linka), bezdrát).

Cvičení

odkazy na Web:
CCNA: http://en.wikibooks.org/wiki/CCNA_Certification
CCNA Příručka: http://www.unixlead.com/CCNA-GUIDE.htm
Historie komunikace: Shanon: *"A Mathematical Theory of Communication."* http://cm.bell-labs.-com/cm/ms/what/shannonday/shannon1948.pdf

Bezpečnost informačních systémů

SANS Institute (SysAdmin, Audit, Networking, and Security, komerční organizace pro bezpečnost) – http://www.sans.org
National Vulnerability Database Home (Národní databáze zranitelných míst informačních systémů - v USA) – nvd.nist.gov
Computer Emergency Readiness Team (CERT, USA) databáze zranitelných míst informačních systémů http://www.kb.cert.org/vuls

Domácí cvičení

- Převody v číselných soustavách (binární, dekadická a hexadecimální), logický součin (AND) - „z hlavy“ = bez kalkulačky (v rozsahu jednoho bajtu).
- **Nainstalujte si** doma program Packet Tracer (download – pro registrované uživatele - z portálu NetAcad).

Kontrolní opakovací otázky a odpovědi (kvíz):[9]

1) Jaká je známá moderní forma převážně textové komunikace mezi dvěma či více lidmi v reálném čase?

   a) Instant Messaging

2) Který typ sítě poskytuje zákazníkům omezený přístup k firemním datům (jako jsou skladové zásoby, objednávky, ...)?

   a) Extranet (opakem je síť dostupná pouze oprávněným uživatelům pouze uvnitř firmy – intranet (= privátní síť, technologicky se jedná o stejnou síť na bázi protokolové sady TCP/IP))

9 V uváděných kvízech uvádím vesměs pouze správné odpovědi. Schopnost spolehlivě určit také odpovědi určitě nesprávné je ale samozřejmě stejně důležitá – zvláště při nejistotě správné odpovědi. Tyto kvízy představují vhodnou přípravu před vlastními testy. Pro zvládnutí testů však nepoužívejte drilování správných odpovědí, ale snažte se o pochopení konceptu skrytého za tou kterou konkrétní otázkou.

3) Co vyrovnává mezi důležitostí datového přenosu a jeho charakteristikou při řízení a správě datového provozu?
   a) QoS (kvalita služeb – řízení datového provozu)
4) Které dva postupy se používají, aby správně pracovaly strategie kvality služeb (QoS)?
   a) Síťový provoz je klasifikován na základě požadavků kvality služeb
   b) Ke každé klasifikaci aplikačních dat je přiřazena priorita provozu.
5) Dvě základní komponenty síťové architektury:
   a) naprogramované služby a protokoly, které přenášejí zprávy v síti,
   b) technologie podporující síťovou komunikaci.
6) Ze kterých tří důvodů byly při vývoji Internetu zavrženy přepínané okruhy a spojované (spojově orientované) technologie?
   a) Ranné technologie sítí s přepínanými okruhy nevytvářely při selhání přenosového okruhu žádný náhradní okruh.
   b) Technologie přepínaných okruhů (přepojovaných okruhů) vyžadují, aby byl mezi koncovými body vytvořen okruh aniž jsou právě přenášena data.
   c) Vytvoření vícenásobných, simultánních okruhů odolných proti selhání je u technologie přepínaných (přepojovaných) okruhů nákladné.
7) Ze kterých tří důvodů byla při vývoji Internetu použita technologie datové komunikace založená na přepínaní paketů a nespojově orientovaná?
   a) Dokáže se rychle přizpůsobit při ztrátě spojení
   b) efektivní využití síťové infrastruktury pro přenos dat
   c) datové pakety mohou sítí cestovat více cestami simultánně
8) Jaká je role QoS v konvergované síti?
   a) Pro různé typy datové komunikace v síti nastavuje priority pro doručení dat
9) Spárujte definice síťové architektury s jejich názvy:
   a) omezuje dopad HW a SW závad a poskytuje mechanismus pro zotavení po chybě = *fault tolerance* (odolnost vůči chybám)
   b) podporuje rozšíření síťové infrastruktury pro nové uživatele i aplikace = *scalability* (rozšiřitelnost)
   c) poskytuje určitou úroveň konzistentního a nepřerušitelného doručení dat na základě očekávání (požadavků) uživatelů = *quality of service (QoS)* (kvalita služeb)
   d) chrání důvěrné a kritické firemní informace před jejich zcizením a pozměněním = *security* (zabezpečení)
10) Ohrožení bezpečnosti, bezpečnostní hrozba (*security threat*) může být rozdělena do dvou kategorií: bezpečnosti síťové infrastruktury a bezpečnosti obsahu. Rozdělte vyjmenované bezpečnostní hrozby do těchto dvou kategorií:

a) Zabezpečení síťové infrastruktury:
   i. školník odpojí kritické síťové zařízení,
   ii. stavební dělníci během výkopu nechtěně překopnou síťový datový kabel,
   iii. hacker se připojí k síťovému zařízení a změní jeho konfiguraci.

b) Zabezpečení datového obsahu:
   i. naštvaný zaměstnanec změní data v databázi zákazníků,
   ii. sekretářka pošle e-mailem důvěrné informace jako odpověď na podvržený e-mail svého šéfa,
   iii. konkurent se dostane na citlivá data prostřednictvím nezabezpečené bezdrátové sítě.

Kapitola 2 – Komunikace prostřednictvím sítě

V této kapitole se naučíme:

- Popsat strukturu sítě včetně síťových zařízení a přenosového média, které jsou nezbytné pro úspěšnou komunikaci.
- Vysvětlit funkci protokolů v síťové komunikaci.
- Vysvětlit výhody použití vrstvového modelu k popisu činnosti sítě.
- Popsat roli každé vrstvy ve dvou uznávaných síťových modelech: protokolový model TCP/IP a model OSI.
- Popsat důležitost adresních a jmenných schémat v síťové komunikaci.

Síť – termín zahrnující **datovou síť (**neboli **informační síť)**. Skupina vzájemně propojených zařízení schopných přenášet množství různých typů komunikací zahrnujíce tradiční počítačová data, interaktivní hlas, video a zábavné produkty (a sdílet síťový HW i SW).

Síťová infrastruktura umožňuje komunikovat: rychle, spolehlivě, bezpečně a ekonomicky.

Elementy (síťové) komunikace (tok zprávy (v síti) obecně)[10]:

Zdrojová zpráva → kodér → signál → vysílač (*transmitter, sender*) = multiplex (*multiplexing*) → přenosové (síťové) médium = kanál (přenáší signál) → přijímač (*receiver*) = demultiplex (*demultiplexing*) → dekodér → cílová zpráva.

Přenos zprávy (více uživatelů sdílí část šířky pásma, přenosové kapacity (*bandwidth*) přenosového média):

- **segmentace** – rozdělení jedné zprávy do více kousků, které jsou přenášeny samostatně (každý kousek je jednoznačně označen (*labeling*), aby šel zařadit do správného pořadí ve správné zprávě),
- **multiplexing** – simultánní přenos více datových toků přes jedno přenosové médium, to znamená prokládání (*interleaving*) jednotlivých kousků (segmentů) různých zpráv (komunikací) z různých zdrojů, když jsou přenášeny přes jedno společné přenosové médium.

Komponenty sítě a jejich funkce v síti

(Aktivní) prvky sítě (devices)

- **koncová zařízení** (*end devices*) – přímo je používá koncový uživatel – v kontextu sítě se nazývají **hostitelé** (*host*) (= hostí IP adresu) nebo také **uzel** sítě, hostitel může pracovat jako **klient, server** nebo obojí. **Hostitel zahajuje komunikaci jako klient** a získává informaci ze serveru. Hostitelé jsou například:
  - počítače (*work stations, laptops, file servers, web servers*) ,
  - síťové tiskárny,
  - VoIP telefony,
  - bezpečnostní kamery,

10 Komunikační proces – přenosový model popisuje KDO, CO, KOMU, jakým MÉDIEM a s jakým ÚČINKEM sděluje.

    - mobilní handheld zařízení (jako jsou bezdrátové snímače čárového kódu, PDA, ...)
    - POS (*Point of Sale*) – pro platbu platební kartou, ATM (*Automatic Teller Machine*) - bankomat, ...
- **propojovací (mezilehlá) zařízení** (*intermediary*) – propojují různé části jedné sítě nebo různé sítě dohromady
    - nezahajují sama komunikaci,
    - regenerují a přeposílají datové signály,
    - spravují informace o cestách skrz jednu síť a propojené sítě,
    - informují ostatní zařízení o chybách a selhání komunikace,
    - směrují data přes alternativní cestu v případě závady linky,
    - klasifikují zprávy a řadí je do fronty v souvislosti s QoS,
    - povolují nebo zakazují tok dat v závislosti na nastaveném zabezpečení.
      Jsou to:
        - **přístupová zařízení (*Network Access Devices*)** – připojují koncového uživatele do sítě: rozbočovače (*hub*), přepínače (*switch*), bezdrátové přístupové body (*wireless access point*)
        - **propojovací mezilehlá zařízení pro propojení sítí (*Internetworking Devices*)** – propojují jednu síť do jiné sítě nebo sítí:
            - **směrovač (router)** – někdy se pro něj používá název mezilehlý systém (*intermediary system*),
            - **komunikační server** (*Communication Server*)
            - a **modem** (*modem*).
        - **bezpečnostní zařízení** *(Security Devices) (firewall)*

Přenosová média

Kritéria pro výběr vhodného média jsou přenosová vzdálenost, prostředí, do kterého má být instalováno, objem dat a požadovaná rychlost přenosu, cena média a cena instalace:

- kovové kabely
- skleněné nebo plastové optické kabely (*fiber optic cable*)
- bezdrátové přenosy

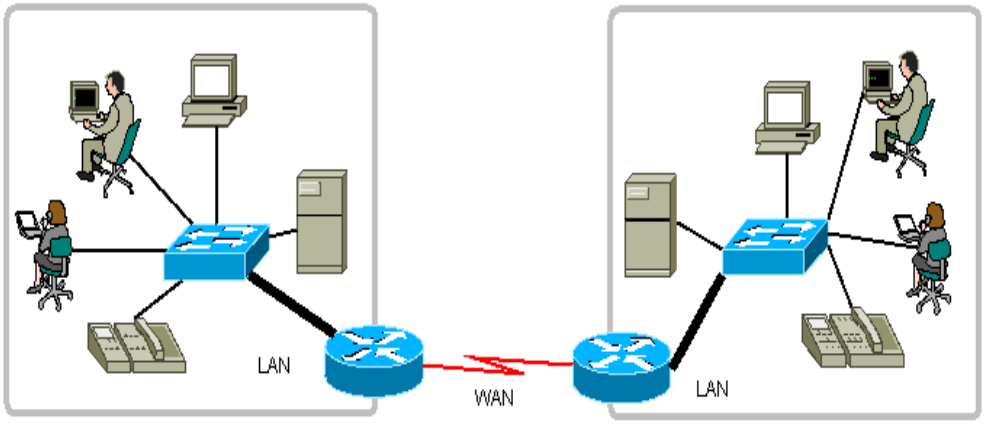
Médium	***Příklad***	***Kódování (signál)***
Měď	Kroucená nestíněná dvoulinka (= UTP), obvykle používaná v LAN, kroucená stíněná dvoulinka (= STP), ...	Elektrické pulsy
Optický kabel	Skleněné nebo plastové vlákno použité na dlouhé vzdálenosti - WAN nebo jako kmenové vedení, páteřní linka LAN	Světelné pulsy
Bezdrátové	Koncoví uživatelé připojeni přes vzduch (např. WLAN)	Elektromagnetické vlny

LAN, WAN a propojení sítí

LAN (*Local Area Network*) lokální síť nebo skupina propojených lokálních sítí, které jsou pod stejnou administrativní kontrolou. V minulosti se o sítích LAN uvažovalo pouze jako o malých sítích, které jsou v jedné fyzické lokalitě. Tehdy byly sítě LAN tak malé jako je jedna lokální síť instalovaná doma nebo v malé kanceláři, nyní sítě LAN zahrnují propojené sítě, složené z mnoha set hostitelských počítačů, instalované v několika budovách a lokalitách. Všechny lokální sítě v LAN jsou pod jednou administrativní kontrolou, která nastavuje zabezpečení a zásady omezování přístupových práv, které jsou tak v síti vynuceny.

Bezdrátová (*wireless*) LAN se nazývá **WLAN (*Wireless LAN*)**.

Geograficky vzdálené lokální sítě LAN jsou propojené sítí známou jako WAN (Wide Area Network).



WAN (*Wide Area Network*) rozsáhlá, rozlehlá síť: provozována telekomunikačním operátorem (TSP) nebo internetovým poskytovatelem ISP (*Internet Service Provider*) v geograficky rozsáhlém území, propojuje různé LAN dohromady. Ačkoliv jednotlivé sítě LAN mohou mít na obou koncích propojovací sítě WAN stejnou správu, zásady uvnitř sítě WAN jsou pod kontrolou TSP. Sítě WAN používají speciálně navržená síťová zařízení pro propojování se sítěmi LAN.

MAN (*Metropolitan Area Network*) – metropolitní síť (síť typu WAN ve velkých městech)

PAN (*Personal Area Network*) – osobní síť, například telefon připojený k PC pomocí technologie BlueTooth.

SAN *(Storage Area Network)* – datová síť, která slouží k připojení zálohovacích zařízení k serverům.

LAN a WAN mohou být propojeny do „intersítí“ (*internet, internetwork, internetworking*).

Internetwork – skupina vzájemně propojených sítí. Nejznámější a nejpoužívanější veřejně přístupná skupina propojených sítí je Internet. Samotná činnost propojování sítí se anglicky nazývá *internetworking*.

Internet – síť sítí (zkratka z *Internetwork* = propojená síť) – nejznámější veřejně přístupné propojení sítí – připojení do něj prostřednictvím poskytovatele internetového připojení - ISP (*Internet Service Provider*). K zajištění efektivní komunikace prostřednictvím různorodé infrastruktury sítě

vyžaduje aplikaci konzistentních a společně uznávaných technologií a protokolů a stejně tak i spolupráci mnoha agentur pro správu sítě.

Cvičení

Systémové utility (služební programy)

- Příkazy v příkazové řádce: ipconfig, ping, tracert, nslookup

Výpis konfigurace IP: (ipconfig nebo $/sbin/ifconfig)[11]

```
c:\>ipconfig /all

Konfigurace protokolu IP systému Windows
        Název hostitele . . . . . . . . . : 3303-31
        Primární přípona DNS. . . . . . . :
        Typ uzlu  . . . . . . . . . . . . : neznámý
        Povoleno směrování IP . . . . . . : Ne
        WINS Proxy povoleno . . . . . . . : Ne
        Prohledávací seznam přípon DNS. . : spse.pilsedu.cz

Adaptér sítě Ethernet Připojení k místní síti 2:
       Přípona DNS podle připojení . . . : spse.pilsedu.cz
       Popis . . . . . . . . . . . . . . : 3Com 3C920 Integrated Fast Ethernet Controller (3C905C-
TX Compatible) #2
       Fyzická Adresa. . . . . . . . . . : 00-B0-D0-D6-D8-90
       Protokol DHCP povolen . . . . . . : Ano
       Automatická konfigurace povolena  : Ano
       Adresa IP . . . . . . . . . . . . : 192.168.105.33
       Maska podsítě . . . . . . . . . . : 255.255.255.0
       Výchozí brána . . . . . . . . . . : 192.168.105.254
       Server DHCP . . . . . . . . . . . : 172.16.1.1
       Servery DNS . . . . . . . . . . . : 172.16.1.1
                                           172.16.1.222
       Zapůjčeno . . . . . . . . . . . . : 14. prosince 2010 14:33:42
       Zápůjčka vyprší . . . . . . . . . : 21. prosince 2010 14:33:42
```

Minimální potřebné nastavení klienta v síti TCP/IP:

- IP adresa (*IP address*) – logická adresa - jednoznačně určuje klienta v síti,
- maska podsítě (*subnet mask*) - určuje síťovou část IP adresy, to znamená adresu sítě, ve které IP adresa leží,
- výchozí (implicitní) brána (*default gateway*) – vstupní rozhraní směrovače, který propojuje tuto síť s jinou sítí,
- servery DNS – primární a sekundární jmenný server pro překlad doménového jména na IP adresu.

Test dostupnosti síťového zařízení s danou IP adresou:

```
c:\>ping 172.16.1.1

Příkaz PING na 172.16.1.1 s délkou 32 bajtů:

Odpověď od 172.16.1.1: bajty=32 čas < 1ms TTL=63
Odpověď od 172.16.1.1: bajty=32 čas < 1ms TTL=63
Odpověď od 172.16.1.1: bajty=32 čas < 1ms TTL=63
Odpověď od 172.16.1.1: bajty=32 čas < 1ms TTL=63

Statistika ping pro 172.16.1.1:
```

11 V Linux/Unix není přímý ekvivalent ipconfig. Ifconfig vypíše konfiguraci pro síťové rozhraní, route respektive netstat -nr vypíše směrovací tabulku (a též *default gateway*) a dhclient popřípadě nslookup zjistí adresu DNS serveru.

```
Pakety: Odeslané = 4, Přijaté = 4, Ztracené = 0 (ztráta 0%),
Přibližná doba do přijetí odezvy v milisekundách:
   Minimum = 0ms, Maximum = 0ms, Průměr = 0ms
```

- Utilita[12] ping (v americké angličtině je to termín pro vyslání a přijetí odrazu signálu sonaru v ponorce) používá dva typy zpráv protokolu ICMP – žádost o odpověď a odpověď na žádost (*echo request* a *echo response*)
- TTL = Time To Live – životnost (doba života) IP paketu **ve skocích** (*hop*) = počtech směrovačů, přes které může projít než je zahozen. (Na každém směrovači je TTL zmenšen o jedničku. Při TTL = 0 paket „zemře“ = je zahozen. O tom je podána zpráva „překročení doby života“ pomocí protokolu ICMP.)

Trasování cesty, kterou paket dosáhl cílové zařízení. Výpis všech směrovačů na cestě:

```
c:\>tracert www.seznam.cz

Věpis trasy k seznam.cz [77.75.76.3]
s nejvýše 30 směrováními:

 1     2 ms    31 ms     2 ms  192.168.105.254
 2    < 1 ms    < 1 ms    < 1 ms  ns.spse.pilsedu.cz [172.16.1.1]
 3    < 1 ms    < 1 ms    < 1 ms  igw-1.pilsedu.cz [195.113.181.222]
 4     1 ms     1 ms     1 ms  zcu-pilsedu-gw.pilsedu.cz [195.113.181.254]
 5     3 ms     2 ms     1 ms  ic-cat6509-gw.zcu.cz [147.228.200.21]
 6     1 ms     1 ms    < 1 ms  r99-pm.zcu.cz [147.228.200.2]
 7     2 ms     2 ms     2 ms  r105-r99.cesnet.cz [195.113.156.77]
 8     2 ms     3 ms     2 ms  r84-r105.cesnet.cz [195.113.156.165]
 9     4 ms     3 ms     3 ms  nix-pv.pater.iol.cz [194.50.100.160]
10     3 ms     3 ms     *     194.228.21.101
11     3 ms     5 ms     3 ms  194.228.36.1
12     3 ms     4 ms     3 ms  www.seznam.cz [77.75.76.3]

Trasování bylo dokončeno.
```

- Pracuje na bázi zpráv protokolu ICMP, postupně zapouzdřovaných do IP paketů s postupně se zvětšující životností TTL = 1, 2, 3, … .
- Vyzkoušejte: *ping -i 1 www.seznam.cz* (Windows) nebo *ping -t 1 www.seznam.cz* (Linux)

Vyhledávání převodů doménového jména na IP adresu a naopak = nslookup. Dotazovací nástroj na jmenný server (DNS) (ns = name server = jmenný server, lookup = rychlé vyhledání):

```
C:\Documents and Settings\zak>nslookup
Výchozí server:   ns.spse.pilsedu.cz
Address:  172.16.1.1

> www.seznam.cz
Server:  ns.spse.pilsedu.cz
Address:  172.16.1.1

Neautorizovaná odpověď:
Název:   www.seznam.cz
Address:  77.75.76.3

> exit

C:\Documents and Settings\zak>
```

- Výchozí server = primární jmenný server (DNS) (= *domain name server*)
- nslookup lze spustit i přímo s parametrem (doménou nebo IP adresou) bez uživatelské výzvy (= *prompt*)

12 Utilita (*utility*) = služební program.

V Linuxu nevidíte v nastavení ifconfig primární jmenný server domény klienta (výchozí server):

```
$ nslookup
> www.seznam.cz
Server:     172.16.1.1
Address:    172.16.1.1#53

Non-authoritave answer:
Name:       www.seznam.cz
Address:    77.75.72.3
> exit
$
```

Další užitečný SW

- Packet Tracer – simulátor sítí – instalace a síť peer-to-peer, topologie sítí
- WireShark – analyzátor síťových protokolů – instalace, spuštění jako privilegovaný uživatel a zachytávání provozu („čmuchání“ v síti = "*sniffing*"): FTP, ping
- Neo Trace – rozšiřuje příkaz tracert (respektive traceroute)

Protokoly, sady protokolů

Protokol nebo **sada protokolů** (to jsou protokoly, které vzájemně spolupracují) poskytuje respektive popisuje procesy jako jsou:

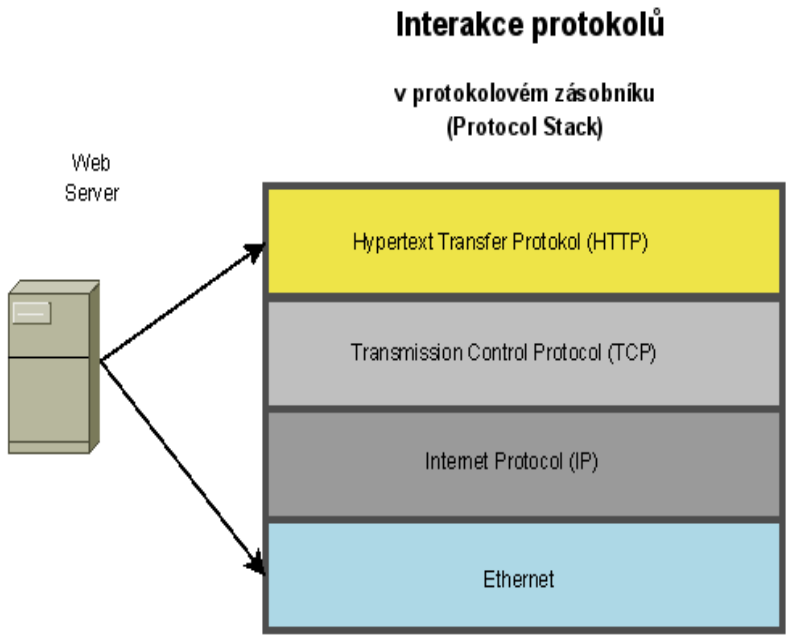
- formát a struktura zprávy,
- jak síťová zařízení sdílejí informace o cestách s jinými sítěmi,
- jak a kam se posílají chybové a systémové zprávy mezi zařízeními,
- navázání a ukončení datového spojení (sezení) (*session*).

Sady protokolů a průmyslové standardy

Sady protokolů a průmyslové standardy jsou zajišťovány následujícími institucemi:

- *Institute of Electrical and Electronics Engineers (IEEE),*
- *Internet Engineering Task Force (IETF)*

Vzájemná interakce protokolů v jedné sadě = protokolovém zásobníku (*protocol stack*) (například: **HTTP->TCP->IP->Ethernet** v sadě TCP/IP)



Protokoly jsou nezávislé na použité technologii.

Výhody použití vrstvových modelů

- Definice základních standardů pro komunikaci v datové síti.
- Rozdělení na jednotlivé vrstvy (*layer*) rozdělí komunikaci na snáze pochopitelné a popsatelné celky.
- Pomáhá při vytváření komplexních, více uživatelských, více dodavatelských (= neproprietárních) sítí.
- Pomáhá při vytváření protokolů, protože každý protokol pracuje na určité vrstvě.
- Definuje se rozhraní na sousední (spodní a horní) vrstvy. Vyšší vrstva **používá služby** pod ní ležící nižší vrstvy (která **poskytuje služby**).
- Podporuje vzájemnou spolupráci výrobků různých (konkurenčních) výrobců.
- Předchází vynuceným změnám vyvolaných změnou v sousední vrstvě.
- **Zapouzdření** (*encapsulation*) dat – na příslušné vrstvě se pracuje pouze se záhlavím příslušné vrstvy a nezkoumá se obsah zapouzdřené **datové jednotky protokolu** (*Protocol Data Unit = PDU*) to znamená nezkoumá se obsah zapouzdřených dat z vyšší vrstvy.
- Společná řeč pro popis sítě mezi síťovými profesionály.
- Snáze se naučí a pochopí komunikace v síti.

Vrstvové modely TCP/IP a ISO OSI[13]

Vrstvy referenčního modelu ISO OSI

Vrstva (Layer, Lx) a její popis	***PDU***	***Adresace (v záhlaví)***	***Aktivní prvek***		***Název***
Vrstva 7 (L7) uživatelské rozhraní. Vstup dat koncového uživatele. Koncová komunikace ***(end-to-end)*** **mezi uživateli.**	Data		SW: Gateway - brána		Application Aplikační
Vrstva 6 (L6) reprezentace dat ze služeb aplikační vrstvy, překlad (kódování) dat mezi dvěma systémy, komprese, dekomprese, šifrování.	Data		SW		Presentation Prezentační
Vrstva 5 (L5) udržuje spojení – relaci *(session)* mezi aplikacemi dokud je potřebné, provede ukončení spojení, zabezpečovací, přihlašovací a správní funkce.	Data		SW		Session Relační (relace = sezení, spojení)
Vrstva 4 (L4) Služby pro přenos segmentu a opětovné složení zprávy. Zajišťuje spolehlivé (= bezchybné) doručení dat pro jednotlivé komunikace koncových zdrojových a cílových aplikací. Koncová komunikace ***(end-to-end)*** **mezi aplikacemi, procesy (koncovými systémy).**[14]	Segment	Port Číslo portu	SW		Transport Transportní
Vrstva 3 (L3) Doručení dat mezi síťovými koncovými zařízeními. Vyhledání nejlepší cesty ze zdrojové do cílové sítě = směrování. (Převádí logickou IP adresu počítače na fyzickou adresu síťové karty MAC (pomocí protokolu ARP).)	Packet (Paket) Datagram[15]	IP adresa logická adresa	SW Router (Směrovač)[16]		Network Síťová
Vrstva 2 (L2) Řídí přístup ke sdílenému přenosovému médiu - výměna dat v rámci sousedních zdrojových a cílových počítačů (v jedné síti LAN). Má dvě podvrstvy: ● horní Logical Link Control (LLC) ● spodní Media Access Control (MAC).	Frame (Rámec) (**v zápatí** obsahuje kontrolní součet)	MAC adresa fyzická adresa	SW + HW: Bridge (Můstek) Switch (Přepínač) NIC[17]		Data Link Spojová (Linková)
Vrstva 1 (L1) Popisuje elektrické nebo optické **signály** a postupy používané pro komunikaci mezi koncovými zařízeními (**popisuje fyzickou linku**: médium, konektory, přenosové rychlosti, ...).	- pouze bity	-	HW: Hub (Rozbočovač) Repeater (Opakovač)		Physical Fyzická

13 ISO = International Standard Organization, International Organization for Standardization = mezinárodní organizace pro normy, OSI = Open Systems Interconnection, propojení otevřených systémů.

14 Transportní vrstva OSI modelu předpokládá vždy spolehlivý spojovaný přenos. (Na rozdíl od protokolového modelu TCP/IP, kde je na transportní vrstvě ke spolehlivému, spojovanému protokolu TCP (TCP PDU: segment) přidán i nespolehlivý, nespojovaný protokol UDP (UDP PDU: datagram).)

15 Datagram = nepotvrzovaná PDU, PDU pro nespojovanou službu

16 L7 až L3 je realizováno operačním systémem klienta.

17 NIC = Network Interface Card = síťová karta, síťový adaptér.

Pro zapamatování posloupnosti (anglických) názvů vrstev slouží různé mnemotechnické (*mnemonic*) pomůcky: *„All People Seem To Need Data Processing.“ (Zdá se, že všichni lidé potřebují zpracování dat.)* a také už méně používané *„Away Pizza Sausage Throw Not Do Please.“*

Párování modelu OSI na TCP/IP

Číslo vrstvy OSI	***Název vrstvy OSI***	***Číslo vrstvy TCP/IP***	***Název vrstvy TCP/IP***	***Protokoly modelu TCP/IP (příklady)***
7	Aplikační (*Application*)	4	Aplikační (*Application*)	, SMTP, POP3, FTP, Telnet
6	Prezentační (*Presentation*)			
5	Relační (*Session*)			
4	Transportní (*Transport*)	3	Transportní (*Transport*)	TCP, UDP
3	Síťová (*Network*)	2	Internetová / síťová / mezisíťová	IP (IPv4, IPv6), ICMP
2	Spojová / linková (*Data Link*)	1	Síťový přístup (*Network Access*)	Ethernet, Frame Relay, PPP, FDDI RS-232, 100BaseT na fyzické vrstvě
1	Fyzická (*Physical*)			

TCP/IP protokolový model (protokolová architektura[18])

Protokolová sada (protokolový model, protokolová architektura) TCP/IP je sada vzájemně spolupracujících protokolů. Spolupráce vrstev probíhá takto:

- Program (= aplikace) potřebuje navázat spojení se svým protějškem na jiném počítači (s protilehlým koncovým systémem). Pro přístup ke službám sítě aplikace použije **protokol na aplikační vrstvě**.
- Z aplikační vrstvy putuje požadavek na spojení do transportní vrstvy. **Transportní vrstva** zorganizuje dopravu dat mezi procesy pod operačním systémem v operační paměti na koncových zařízeních. Pokud je použit protokol TCP, jsou data rozdělena do segmentů, TCP naváže spojení (relaci) s protilehlým systémem ještě před vlastním přenosem aplikačních dat a také zkontroluje, zda byla data skutečně doručena. (V případě protokolu UDP jsou použity nespojované a nepotvrzované datagramy a relace se předem nevytváří.)
- Přenos dat na jiné síťové zařízení zajišťuje nižší **internetová ((mezi)síťová) vrstva**. Segmenty, které obdržela od vyšší transportní vrstvy zabalí = zapouzdří (*encapsulate*) do IP **paketů**.
- Pro vlastní přenos signálu po přenosovém médiu systém použije služeb **vrstvy síťového přístupu**, která paket zapouzdří do rámce a **rámec** – jeho jednotlivé bity - zakóduje do **signálu**, který je potom přenesen přes **přenosové médium**.

18 **Síťový model** je představa o tom jak mají být sítě řešeny. Obsahuje představu o počtu vrstev a o tom co má mít která vrstva na starosti. Neobsahuje konkrétní představu o tom, jak má která vrstva své úkoly plnit (konkrétní protokoly). **Síťová architektura** obsahuje navíc konkrétní představu o způsobu fungování jednotlivých vrstev tedy konkrétní protokoly.

Název a funkce vrstvy sady TCP/IP	*Nejpoužívanější protokoly ve vrstvě*
***Application* (aplikační)** uživatelské rozhraní, reprezentace uživatelských dat – kódování dat (*encoding*) a řízení dialogu	• **Přenos souborů** FTP*= File Transfer Protocol (spojově orientovaný[19], používá TCP), TFTP* = Trivial File Transfer Protocol (nespojovaný, používá UDP) • **Distribuované sdílení souborů** NFS = Network File System (Sun, přístup na HDD v síti) • **E-mail** SMTP = Simple Mail Transfer Protocol (pouze čistý text – přenos e-mailu z poštovního serveru na jiný poštovní server), POP = Post Office Protocol, IMAP = Internet Message Access Protocol (správa e-mailů, z klienta na server) • **WWW (World Wide Web)** HTTP = Hypertext Transfer Protocol • **Vzdálené přihlášení (virtuální terminál)** Telnet*, rlogin (remote login), ssh (secure shell) • **Správa sítě** SNMP* = Simple Network Management Protocol (správa komunikace, zabezpečení, …) • **Správa jmen** DNS* = Domain Name System (překlad doménových jmen na IP adresy) *) použito směrovačem (router)
***Transport* (transportní)** řízení toku dat mezi koncovými aplikacemi = procesy (*application end-to-end conecction*) na různých zařízeních v různých sítích	• TCP = Transmission Control Protocol (spojově orientovaný protokol, potvrzování doručení a zotavení po chybě – znovu odeslání chybějících dat), • UDP = User Datagram Protocol (nespojový protokol, nekontroluje doručení)
Internet určení a výběr nejlepší cesty do cílové sítě (mezi sítěmi) = *routing* = směrování	• IP = Internet Protocol (nespojové směrování paketů), • ICMP = Internet Control Message Protocol (řízení a zprávy), • ARP = Address Resolution Protocol (určí pro známou IP adresu její MAC adresu), • RARP = Reverse Address Resolution Protocol (určí pro známou MAC adresu její IP adresu) • OSPF = Open Shortest Path First (směrovací protokol – algoritmus stavu linky)
Network Access **(síťového přístupu)** řízení HW síťových zařízení a přístupu k přenosovému médiu, kódování signálu	• Ethernet, Fast Ethernet, Giga Ethernet • SLIP = Serial Line Internet Protocol a PPP = Point-to-Point Protocol, • FDDI = Fiber Distributed Data Interface, • ATM = Asynchronous Transfer Mode, Frame Relay a SMDS = Switched Multimegabit Data Service, • ARP, • Proxy ARP, • RARP Poznámka: ARP a RARP pracují na obou vrstvách (Network Access i Internet)

19 Spojovaný/nespojovaný souvisí s potvrzováním/nepotvrzováním přijatých dat. => „Spolehlivý“/“nespolehlivý“ protokol. Spojová orientovanost je obvykle řešená na transportní vrstvě.

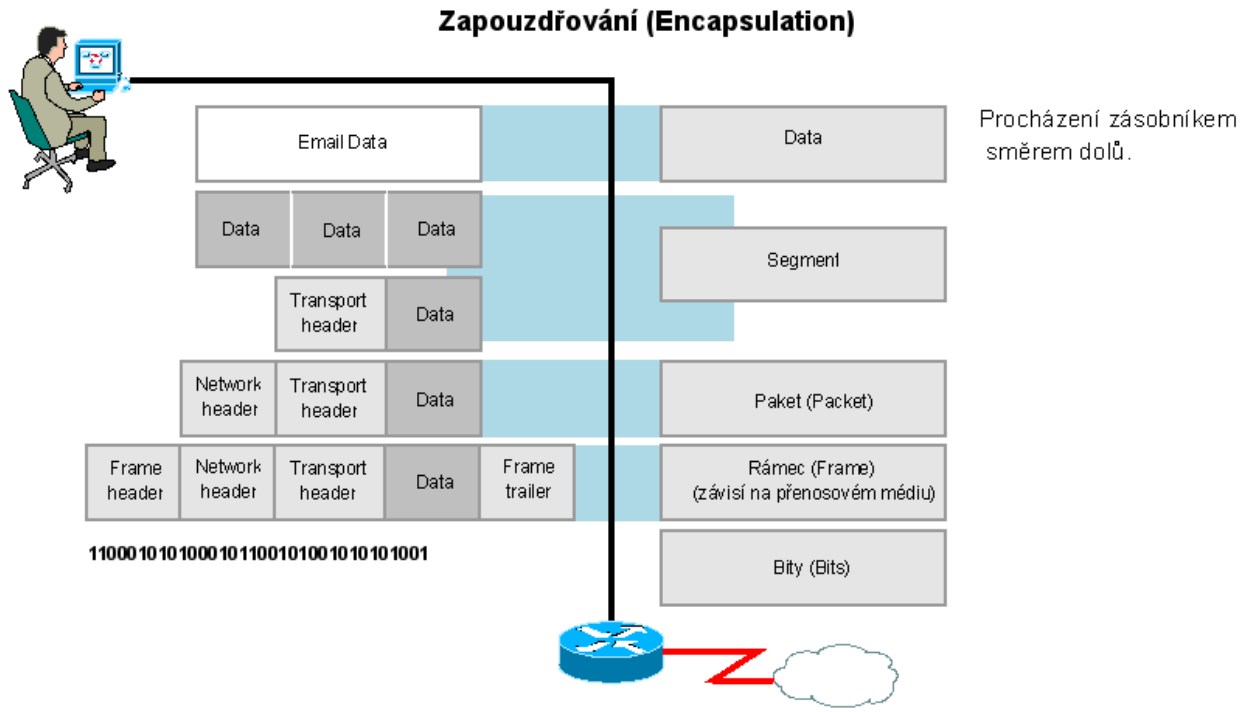
Průchod dat v síti

Průchod dat v síti z jednoho koncového systému (instance aplikačního programu na počítači) do druhého probíhá následovně: Aplikační data (například nepřetržitý datový tok, *datastream*) jsou segmentována a postupně na jednotlivých nižších vrstvách **zapouzdřována (*encapsulation*)** tzn. Na jednotlivých vrstvách jsou k datům z předchozí vyšší vrstvy přidávána záhlaví (hlavičky) jednotlivých konkrétní vrstvě příslušných PDU (*Protocol Data Unit*, datových jednotek protokolu).[20]

Posloupnost datových jednotek (*PDU*) během síťové komunikace:

aplikační data -> segment -> paket -> rámec -> bit (bit už ale není samostatná PDU)

Data (jednotlivé bity) jsou potom přenášena v binární podobě přenosovým médiem (kanálem) a v druhém systému jsou postupně **odpouzdřována (*decapsulation*)** (tj. jsou odstraňovány hlavičky): bit -> rámec -> paket -> segment -> data až do aplikační vrstvy.



Proces zapouzdřování (a odpouzdřování) na dvou vzájemně komunikujících systémech je uveden v následující tabulce:

20 Můžeme si pro představu pomoci s metaforou: analogie zapouzdřování s klasickou poštou znamená vkládání zpráv do obálek, kdy každá obálka má adresu příjemce a odesílatele. Obálka je potom zase vložena do jiné obálky pro doručení v jiné oblasti. Aplikační vrstva předává prostřednictvím operačního systému do nižších vrstev zdrojový a cílový socket. (Viz dále.)

Zdrojový systém (zapouzdřování)	PDU (Protocol Data Unit) = datová jednotka protokolu = zapouzdření na příslušné vrstvě (layer)							**Cílový systém (odpouzdřování)**
▼								▲
7. Aplikační			Data					**7. Aplikační**
▼								▲
6. Prezentační								**6. Prezentační**
▼								▲
5. Relační								**5. Relační**
▼								▲
4. Transportní, segmentace	Segment			Zdrojové + cílové číslo portu	Data (segmentovaná aplikační data)			**4. Transportní, opětovné složení**
▼								▲
3. Síťová	Paket		**Zdrojová + cílová IP adresa**	Data (obsah L4 segmentu)				**3. Síťová**
▼								▲
2. Spojová, multiplexing	Rámec		**Zdrojová + cílová MAC adresa**	Data (obsah L3 paketu)		CRC [21]		**2. Spojová, demultiplexing**
▼								▲
1. Fyzická			**Tok bitů ...01011100.....**					**1. Fyzická**
▼ ►	►	►	►	►	►	►	▲	

Význam adres na jednotlivých vrstvách

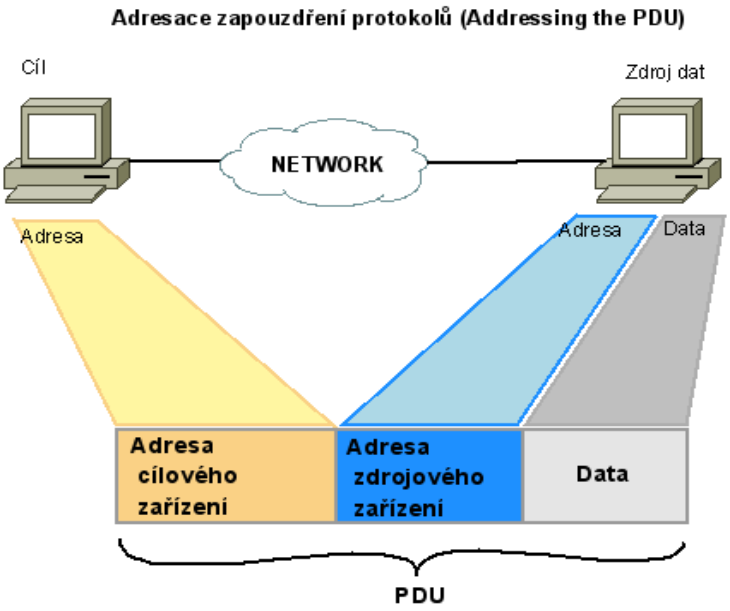
Během procesu zapouzdřování jsou vždy přidávány hlavičky specifické pro konkrétní vrstvu, které vždy obsahují minimálně zdrojovou a cílovou adresu specifickou pro danou vrstvu.

- Zdrojové a cílové **číslo portu** – určuje zdrojový a cílový proces (= instanci aplikace v operační paměti) na konkrétním koncovém zařízení v síti. Slouží k rozlišení konkrétní jedné komunikace mezi klientem a serverem příslušné síťové služby. (Transportní vrstva).
- Zdrojová a cílová **(logická) IP adresa** – určuje zdrojové a cílové koncové zařízení ve zdrojové a cílové IP síti. Slouží k vyhledání nejlepší cesty ze zdrojové do cílové sítě (= směrování). Ta cesta může vézt přes velký počet jiných vzájemně propojených sítí (Síťová, Internetová vrstva.)[22]
- Zdrojová a cílová **(fyzická) MAC adresa** – určuje zdrojové a cílové síťové zařízení v jedné lokální síti (LAN). (Spojová (linková) vrstva, vrstva síťového přístupu.)

V odpovědi na zprávu se potom vždy původní zdrojová a cílová adresa vzájemně zamění.

21 CRC – Cyclic Redundancy Check = kontrolní součet, pro detekci změn nebo chyb vzniklých při přenosu.

22 Zdrojový port a zdrojová IP adresa tvoří dohromady zdrojový socket, stejně tak cílový port a cílová IP adresa tvoří cílový socket.



Záhlaví PDU obsahuje políčka s cílovou a zdrojovou adresou koncových zařízení.

Cvičení

Animovaný film o komunikaci v síti ***Warriors of the Net*** (Válečníci sítě) (download: http://www.-warriorsofthe.net)

POZOR: film obsahuje také některé nepřesnosti. Např.: znovu odvysílání ztracených paketů obstarává transportní vrstva (protože IP je kvůli rychlému a efektivnímu přenosu nespojovaný protokol), vůbec nejsou zmíněny IP a MAC adresy.

Simulátor sítě: PacketTracer – režim simulace, ukázka zapouzdření dat v PDU na vrstvách modelu OSI. (**Lab 2.6.1:** dva počítače propojené překříženým kabelem do sítě peer-to-peer (IP: 192.168.1.2/24 – 192.168.1.3/24) proveďte všechny úkoly v aktivitě (*PT Activity*) ve všech čtyřech stránkách, potom ověřte výsledky (*Check Results*, *Assessment Items*) a vyzkoušejte v simulačním režimu (*Simulation*) včetně prohlédnutí obsahu PDU (*PDU Information at Device*).)

Analyzátor síťových protokolů: Wireshark (úkol je zachytit (*capture*) a analyzovat komunikaci utility ping (ECHO request na jmenný server domény (DNS server) školní sítě a odpověď ECHO response, včetně obsahu jednotlivých PDU: ICMP, IP, Ethernet II)

Najděte na Internetu obrázek analogie OSI modelu a běžné pošty (Vyhledejte: osi AND mail).

Termíny, které bychom měli znát

- *Network Interface Card (NIC)*, *LAN adapter* – síťová karta, síťový adaptér poskytuje fyzické připojení do sítě na PC nebo jiném hostitelském zařízení. Do síťové karty je přímo připojeno přenosové médium.
- *Physical (HW) Port* – fyzický port, konektor na síťovém zařízení, kde je připojeno médium.
- SW Port – číslo portu – číslo koncového procesu (aplikace) – dobře známé porty, dobře zná-

mé aplikace (aplikační protokoly) – 0 až 1023.

- *Interface (HW)* – rozhraní, specializovaný (HW) port na propojovacím zařízení, které připojuje do jednotlivé sítě. Protože router je použit k propojení sítí, port na routeru je zmiňován jako síťové rozhraní.
- *Interface (SW)* – logický interakční bod mezi softwarovými aplikacemi
- Přímý UTP (= *Unshielded twisted pair* = nestíněná kroucená dvoulinka, kabel se 4 páry měděných drátů) kabel (*straight-through cable*) (= *patch cable* = montážní kabel) (Propojuje logicky různá síťová zařízení např switch (DCE) a PC (DTE).)
    - DCE = *Data Communications Equipment* (EIA[23]) nebo *Data Circuit-Terminating Equipment* (ITU-T[24]) (*modem (CSU/DSU), NIC*) – průchozí komunikační zařízení umožňující připojení do sítě – pokud jde o přenos mezi DCE a DTE poskytuje hodinový signál pro synchronizaci dat,
    - DTE = *Data Terminal Equipment* – rozhraní mezi směrovačem a DCE - zakončovací zařízení.
- Překřížený UTP kabel (*cross-over cable*) (Propojuje logicky stejná zařízení např.: PC (= DTE) a router (= DTE), switch (= DCE) a hub (=DCE), ...)
- Sériový kabel – typický pro pronajaté linky WAN
- Ethernet – dominantní technologie LAN
- *MAC Address*: Ethernet L2, fyzická adresa
- *IP Address*: L3 logická adresa
- Maska podsítě, *Subnet Mask*: Požadována pro interpretaci IP adresy (určení adresy sítě, ve které IP adresa leží, pomocí logického součinu AND)
- Implicitní (výchozí) brána, *Default Gateway*: IP adresa síťového rozhraní routeru, na kterou se odesílá provoz opouštějící lokální síť
- PC, počítač, pracovní stanice, hostitelský počítač – koncová zařízení
- L7, L6, ..., L1 = Layer 7, 6, ... = Vrstva 7, 6 atd. Modelu ISO OSI
- PDU (= *Protocol Data Unit)* – datová jednotka protokolu = zapouzdření (*encapsulation*) na příslušné vrstvě OSI modelu.
- *Switch*, přepínač: propojovací zařízení rozhodující se na základě MAC adres rámců na L2 (typicky MAC adresy Ethernetové síťové karty) pracuje na L2 i L1.
- *Router*, směrovač: zařízení pracující na L3, L2, L1 rozhodující se na základě L3 adres paketů (typicky IPv4 adresy)
- *Bit: Binary digit*, binární číslice, logická 1 nebo 0, má různou fyzickou reprezentaci jako elektrické, optické nebo elektromagnetické pulzy, L1 PDU.
- *Frame*, rámec: L2 PDU
- *Packet*, paket, datagram: L3 PDU

Kontrolní opakovací otázky a odpovědi (kvíz):

1) Ke které vrstvě OSI modelu se vztahuje IP adresa?

    a) 3. - síťová - vrstva

2) Jaký typ adresy je na druhé (spojové (linkové)) vrstvě OSI modelu? (2 odpovědi)

    a) Fyzická

    b) MAC

3) Když server odpovídá na webovou žádost (*web request*), co se děje v procesu zapouzdření

23 EIA = Electronic Industries Alliance (www.eia.org)
24 ITU-T = standardizační sektor spadající pod International Telecommunication Union (www.itu.int/ITU-T/)

potom, co je webová žádost zapouzdřena do segmentu TCP?

a) Ke každému segmentu TCP je přidáno záhlaví protokolu IP, které obsahuje zdrojovou a cílovou IP adresu potřebnou pro doručení paketu do cíle.

4) Který termín (*term*) popisuje specifickou sadu pravidel, které určují formátování zpráv a proces jejich zapouzdření potřebný pro jejich přeposílání?

a) Protokol

5) Které dva protokoly se vztahují k 4. vrstvě OSI modelu? (Ve skutečnosti jsou konkrétní protokoly obsaženy pouze v protokolovém modelu (protokolové architektuře) TCP/IP.)

a) TCP,

b) UDP.

6) Přiřaďte k jednotlivým termínům jejich definice:

a) segmentace (*segmentation*) = rozdělení datového toku na menší kousky vhodné pro přenos,

b) zapouzdřování (*encapsulation*) = proces přidávání záhlaví specifického pro konkrétní vrstvu, potřebné pro přenos dat,

c) multiplexing = prokládání simultánních datových proudů (*data stream*) na sdíleném komunikačním kanálu nebo síťovém médiu,

d) protokol (*protocol*) = formální pravidla nastiňující struktury a postupy síťové komunikace,

e) PDU (*Protocol Data Unit*), datová jednotka protokolu = termín pro balíček dat, často implikující konkrétní protokol nebo vrstvu OSI modelu.

7) Přiřaďte jednotlivé termíny k odpovídajícím vrstvám OSI modelu:

a) transportní = segment, číslo portu, číslo sekvence

b) síťová = paket, IP adresa, logická adresa

c) spojová = rámec, MAC adresa, fyzická adresace v rámci lokální sítě

8) Spárujte název vrstvy OSI modelu s popisem její funkce:

a) aplikační = definuje rozhraní na aplikační software,

b) prezentační = standardizuje formát dat mezi systémy,

c) relační = spravuje a řídí uživatelské relace a dialogy,

d) transportní = koncové doručení (*end-to-end message delivery*) zprávy v síti (= doručení zprávy mezi procesy na koncových zařízeních),

e) síťová = směruje pakety mezi sítěmi na základě jedinečné síťové adresy (= doručení mezi koncovými zařízeními),

f) spojová = definuje postupy pro přístup k přenosovému médiu (a doručení mezi uzly v rámci jedné lokální sítě),

g) fyzická = kabeláž, bity, signály, přenosové rychlosti.

Kapitola 3 – Aplikační vrstva

V této kapitole se naučíme:

- Popsat, jak funkce tří horních vrstev OSI modelu poskytují služby aplikacím koncových uživatelů.
- Popsat, jak protokoly aplikační vrstvy modelu TCP/IP poskytují služby specifikované horními vrstvami OSI modelu.
- Definovat, jak lidé používají aplikační vrstvu ke komunikaci prostřednictvím sítě.
- Popsat funkce dobře známých aplikací a služeb TCP/IP, jako jsou World Wide Web a e-mail a jejich souvisejících protokolů (HTTP, DNS, SMB, DHCP, SMTP/POP, a Telnet).
- Popsat sdílení souborů, které používají aplikace peeer-to-peer a protokol Gnutella.
- Vysvětlit, jak protokoly zajistí, aby služby běžící na jednom druhu zařízení mohli vysílat a přijímat data z a do různých druhů síťových zařízení.
- Použití síťových analytických nástrojů (analyzátoru síťových protokolů) k otestování a vysvětlení jak pracují běžné uživatelské aplikace.

SW procesy

- **Aplikace** (*application*) – uživatelský aplikační program, SW, rozhraní pro koncového (= lidského) uživatele, koncová komunikace (*end-to-end*[25] *communication*) mezi aplikacemi,
- **služby** (*service*) – SW, program poskytující své služby aplikacím,
- **systémové operace**,
- jeden program může být v operačním systému spuštěn víckrát – každé spuštění vytváří (alespoň jeden) vlastní **proces =** instance programu v operační paměti (každý proces má své číslo procesu PID (*process ID*)),
- **démon** – část služby na serveru, která naslouchá a čeká na požadavky klientů (např. *httpd* – démon webové služby), pracuje s mnohonásobnými přístupy.

Cvičení

Správce úloh *(Task Manager)* ve Windows (CTRL+ALT+DEL spustí zde ve škole, klienta Novell, Tlačítko Správce úloh, vyberte záložku Procesy, menu Zobrazit - sloupce: PID.
Další způsob: stáhněte si z http://technet.microsoft.com balík utilit PsTools nebo ProcessExplorer):
Příkaz ***tasklist /SVC*** ve Windows XP Professional.
Příkaz ***ps*** *-**A*** v Linuxu.
Příkaz ***netstat*** *-**ao*** ve Windows (XP, Vista).

Vazba mezi aplikacemi, službami a protokoly

- **Aplikace** – aplikační program (*application SW, ASW*), který slouží rozhraní pro koncového uživatele.
- **Služby** – základní programy, které propojují aplikační vrstvu s nižšími vrstvami síťového modelu, poskytují síťové služby ASW.
- **Protokol** – popis komunikace na úrovni dané služby (nebo vrstvy).

25 Terminologicky koncová (end-to-end) komunikace znamená, že nás nezajímá, co se děje mezi tím (na nižších vrstvách).

Protokol

Protokoly poskytují strukturu schválených pravidel a postupů, které zajišťují, že běh služeb na jednom zařízení může posílat a přijímat data ze širokého spektra jiných síťových zařízení. **Protokol:**

- definuje procesy (postup zpracování) na obou koncích komunikace,
- definuje typy zpráv,
- definuje syntaxi zprávy,
- definuje význam každého použitého informačního pole ve zprávě,
- definuje, jak je zpráva odeslána a jaká je na ní odpověď,
- definuje interakci se sousední spodní vrstvou (rozhraní na služby nižší vrstvy).

http://www.protocols.com/

Komunikační model klient-server

Komunikaci vždy začíná (iniciuje) klient. Server je skladiště dat (informací). Procesy na něm řídí doručení dat pro klienta. Aplikační protokoly pracují v komunikačním modelu klient-server.

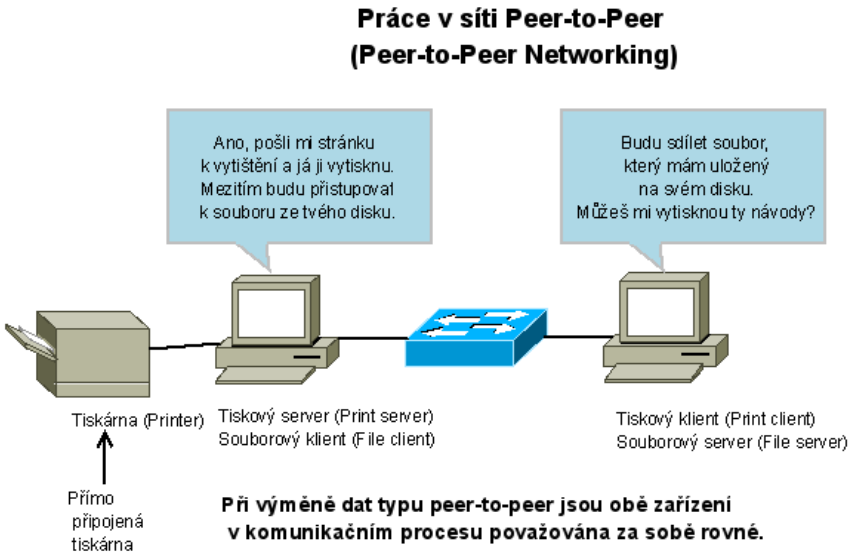
- *upload* (umístění) – z klienta na server,
- *download* (stažení) – ze serveru na klienta.

Komunikaci zahajuje klient a nikoliv server. Server „slouží“ tzn. čeká na požadavek klienta.
Síť typu klient-server hierarchicky organizovaná síť, používající pro poskytování síťových služeb vyhrazené (*dedicated*) servery („farma serverů“).
Aplikace typu klient-server lze provozovat v síti peer-to-peer (například dva počítače propojené překříženým UTP kabelem a na jednom z nich běží FTP server).

Výhody (klient-server)	*Nevýhody (klient-server)*
• centrální správa = jednotné zásady (tzv. politiky) (například centrální zásady zabezpečení), • jednotná infrastruktura, • komfortní poskytování síťových služeb	• nákladnější centrální HW i SW, • je třeba platit administrátora sítě.

Komunikační model peer to peer (p2p)

Peer-to-peer = rovný s rovným, „já pán, ty pán“. Oba klienti vysílají (iniciují vznik) zprávy (zahajují komunikaci) a přijímají zprávy, oba klienti simultánně (současně) vysílají i přijímají. Pracují současně jako klient i server. Obecně síťové zdroje jsou decentralizované. V **hybridním režimu** může aplikace pracovat se sdíleným centrálním adresářem souborů. Aplikace P2P může být provozována v síti klient-server (například sdílení souborů pomocí výměnné sítě Direct Connect (DC) ve firemní síti klient-server).
Síť typu peer-to-peer: spojení dvou nebo více počítačů, které mohou sdílet zdroje (jako je tiskárna, soubory, ...) bez toho, aby měla pro tuto službu vyhrazený (*dedicated*) server.



Výhody (peer to peer)	*Nevýhody (peer to peer)*
• snadno se vytvoří, • není centrální správa (co se týče nákladů na HW, SW a administrátora i případné právní odpovědnosti).	• není vhodné pro hierarchicky řízené organizace (chybí centrální správa), • špatné poskytování některých síťových služeb.

Síťové aplikační služby z pohledu uživatele (výběr)

Datové sítě jsou tu od toho, aby uživateli poskytovaly možnost komunikace pomocí **síťových aplikačních služeb**. Služby sítě jsou využívány v komunikačním modelu klient-server.

Služba	*Popis*
Jmenné služby	Klienti požadují od jmenného serveru domény překlad doménového jména na IP adresu. Pomocí databáze zdrojových záznamů na DNS serveru.
Vzdálené přihlášení	Klient se přihlásí jako virtuální terminál ke vzdálenému serveru Telnet
Souborové služby	Soubory jsou uloženy na určitém počítači, takzvaném souborovém serveru (file server). Ostatní, klientské počítače mohou ze souboru přímo číst a zapisovat, takže si je nemusí kopírovat na svůj pevný disk. Pro koncového uživatele je tato služba zpravidla transparentní (funguje bez jeho vědomí). Např. SMB, AFS (Linux).
Tiskové služby	K počítači, takzvanému tiskovému serveru (print server), je připojena tiskárna (tiskárny); klientský počítač odešle tiskový výstup do tis-

Služba	***Popis***
	kového serveru a ten jej odešle na tiskárnu. Tato služba je pro koncového uživatele většinou transparentní. Např. LPD, SMB.
Webové služby	Na serveru (Web server HTTP) je uloženo množství různých informací jako je například text, grafika, animace, video nebo zvukové klipy. Koncový uživatel odešle požadavek na informace z webového prohlížeče, server mu je vrátí a webový prohlížeč je zobrazí.
Elektronická pošta	Koncový uživatel sestaví v e-mailovém klientu zprávu elektronické pošty (e-mail) a odešle ji konkrétní osobě (uživatel@doména). Procesu doručování elektronické pošty se zúčastní různé e-mailové servery (E-mail Server). Využívá protokoly SMTP a POP3 nebo IMAP.
Dynamická konfigurace klientů v lokální síti	Klientská stanice si požádá o přidělení (zapůjčení) IP adresy a masky z DHCP serveru.

Protokoly aplikační vrstvy

Protokol aplikační vrstvy	***RFC***	***Protokol transportní vrstvy***	***Číslo „dobře známého“ portu***
Domain Name System (DNS)	1034, 1035	TCP/**UDP**	53
Hypertext Transfer Protocol (HTTP)	2616	TCP	80
Simple Mail Transfer Protocol (SMTP)	2821, 821	TCP	25
Post Office Protocol version 3 (POP3)	1939	TCP	110
Internet Message Access Protocol version 4 (IMAP4)	3501	TCP	143
Telnet	854	TCP	23
Dynamic Host Configuration Protocol (DHCP)	2131	UDP	67 (*bootstrap*)
File Transfer Protocol (FTP)	959	TCP	20 a 21
Simple Network Management Protokol (SNMP)	1157	UDP	161, 162 (*trap*)

- Protokoly aplikační vrstvy pracují v **komunikačním režimu klient-server**.
- Standardy pro sadu protokolů TCP/IP se nazývají **RFC (***Requests for Comments* = žádosti o komentáře**)**, které udržuje ***Internet Engineering Task Force*** (http://www.ietf.org/).
- **Čísla dobře známých portů aplikačních protokolů (*well-known ports*)** a jména **domén nejvyššího řádu (TLD = *Top Level Domains*)** přiděluje ***IANA*** *(Internet Assigned Numbers Authority)* (http://iana.org).

Servery poskytující služby

Jednotlivé síťové služby definované protokoly na aplikační vrstvě OSI jsou realizovány běžícími programy typu démon na serveru. Démon čeká na požadavky klientů. Klienti služby potom přistupují na server tuto službu poskytující (v komunikačním modelu klient-server). Pro zlepšení výkonu

sítě je vhodné, pro každou hodně používanou službu, mít vyhrazený (*dedicated*) server. Této architektuře se potom někdy říká **farma serverů** (*server farm*). Obvykle jde též o síť typu klient-server.

Jmenné služby a DNS

Domain Name Service (DNS) protokol pro překlad (*resolve*) jmen Internetových domén (= doménových jmen) na IP adresy. (Proto se také klientu služby DNS říká *DNS resolver*.) Doménové jméno je jednoznačná identifikace jednoho síťového hostitele nebo jedné celé v sítě v Internetu. Domény mají hierarchickou stromovou strukturu. Každý jmenný server (DNS server) má jednoznačně definován nadřazený server a DNS klient (*DNS resolver*) má jednoznačně definován svůj DNS server. Na nejvyšší úrovni doménového jména (od prava) je prázdná doména 0. řádu a pod ní domény 1. řádu, 2. řádu, atd. oddělené tečkami. Celková maximální délka řetězce se jménem domény je 255 znaků s až 127 úrovněmi. Ve jméně domény lze použít ASCII znaky písmena a číslice, nerozlišuje malá/velká písmena. Doména nultého řádu (kořenový uzel) je obhospodařována 13-ti kořenovými servery (*root name server*, http://www.root-servers.org).

Plné doménové jméno

(*FQDN - Fully Qualified Domain Name* – plné doménové jméno služby v doméně)
Například www.seznam.cz: jednotlivé domény jsou odděleny tečkou, odprava 1., 2., řádu. Kde CZ = doména prvního řádu, SEZNAM = doména druhého řádu, WWW = doména třetího řádu, atd.
Doména prvého řádu se také nazývá **doména nejvyššího řádu** (*TLD, Top Level Domain*) jsou celosvětově přidělované IANA (*Internet Assigned Numbers Authority*), kterou nyní řídí ICANN (anglicky „aj ken“, *Internet Corporation for Assigned Names and Numbers*):

- ccTLD (*country code*, národní, dvouznakové kódy zemí, .cz, .uk, .us, .sk (ISO-kódy zemí)),
- gTLD (*generic*, všeobecné, generické, tříznakové kódy oboru činnosti vlastníka domény, .biz, .com, ,org, .gov., .mil, .edu, nově 4-znakové: .info,
    - sponzorované (sponsored) všeobecné domény (nově též 4-6 znakové: .museum, .jobs, ...).

Typ	*Doména*	*Popis*
gTLD		**Generic Top Level Domain - Všeobecná doména nejvyššího řádu – určuje typ organizace**
	.COM	Komerční organizace
	.EDU	Vzdělávací instituce (exkluzivní použití pouze v USA)
	.GOV	Vládní instituce (exkluzivní použití pouze v USA)
	.MIL	Armádní skupiny (exkluzivní použití pouze v USA)
	.NET	Hlavní správní síťová centra
	.ORG	Neziskové organizace
	.ARPA	Infrastrukturní doména ARPANETu.
	.INT	Mezinárodní organizace
ccTLD		**Country Code Top Level Domain - národní doména nejvyššího řádu**

Typ	*Doména*	*Popis*
	.CZ	Česká republika
	.SK	Slovenská republika
	.DE	Spolková republika Německa
	.UK	Spojené království
	.EU	Evropská unie

Registrovaná doména

Správa domén nejvyššího řádu: http://www.iana.org/ → www.iana.org/cctld/ .
Doména 1. a 2 řádu tvoří dohromady tzv. **Registrované domény**, domény 2. řádu jsou přidělovány **registrátorem** (*domain name registrar*) (= *Network Information Centre, NIC*) příslušné domény 1. řádu. (Například pro ČR je to správce domény http://nic.cz pro doménu EU http://www.eurid.eu/). Další doménu 3. řádu pro konkrétní službu (nebo pro další síť) už definuje správce příslušné registrované domény.

Formát zpráv DNS

DNS používá ten samý formát zpráv pro:
- všechny typy dotazů z klientů a odpovědí ze serverů,
- chybová hlášení,
- přenos informací ze zdrojových záznamů do jiných serverů

Formát zprávy (5 sekcí DNS zprávy):
- záhlaví (*Header*) – hlavička DNS zprávy
- dotaz (*Question*) – dotaz na jmenný server DNS
- odpověď (*Answer*) – odpověď DNS serveru na dotaz
- autorita (*Authority*) – sekce ukazující na autoritativní servery (autoritu)
- dodatečné informace (*Additional*) – další dodatečné informace ze zdrojového záznamu

Na DNS serveru je databáze tzv. zdrojových záznamů.[26]

Protože dotaz na překlad domény na IP se řeší na více serverech, které jsou hierarchicky uspořádané, je celý DNS systém decentralizovaná hierarchická databáze.

Zdrojové záznamy

Zdrojové záznamy slouží na serveru DNS k převodu jmen domén na IP adresy a naopak.

Typy zdrojových záznamů DNS (*Resource Record*, *RR*):
- **A** – adresa koncového zařízení
- **NS** – autoritativní jmenný server
- **CNAME** – kanonické jméno (*canonical name*) (neboli úplné doménové jméno - *Fully Qualified Domain Name, FQDN*) pro alias; použito když má více služeb jednu síťovou adresu, ale každá služba má svůj vlastní záznam v DNS
- **MX** – záznam typu **mail exchange**; mapuje doménové jméno do seznamu serverů mail ex-

26 Před dotazem na jmenný server se klient vždy podívá do lokálního textového souboru /etc/hosts (ve Windows i v Linuxu) s lokálními překlady domén na IP adresy.

change (SMTP) které přijímají elektronickou poštu pro tuto doménu
Tyto typy lze při dotazu filtrovat.

Dotazy na jmenný sever v příkazové řádce

Utilita **nslookup**

Filtrace různých typů zdrojových záznamů DNS na (vzdáleném) jmenném serveru domény
nslookup
(příklad dotazu na mailové servery domény zvolením typu zdrojového záznamu = MX (mail exchanger) což je naslouchající SMTP server v příslušné doméně)

```
>set type=mx
>seznam.cz

>set type=ns                    //POZOR toto nevynutí autoritativní odpověď
>seznam.cz
>exit
```

Odpovědi se rozlišují na:

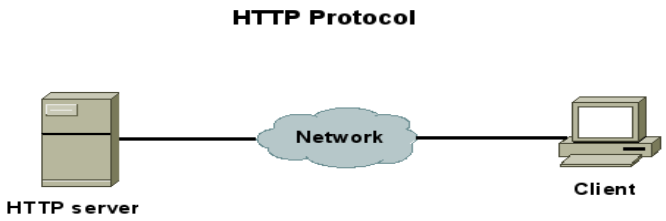
- autoritativní – odpověděl autoritativní jmenný server (NS) dotazované domény,
- neautoritativní – odpověděl jmenný server, který měl tento překlad ve vyrovnávací paměti (po předchozím dotazu).

V Linuxu je také ještě příkaz **dig** (kde lze, na rozdíl od nslookup, autorizovanou odpověď vynutit). Ve Windows je **dig** dostupná jako samostatná utilita.

Zobrazení DNS cache na lokálním klientu:
ipconfig /displaydns ve Windows (obdoba v Linuxu je *rndc dumpdb*)
Životnost záznamu (*Time to Live*) je uvedena v sekundách a výchozí hodnota je definována v autoritativním serveru domény, pokud je nastavena na 0, záznam se neukládá ve vyrovnávací paměti.

WWW a HTTP

Hypertext Transfer Protocol (HTTP) pro přenos souborů HTML (*HyperText Markup Language*, značkovací jazyk pro hypertext, jazyk párových značek pro tvorbu webových stránek), které vytvářejí webové stránky WWW (*World Wide Web*) z web serveru na web klienta. Většina webových stránek je přístupná přes protokol .



URL, URI

URL (*Uniform Resource Locator*) nebo také URI (*Uniform Resource Identifier*) je specifikace umístění zdrojů informací na Internetu („jednotný lokátor zdrojů“, „webová adresa“) zadávaná ve webovém prohlížeči (*web browser*).
Příklad formátu: http://jonatan.spse.pilsedu.cz:80/~cibulkova/index.php
(**protokol:// doména : číslo portu/adresář/soubor**)

Typy zpráv HTTP

1. GET – žádost klienta o data ze serveru. Webový prohlížeč posílá zprávu GET s žádostí o stránku na webový server. Když server dostane zprávu GET odpoví stavovou řádkou jako: HTTP/1.1 200 OK, a tělem (body), které může obsahovat požadovaný soubor, chybovou zprávu nebo nějaké jiné informace.
2. POST a PUT jsou použity k odeslání zprávy, která umisťuje (upload) data z klienta na webový server.
    - Například, když uživatel vloží data do formuláře vloženého do webové stránky, POST začleňuje data do zprávy posílané na server.
    - PUT – umisťuje (*upload*) zdroje nebo obsah na webový server. server.

Odposlechnutá komunikace:
HTTP GET /doma.html HTTP/1.1
HTTP HTTP/1.1 200 OK (text/html)

Třebaže je pozoruhodně flexibilní, není HTTP zabezpečený protokol. Zpráva POST umisťuje informace na server v podobě čistého textu, který může být zachycen a čten. Podobně odpovědi serveru, typicky HTML stránky, jsou také nešifrované.
Kde je třeba bezpečný provoz, je nutné používat šifrovaný protokol **HTTPS** (port 443/TCP) (HTTP over Secure Socket Layer).

E-mail a SMTP/POP

Simple Mail Transfer Protocol (SMTP) pro přenos emailových zpráv a jejich příloh (*attachments*) mezi poštovními servery (z klienta se přihlásím na poštovní server (SMTP) a odtud odešlu zprávu).

Ve své standardní základní verzi neposkytuje autentizaci uživatelů (je snadno zneužitelný).

Post Office Protocol (POP) pro přenos zpráv z poštovního serveru pro danou doménu na klienta. Umí stáhnout pouze všechny maily ze schránky.

(Inteligentnější služby stáhnutí pošty ze serveru klienta poskytuje **Internet Message Access Protocol (IMAP)**. Stáhne hlavičky zpráv a potom může stáhnout jednu konkrétní zprávu.)[27]

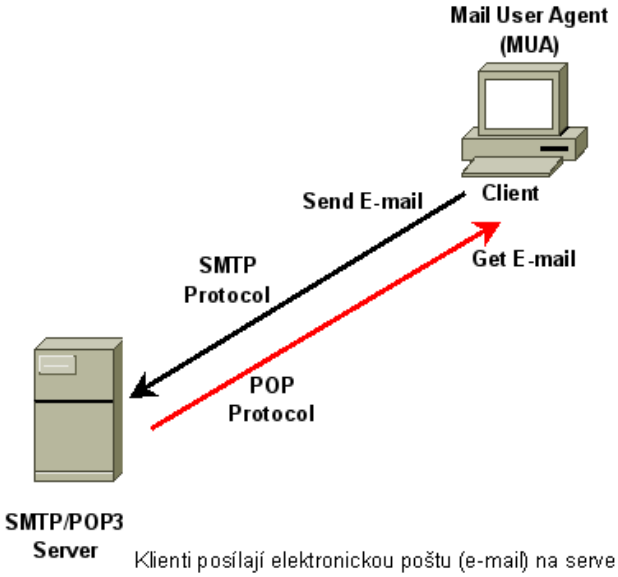
Aby bylo možné elektronickou poštu přijímat a číst „odkudkoliv“ nejenom ze vzdáleného přihlášení na poštovním serveru, má elektronická pošta následující strukturu:

- **Mail Transfer Agent (MTA) - poštovní přenosový agent** – ***poštovní server***, který je provozován jako program na počítači, jehož úkolem je zajišťovat poštovní transakce. tento program sám nedoručuje zprávy do jednotlivých poštovních schránek, pouze zprávy přebírá a zjišťuje podle jejich obálek, zda jsou přijatelné (tj. zda má jejich adresát na počítači zřízen poštovní účet). MTA je SMTP server.
  - Přijímá poštu od klientů (z MUA pomocí SMTP),
  - Posílá poštu mezi servery (mezi MTA pomocí SMTP),
  - Předává poštu ke konečnému doručení do MDA, který je ukládá do určených poštovních schránek.
- **Mail Delivery Agent (MDA) – *poštovní doručovací agent*** – program, který od MTA přebírá zprávy a ukládá je do skutečných poštovních schránek adresátů nebo je předává pro konečné doručení dalšímu MTA. (MTA i MDA jsou na jednom počítači.) MDA je server POP nebo IMAP.
  - Skutečné doručení do poštovní schránky
  - Řeší problémy cílového doručení (spam filtr, antivirová kontrola).
- **Mail User Agent (MUA) - poštovní uživatelský agent** – ***poštovní klient*** - program, který zprostředkuje uživateli odeslání poštovní zprávy a vyzvednutí došlých zpráv z jeho poštovní schránky. Psaní a čtení zpráv bývá zpravidla součástí tohoto programu, nicméně se mohou tyto úkony provádět samostatně pomocí textového editoru. MUA je v SMTP definován, ale detaily implementace nikoliv. MUA je klientem SMTP a zároveň POP nebo IMAP.
  - Získává zprávy pomocí POP nebo IMAP
  - Klient pomocí něho získává a čte poštu
  - **Mail Retrieval Agent (MRA) – agent vyzvedávání pošty**- uživatelský program, který zprostředkuje přístup do poštovní schránky uživatele, umístěné na vzdáleném poštovním serveru. MRA potom předá zprávy umístěné ve vzdálené schránce MUA.

Formát poštovní adresy: ***příjemce@doména***. Znak @ = zavináč čtěte anglicky jako „at“ (= na doméně).

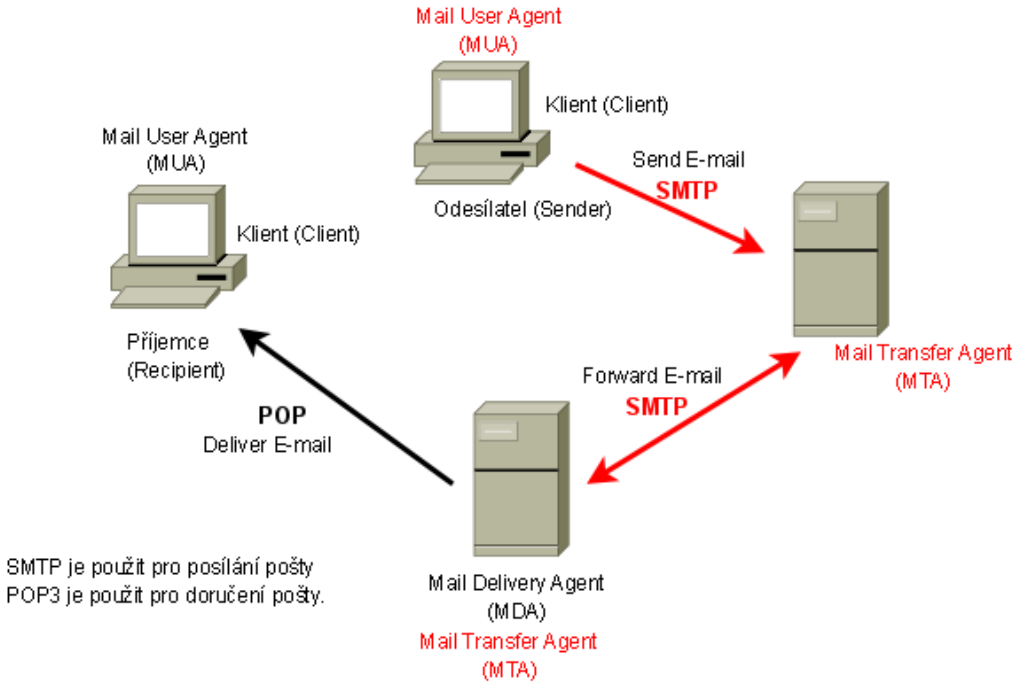
27 Kromě klienta e-mail, který přímo používá protokoly SMTP a POP3/IMAP4 je možné použít webovou aplikaci přes webové rozhraní. Tyto službu „zdarma“ nabízejí např.: centrum.cz, seznam.cz, gmail.com atd. (Uživatel za tuto službu platí čtením reklam.)

E-mail Client (MUA)



Klienti posílají elektronickou poštu (e-mail) na server pomocí SMTP a přijímají ji pomocí POP3 (nebo IMAP).

E-mail - celkové schéma komunikace



SMTP je použit pro posílání pošty
POP3 je použit pro doručení pošty.

Cvičení

Vytvoření SMTP zprávy (e-mail). Použijeme klienta protokolu Telnet pro připojení k serveru SMTP na portu číslo 25.

Telnet <doménové jméno> <číslo portu>
telnet mail.spse.pilsedu.cz 25

Komunikace se SMTP je nešifrovaná bez autentizace, pomocí textových příkazů (výběr):
HELO – přihlášení se k SMTP serveru
EHLO – novější verze HELO, rozšířené možnosti
MAIL FROM: – identifikace odesílatele (v základní verzi SMTP zde lze zapsat cokoli)
RCPT TO: – identifikace příjemce (*recipient*)
DATA – identifikace začátku těla zprávy (následuje tělo textové zprávy ve formátu RFC 822)
Ukončení těla zprávy = <CRLF>.<CRLF> (samotný znak „tečka“ na samostatné řádce)
QUIT – ukončení relace (sezení, *session*)

Kvůli možnému zneužití pošty např. spammery (šířícími nevyžádanou poštu) existuje i **rozšířená verze SMTP** (*Enhanced SMTP - ESMTP*) SMTP-AUTH s autentizací skutečného odesílatele. Pokud je na poštovním serveru použit SMTP-AUTH vynutí si použití SMTP-AUTH i na poštovním klientu. (V současné době je více než 90% elektronické pošty tvořeno nevyžádanou poštou – *spam*[28].)
Dalším typem zneužití neautentizované služby elektronické pošty je *phishing* (česky „rhybaření“), kdy odesílatel předstírá falešnou identitu, například Vaší banky a snaží se získat citlivé údaje, jako je číslo účtu/platební karty a jeho/její PIN.
Z důvodů snadné zneužitelnosti elektronické pošty je vhodné kontrolovat i zdrojový text e-mailové zprávy. V něm lze nalézt SMTP servery, přes které byla zpráva odeslána.

Přenos souborů a FTP

FTP

File Transfer Protocol (FTP) pro interaktivní přenos souborů mezi systémy.
Je to nešifrovaný protokol. (Síťový profesionál, všude tam kde to jde, používá ssh a scp.)
FTP vytváří dvě spojení mezi klientem a serverem – jedno pro přenos příkazů z klienta a (port 21) a druhé pro přenos souborů (port 20). Na serveru je spuštěn FTPd (démon FTP)
Příkazy:

- open (připojit se ke vzdálenému FTP serveru),
- dir (vypsat obsah adresáře),
- put (poslat jeden soubor),
- get (přijmout jeden soubor).
- Pro přenos mezi různými operačními systémy nebo raději vždy používejte binární typ přenosu (>binary).

Příklad stažení souboru pomocí FTP (v závorce jsou komentáře):
C:\>ftp
>open jonatan.spse.pilsedu.cz (= otevření relace s FTP serverem)

28 Spam – jméno (***Sp****iced h****am***) vzniklo na základě scénky britské skupiny *Monty Python's Flying Circus*.

>user: **ftp**[29]
>password: *heslo*
>dir (= výpis obsahu vzdáleného pracovního adresáře)
>cd pub (= změna vzdáleného pracovního adresáře (na pub))
>binary (= binární režim přenosu)
>dir
>get *soubor* (= stáhnutí souboru (*vyberte si sami jeho jméno*))
>close (= ukončení relace se serverem ftp)
>bye (= ukončení relace ftp a ukončení klienta ftp)

>quit (nebo exit) (= ukončení relace ftp a ukončení klienta ftp)

```
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x[30]    4 0        0            4096 Sep 23  2005 3303
-rw-r--r--     1 0        0         2581027 Jul 01  2005 BlueJ.zip
```

Ve výpisu obsahu adresáře jsou zvýrazněna přístupová práva.

Přenosové režimy:

- **aktivní** – klient inicializuje sezení pro **řízení přenosu** na serveru na dobře známém portu TCP 21 (ve WireSharku označeno jako protokol FTP) a **server iniciuje spojení pro přenos dat ze zdrojového portu TCP 20** na serveru a na cílovém portu větším než 1023 na klientu (ve WireSharku označeno jako protokol FTP-DATA). Pokud je na FTP klientu instalován firewall, může toto spojení selhat. Je třeba povolit otevření spojení FTP na klientu ze serveru nebo vypnout SPI (*Stateful Packet Inspection*) na firewallu. Též aktivní režim nelze provozovat na klientech s privátní adresou (za NAT = *Network Address Translation*, „IP maškaráda“[31]) – server nevidí konkrétní stanici.
- **pasivní** – klient iniciuje spojení na serveru na portu TCP 21 (to samé jako v aktivním režimu). Pro přenos dat jsou zde ale dvě důležité změny – **klient iniciuje datový přenos** na serveru a pro oba konce tohoto spojení (FTP-DATA) jsou použity dynamicky přidělované porty (vyšší než 1023), nepoužívá tedy port 20. (Projde potom přes SPI firewall.)

Změnu přenosového režimu nepodporují všichni FTP klienti.

Přehled příkazů FTP:

```
ftp>help
!           delete      literal     prompt      send
?           debug       ls          put         status
append      dir         mdelete     pwd         trace
ascii       disconnect  mdir        quit        type
bell        get         mget        quote       user
binary      glob        mkdir       recv        verbose
bye         hash        mls         remotehelp
cd          help        mput        rename
close       lcd         open        rmdir
```

29 V OS Linux je místo položky User položka Name. V příkladu je použito jako jméno uživatele slovo ftp.
30 Obdoba práv v Linux/Unix: r-Read, w-Write, x=eXecute, d=Directory (vždy pro vlastníka, skupinu a ostatní).
31 NAT zajišťuje překlad privátní IP adresy na veřejnou a naopak. (Probereme později.)

FTP je nezabezpečený protokol. Je vhodnější použít zabezpečený přenos souborů pomocí SFTP nebo příkaz SCP po přihlášení v SSH.

Cvičení:

zachycení komunikace FTP -> heslo ve WireShark (***Capture (Start, Stop)*** → ***Analyze*** → ***Follow TCP Stream***).

TFTP

Trivial File Transfer Protocol (TFTP) pro zjednodušený přenos souborů. Běží na transportním protokolu UDP. Vzhledem k FTP umožňuje pouze omezený počet příkazů (příkazy PUT a GET plus něco málo dalšího):

```
tftp>?
connect       mode          put           get           quit
verbose       trace         status        binary        ascii
rexmt         timeout       ?
```

Protože je velmi jednoduchý vejde se tento protokol i do paměti ROM na síťové kartě a může sloužit k zavedení operačního systému ze sítě do bezdiskových stanic[32]. Používá se dále například pro přenos obrazu operačního systému po „katastrofě“ (smazání nebo upgrade OS) do směrovače nebo pro přenos konfiguračních souborů směrovačů (viz druhý semestr).

Konfigurace hostitele a DHCP

Bez **DHCP (Dynamic Host Configuration Protocol),** protokolu pro dynamickou konfiguraci hostitelských počítačů, by uživatelé (nebo administrátoři) museli ručně nastavovat:

- IP adresu,
- masku podsítě,
- výchozí bránu,
- primární a sekundární DNS server, ...

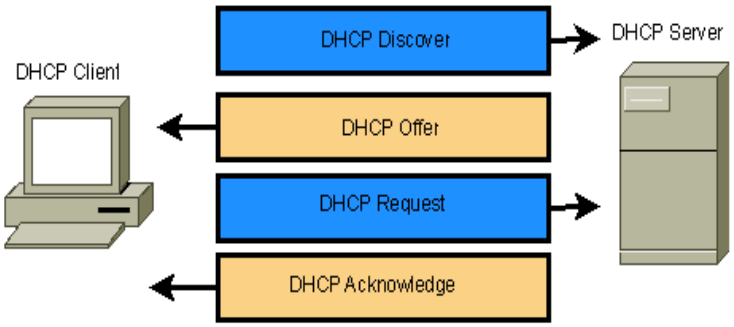
Na každém klientu (uzlu) sítě.

DHCP server udržuje povolený sdílený rozsah (*pool*) IP adres a zapůjčuje IP adresu každému DHCP klientu po jeho zapnutí.

Způsoby zapůjčování – možná nastavení:

- V některých případech je lepší adresy **dynamicky** zapůjčovat z a po odhlášení klienta vracet do **sdíleného rozsahu** (*pool*) k opětovnému zapůjčení,
- než adresy přidělovat **staticky** (= přidělovat stejnému zařízení stále stejnou adresu podle jeho MAC adresy) (tzv. Statické mapování).

32 Při natažení OS do bezdiskové stanice ze sítě je jméno obrazu zaváděného OS nastaveno přímo na serveru TFTP. (Na klientu to nelze, není kde.)



DHCP Discover (poptávka klienta →)	(broadcast)[33]
DHCP Offer (nabídka DHCP serveru ←)	(unicast - L2)[34]
DHCP Request (žádost klienta →)	(broadcast)
DHCP Acknowledge (potvrzení přiděleného nastavení ze serveru ←)	(unicast - L2)[35]

Příklad odposlechnuté komunikace (Linux):

DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 4	(broadcast)
DHCPOFFER from 172.16.1.1	(unicast - L2)
DHCPREQUEST on eth0 to 255.255.255.255 port 67	(broadcast)
DHCPACK from 172.16.1.1	(unicast - L2)[36]

Všimněte si: IP adresa je zde binárně samé jedničky = B/C (broadcastová = všesměrová, nesměrová adresa) na žádostech ze strany klienta (protože klient není nastavený a tedy neví, kde je v síti server DHCP)

Cvičení:

- #dhclient, odposlech Wireshark: **ipconfig /renew**, **ipconfig /release**.
- Totéž nasimulovat v PacketTraceru (viz poslední cvičení v PT v této kapitole.)

Vzdálené přihlášení

Telnet

Patří mezi nejstarší protokoly TCP/IP z počátku sedmdesátých let. **Telnet (TELetype NETwork Service)** - protokol (služba) **emulace terminálu**, pro **vzdálený přístup** k serverům a síťovým zařízením. Relace **VTY (Virtual Terminal)** vytvoří rozhraní příkazové řádky (*command line interfa-*

33 Broadcast = všesměrové (nesměrové, oběžníkové) vysílání. Toto vysílání přijmou všichni zapnutí hostitelé v síti. Klient není nastaven a tedy neví, kde je DHCP server.

34 V případě zapnutí DHCP klienta (zapnutí počítače) je místo transakce DHCP Offer provedena transakce DHCP Inform.

35 Unicast = jednosměrové vysílání.

36 Pokud už je adresa, která se má přidělit pomocí statického mapování v DHCP, přidělená staticky, klient o tom pošle zprávu DHCPDECLINE. Samotnou skutečnost již přidělené adresy klient zjistí pomocí protokolu ARP.

ce (CLI)) připojení na vzdáleném zařízení např. routeru. OS Linux i Windows mají v řádkovém rozhraní (příkazovém řádku) klient Telnetu.
Na serveru běží démon Telnetu. Aplikace běžící jako klient Telnetu jsou např.: HyperTerminal, Minicom, PuTTY a TeraTerm.
Jakmile je vytvořeno spojení telnetu, uživatel může vykonávat všechny autorizované operace na serveru, jako by byl v příkazové řádce samotného serveru. Jestliže na to má práva, může startovat a vypínat procesy, konfigurovat zařízení nebo přímo vypnout celý systém.

Spuštění – formát příkazu: *telnet [host] [port]*
Telnet URL: *telnet://<user>:<password>@<host>:<port>/*

Každý příkaz telnetu se skládá nejméně ze 2 bajtů: První bajt je speciální znak, který se nazývá *Interpret as Command* (IAC). Jak jeho jméno naznačuje, IAC definuje další bajt jako příkaz spíše než text.

Příklady příkazů protokolu Telnet:

- Are You There (AYT) – dovolí uživateli požádat, aby se něco objevilo na obrazovce terminálu, aby se potvrdilo, že relace VTY je aktivní.
- Erase Line (EL) – smaže všechen text z aktuální řádky.
- Interrupt Process (IP) – pozastaví, přeruší, zruší nebo ukončí (*Suspends, interrupts, aborts, or terminates*) proces, ke kterému je VTY připojen. Například, jestliže uživatel spustil program na serveru telnet prostřednictvím VTY, může odeslat IP příkaz, který program ukončí.

Protože Telnet je nešifrovaný protokol, síťový profesionál vždy (pokud to lze) použije zabezpečený protokol ssh.

SSH

Ačkoliv Telnet poskytuje autentizaci uživatele je to nešifrovaný protokol. Proto síťový profesionál, všude tam kde to lze, používá protokol **ssh (Secure Shell – zabezpečené (šifrované) vzdálené připojení)**. **SSH** poskytuje **3 základní komponenty zabezpečené komunikace**:

- autentizace obou účastníků komunikace,
- šifrování přenášených dat,
- integrita dat.

Správa sítě a SNMP

Simple Network Management Protocol. Výměna informací mezi síťovým zařízením a administrativní konzolí o správě síťového zařízení. Například vzdálené zapnutí síťové tiskárny.

Sdílení souborů a protokol SMB

Server Message Block (SMB) je protokol pro sdílení souborů typu klient/server. Vytvořen IBM na začátku osmdesátých let, aby popisoval strukturu sdílených síťových zdrojů, jako jsou adresáře, soubory, tiskárny a sériové porty. Na rozdíl od FTP klient SMB vytvoří dlouhodobé spojení se serverem a uživatel na klientu může přistupovat ke zdrojům na serveru, jako by to byly lokální zdroje na klientském hostiteli.
Počínaje Windows 2000, všechny produkty Microsoft používají DNS a to umožňuje protokolům

TCP/IP přímo podporovat sdílení zdrojů pomocí SMB.
OS LINUX a UNIX poskytují metodu sdílení zdrojů se sítěmi Microsoft s použitím verze SMB, která se nazývá SAMBA. OS Apple Macintosh také podporují sdílení pomocí protokolu SMB.
Zprávy SMB mohou:

- startovat, **autentizovat** a ukončit relace,
- řídit přístup k souborům,
- dovolují aplikaci posílat a přijímat zprávy na nebo z jiného zařízení.

Služba P2P a protokol Gnutella

Sdílení souborů přes Internet je stále více populárnější. P2P aplikace založené na protokolu Gnutella, umožňují lidem sdílet soubory na svém harddisku pro download s jinými jako Gnutella peer. Klient dovoluje hledat sdílené zdroje na jiných peer klientech. Aplikace: BearShare, Gnucleus, LimeWire, Morpheus, WinMX a XoloX. Gnutella Developer Forum udržuje základní protokol, dodavatelé aplikací často protokol rozšiřují, aby lépe spolupracoval s jejich konkrétními aplikacemi.

Gnutella definuje 5 typy paketů:

- ping – pro hledání zařízení,
- pong – odpověď na ping,
- query – dotaz pro lokalizaci souboru,
- query hit – jako odpověď na dotaz query,
- push – jako požadavek downloadu.

Služba Instant Messaging

Služba umožňující uživateli sledovat, kteří uživatelé služby jsou právě připojeni, a dle potřeby jim posílat zprávy, „četovat“ (*chat*, *chatting*), přeposílat soubory.
Výhody proti elektronické poště:

- je rychlejší,
- odesílatel vidí, zda je příjemce „na příjmu“.

Inteligentní uživatel sítě používá vždy, pokud jsou k dispozici, zabezpečené (šifrované) verze protokolů. Pro naši výuku používáme nezabezpečené verze protokolů mimo jiné právě z důvodu možnosti jejich snadného odposlechu a jejich jednoduchosti ve srovnání se zabezpečeným ekvivalentem.

Cvičení

Wireshark:
odposlech provozu aplikačních protokolů: FTP, SMTP (přes Telnet a port 25), DHCP (v příkazové řádce Windows použít **ipconfig /release, ipconfig /renew**). Pozor, aby hostitelský počítač byl nastavený jako DHCP klient. (Ovládací panely – Síťová připojení – Vlastnosti – TCP/IP – vlastnosti.)

Cvičení na aplikační protokoly v PacketTraceru

Poznámka: doporučení (best practices) Cisco pro adresaci jsou následující: klienti jsou adresováni od adresy sítě vzestupně nahoru a gateway (routery, servery) jsou (obvykle) adresováni od adresy všesměrového vysílání sestupně dolů.

Spojte počítač PC0 + Server překříženým (měli bychom již vědět proč) měděným kabelem přes roz-

hraní FastEthernet.
Nastavení PC:

- Config FastEthernet: zapnout použití DHCP

Nastavení Serveru:

- Config Interface:
  - Fast Ethernet: port status on, IP adresa: 192.168.1.254 a maska 255.255.255.0
- Config Services:
  - : on
  - DHCP :on
    - default gateway: 192.168.1.254
    - DNS server: 192.168.1.254
    - start IP address: 192.168.1.1, maximum nuber of users: 254
  - DNS domain name: www.ahoj.cz, IP address: 192.168.1.254

1. Vytvořenou konfiguraci si vždy uložte.
2. Nechte z příkazové řádky počítače PC0 znovu přidělit IP adresu: ipconfig /release, ipconfig /renew.
3. Otevřete z webového browseru PC0 stránku na www.ahoj.cz.,
4. Krokujte **v simulačním režimu** jednotlivé protokoly pro tyto akce a podívejte se na obsah zapouzdření na jednotlivých vrstvách OSI modelu. Prozkoumejte použité unicastové a broadcastové adresy IP i MAC (zdrojové i cílové).
5. Zjistěte, na kterém transportním protokolu běží protokol DNS.

Termíny, které bychom měli znát

Unicast – jednosměrové vysílání (též směrové vysílání) - jednosměrová, směrová adresa (přijme jeden konkrétní hostitel (stanice) v síti)

Broadcast – všesměrové vysílání (též nesměrové vysílání, všeobecné oběžníkové vysílání, všeobecný oběžník) - všesměrová, nesměrová adresa (přijmou všichni právě aktivní hostitelé v dané síti)

Multicast – skupinové vysílání (též vícesměrové vysílání, adresný oběžník) – skupinová adresa (přijme určitá skupina hostitelů např. všechny routery se směrovacím protokolem OSPF v určité skupině sítí).

Kontrolní opakovací otázky a odpovědi (kvíz):

1) Ze kterých tří vrstev OSI modelu se skládá aplikační vrstva TCP/IP modelu? (Uveďte tři.)
   a) aplikační,
   b) prezentační,
   c) relační.
2) Který protokol je použit pro přenos webových stránek ze serveru na klienta (nebo html)?
   a)
3) Jaký termín se používá pro přenos dat z klienta a jejich umístění na server?
   a) Upload (umisťování, nahrávání)
4) Protokoly aplikační vrstvy používající/nepoužívající autentizaci a šifrování

a) používající: HTTPS, SSH

b) nepoužívající: , DNS, SMTP

5) V následující URL: http://www.cisco.com/web/learnig/netacad/index.html, co je doména nejvyššího řádu (*Top Level Domain, TLD*)?

a) .com

6) Spárujte jednotlivé typy zdrojových záznamů DNS (*DNS resource record*) s jejich popisy:

a) A = adresa koncového zařízení,

b) NS = autoritativní jmenný server (*authoritative name server*),

c) CNAME = kanonické jméno neboli *Fully Qualified Domain Name (FQDM)* pro alias,

d) MX = mapuje doménové jméno na seznam mailových serverů (*Mail Exchange Servers*) pro tuto doménu.

7) Spárujte funkce s příslušnými komponentami elektronické pošty:

a) MTA (poštovní přenosový agent):

i. přijímá poštu z klienta,

ii. přeposílá poštu mezi servery pomocí protokolu SMTP.

b) MDA (poštovní doručovací agent):

i. řeší problémy koncového doručení (například spamový a virový filtr),

ii. provádí skutečné doručení do poštovní schránky příjemce (*mail box*).

c) MUA (poštovní uživatelský agent):

i. klient ho používá k přístupu a ke čtení pošty,

ii. stahuje poštu pomocí protokolu POP (nebo IMAP).

8) Administrátor odstraňuje chybu při přístupu k www.cisco.com. Při zápisu IP adresy webového serveru v prohlížeči se korektně otevře požadovaná webová stránka. Který aplikační protokol je zodpovědný za toto selhání?

a) DNS.

Kapitola 4 – Transportní vrstva

V této kapitole se naučíme:

- Vysvětlit požadavky na transportní vrstvu.
- Identifikovat roli transportní vrstvy při poskytování koncového („*end-to-end*“) přenosu dat mezi aplikacemi (procesy).
- Popsat funkci dvou transportních protokolů TCP/IP: TCP a UDP.
- Vysvětlit klíčové funkce transportní vrstvy včetně spolehlivosti, adresace portů a segmentace.
- Vysvětlit, jak každý TCP i UDP pracují se svými klíčovými funkcemi.
- Určit, kdy je vhodné použít TCP nebo UDP a uvézt příklady aplikací, které používají příslušný protokol.

Transportní vrstva umožňuje jednomu zařízení paralelní vícenásobnou komunikaci více aplikací přes síť v jedné chvíli. Pokud je to požadováno, zajistí, že data jsou přijata spolehlivě (=> spojově orientovaný protokol) a vždy ve správné aplikaci. Může používat mechanismy pro detekci a odstranění chyb.
Transportní vrstva:

- segmentuje data zprávy,
- přidává záhlaví pro správné doručení dat konkrétnímu procesu v síti,
- řídí opětovné složení zprávy v cíli.

Zajišťuje:

- sledování a řízení jednotlivých (z mnoha simultánních) komunikací mezi aplikacemi na zdrojové a cílové stanici (*multiplexing*),
- segmentace dat a řízení každého segmentu (pro snazší správu a přenos) (*Segmentation*),
- znovu složení jednotlivých segmentů do tvaru původní zprávy (aplikačních dat) (*Reassembly*),
- identifikace různých aplikací (aplikačních protokolů) prostřednictvím čísla portu.

Spojově orientované a nespojové protokoly

Protokol	***Atributy***
Nespojový, nespojově orientovaný (*connectionless oriented*)	Nejvyšší výkon při doručování dat; vysoká rychlost doručení; nízká režie; schází možnost obnovy nebo opakovaného odesílání dat. Doručuje data v pořadí, jakém přijal. „Nespolehlivý“ (*unreliable*) znamená, že doručení není potvrzováno. PDU pro nespojový protokol se nazývá datagram.
Spojově orientovaný (*connection oriented*)	Ustavení relace (*session*) před samotným přenosem dat z vyšší vrstvy[37]; zrušení relace; potvrzování, sekvenční zpracování; řízení toku dat – správa zahlcení; udržování spojení; spolehlivý, zaručený přenos dat; doručení dat ve stejném pořadí, jako byly vyslány; nižší rychlost doručování; velká režie; možnost zotavení z chyb; možnost opakování přenosu dat. „Spolehlivý“ (*reliable*).

Vývojáři aplikací si vždy vybírají vhodný protokol transportní vrstvy na základě požadavků na

37 Hořejší vrstva (upper layer) je míněna vyšší vrstva než transportní (v TCP/IP modelu tedy aplikační).

konkrétní aplikaci.
U transportní vrstvy modelu OSI předpokládáme pouze spojovaný a spolehlivý protokol v modelu TCP/IP jsou protokoly transportní vrstvy dva: spojovaný, spolehlivý (TCP) a nespojovaný, nespolehlivý (UDP).

Použití čísel portů

Adresace pomocí čísla portu identifikuje jednotlivé síťové konverzace. Například na počítači současně přijímající a odesílající e-mail, IM, webové stránky a telefonní hovor VoIP.

Služby založené na TCP a UDP musí odlišit různé aplikace, které spolu komunikují. K odlišení komunikací mají segmenty a datagramy, jak TCP tak i UDP, v záhlaví pole, které jednoznačně identifikují tyto aplikace. Těmito jedinečnými identifikátory jsou **čísla portů**. V záhlaví každého segmentu nebo datagramu jsou vždy **zdrojový a cílový port**. Číslo zdrojového portu je číslo spojené, pro tuto konkrétní komunikaci, se zdrojovou aplikací na lokálním počítači. Číslo cílového portu je číslo, pro tuto konkrétní komunikaci, spojené s cílovou aplikací na vzdáleném počítači.

Čísla portů jsou přiřazena různými způsoby, v závislosti na tom, zda je konkrétní zpráva žádost (*request*) nebo odezva (*response*). Zatímco procesy na serveru mají k sobě přiřazena statická čísla portů, klienti dynamicky volí číslo portu pro každou jednotlivou konverzaci.

Když klientská aplikace pošle požadavek na aplikační server, **cílový port** obsažený v záhlaví je číslo portu, který je přiřazen k příslušné službě[38] démona (*daemon*) běžícího na vzdáleném počítači. Klientský software musí vědět, jaké číslo portu je spojené s procesem serveru na vzdáleném počítači. Toto číslo cílového portu je nastaveno buď v implicitním nastavení nebo ručně. Například: když aplikace webového prohlížeče pošle dotaz na webový server, prohlížeč používá TCP a číslo portu 80, pokud není uvedeno jinak. To proto, že TCP port 80 je standardní port přiřazený k aplikacím pro obsluhu webu. Mnoho běžných aplikací má implicitní přiřazení čísel portů.

Zdrojový port v záhlaví segmentu nebo datagramu požadavku klienta je náhodně vygenerován z čísel portů větších než 1023. Tak dlouho, dokud to není v rozporu s dalšími porty použitými v systému, si klient může vybírat libovolné číslo portu z rozsahu implicitních čísel portů používaných příslušným operačním systémem. Toto číslo portu funguje jako zpáteční adresa pro žádající aplikaci. Transportní vrstva sleduje tento port a aplikaci, která inicializovala žádost, takže když se vrátí odezva, může být předána správné aplikaci. Číslo portu žádající aplikace je používáno jako cílové číslo portu v odpovědi navracející se ze serveru.

Kombinace čísla portu transportní vrstvy a IP adresy přiřazené k hostiteli na síťové vrstvě jednoznačně identifikuje daný proces běžící na konkrétním hostitelském počítači. Tato kombinace se nazývá **socket**. Občas můžete najít používány termíny číslo portu a socket zaměnitelně. V rámci tohoto kurzu, termín socket odkazuje jen na jedinečnou kombinaci IP adresy a čísla portu. Dvojice socketů skládající se ze zdrojových a cílových IP adres a čísel portů, je také unikátní a identifikuje konkrétní konverzaci mezi dvěma počítači.

Například: HTTP požadavek webové stránky odeslaný na webový server (port 80) běžící na hostitelském počítači s L3 IPv4 adresou 192.168.1.20 by byl určen pro socket 192.168.1.20:80. Pokud webový prohlížeč požaduje webovou stránku běží na hostiteli 192.168.100.48 a dynamické číslo portu přidělené webovému prohlížeč je 49152, socket pro tyto webové stránky by 192.168.100.48:49152.

38 Viz dobře známé porty http://www.iana.org/assignments/port-numbers

Socket = IP adresa:číslo portu například 192.168.1.1:80
Dvojice socketů (zdrojový a cílový) je unikátní a jednoznačná pro jednu síťovou komunikaci. Určuje pro jednu komunikaci konkrétní koncové uzly sítě a konkrétní komunikaci na konkrétním aplikačním protokolu.

- Dvojice čísel portů (zdrojového a cílového) jednoznačně určuje na koncových uzlech sítě jednu komunikaci mezi koncovými procesy v jednom aplikačním protokolu.
- Zdrojový port komunikace z klienta na server je cílovým portem ve zpětné komunikaci ze serveru na klienta. A naopak cílový port komunikace z klienta na server je zdrojovým portem v komunikaci ze serveru na klienta.
- **Jeden samostatný server nemůže mít dvě služby přiřazené k jednomu číslu portu uvnitř jedné služby transportní vrstvy (jednoho protokolu transportní vrstvy)**. Pro jednu službu – jeden otevřený port. Na jednom serveru může být takto otevřeno více portů – služeb.

Dva základní protokoly: TCP a UDP

Základní rozdíl mezi TCP a UDP je spolehlivost (ve smyslu potvrzování doručených dat a spolehlivosti doručení).

TCP (Transmission Control Protocol)

- PDU: segment,
- spojově orientované konverzace[39] (vytvoření relace – *session* = „třícestné navázání spojení“ (3 transakce) před samotným přenosem dat z vyšší (aplikační) vrstvy, a nakonec ukončení spojení (4 transakce)),
- spolehlivé doručení,
- složení doručených dat do správného (původního) pořadí (*reassembly in same order*, *delivers data in order sent*),
- řízení toku dat (*data flow control*) a správa (předcházení, *avoiding*) zahlcení (*congestion management*),
- nevýhodou - cenou za to - je:
  - velká režie (*overhead*),
  - menší rychlost přenosu (část šířky pásma, přenosové kapacity (*bandwidth*) přenosového kanálu spotřebuje režie (*overhead*)).

To se zajistí pomocí:

- sekvenčních, pořadových, čísel (*sequence numbers*, SEQ) a jejich synchronizace,
- potvrzování doručení (čísla potvrzení, *acknowledgement numbers*, ACK),
- znovu odesílání nepotvrzených dat,
- mechanismu posuvného okénka (*sliding window, window size*).

Použití: spolehlivý přenos dat (FTP, HTTP, SSH, SMTP, POP, IMAP, ...).

UDP (User Datagram Protocol)

- PDU: datagram,
- nespojově orientované komunikace,
- nespolehlivé doručení (nepotvrzované),

39 Konverzace = dialog mezi dvěma stranami. V IT konverzace označuje veškerý provoz mezi zdrojem a koncovým uzlem, aby proběhlo uskutečnění transakce.

- data jsou složena v tom pořadí, ve kterém došla (nemusí souhlasit s původním pořadím),
- výhodou je:
  - jednoduchá implementace (programová realizace) – nepotřebuje mnoho systémových zdrojů,
  - malá režie,
  - velká rychlost.

Použití: DNS, SNMP, DHCP, RIP, TFTP, Video Streaming, IP telefonie (VoIP), online hry.

- Domain Name System (DNS) ,
- Simple Network Management Protocol (SNMP) ,
- Dynamic Host Configuration Protocol (DHCP)[40],
- Routing Information Protocol (RIP) ,
- Trivial File Transfer Protocol (TFTP).

Porovnání TCP a UDP

Funkce transportní vrstvy	***Popis***	***TCP***	***UDP***
Segmentace dat (*segmentation*)	před odesláním dělí data (souvislý datový tok (*data flow*) z aplikace) do segmentů, po přijetí je znovu sestavuje, připravuje data pro přenos přes nejnižší čtyři vrstvy OSI modelu	Ano	Ano
Multiplexing pomocí čísel portů (*multiplexing*)	identifikuje aplikaci (proces) podle čísla portu, v jedné chvíli může být v síti více různých komunikací najednou	Ano	Ano
Spojovaný protokol (*connection oriented protocol*)	spojově orientovaný protokol – před samotným přenosem dat z vyšší vrstvy navazuje spojení mezi vysílající a přijímající stranou, vytváří relaci (sezení, *session*)	Ano	Ne
Detekce chyb (*error checking*)	ověřuje, zda byla data při přenosu změněna / poškozena,	Ano	Ne
Doručení dat ve správném pořadí (*same order delivery*)	dává segmenty do správného pořadí (bez ohledu na pořadí doručení)	Ano	Ne
Spolehlivé doručení (*reliable delivery*)	Znova doručeny ztracené nebo poškozené segmenty	Ano	Ne
Řízení toku dat (*flow control*)	řízení rychlosti přenosu (posuvné okénko , *sliding window*)	Ano	Ne
Velká režie (*overhead*)	Data přenášená „navíc“ k „užitečným“ „zaplaceným“ datům (*payload data*)	Ano	Ne

Identifikace jednotlivých konverzací (adresace pomocí čísel portů)

Čísla portů (16-ti bitové číslo): cílový port, zdrojový port. Porty používají protokoly TCP i UDP.

40 Všimněte si, že nespojovaný transportní protokol se používá u aplikačních protokolů, které vždy používají všesměrové vysílání.

Název skupiny portů	*Rozsah hodnot*	*Přidělováno*	*Cíl*	*Zdroj*
Dobře známé porty (*well-known*)	0 – 1023	Cíl - Pro nejprivilegovanější procesy, užité tak, že všechny stanice znají jeho správné číslo portu pro připojení na něj (na cílové straně)	X	
Registrované porty (*registered*)	1024 – 49151	Cíl, zdroj (přidělované dynamicky, nyní již nedoporučované, ale přesto používané)	X	X
Privátní (*private*) a/nebo Dynamické (*dynamic*) (také známé jako pomíjivé = *Ephemeral*)	49152 – 65535	Zdroj (dynamicky) –podle doporučení IANA		X

Aktuální seznam portů: http://www.iana.org/assignments/port-numbers

(Dobře) známé aplikace (aplikační protokoly) a jejich Čísla dobře známých portů

Číslo portu	*Protokol použitý na transportní vrstvě*	*Aplikace*
20	TCP	FTP data
21	TCP	FTP řízení přenosu
22	TCP	SSH – zabezpečené vzdálené připojení do systému
23	TCP	Telnet - emulace terminálu vzdáleného systému
25	TCP	Simple Mail Transfer Protocol (SMTP)
53	TCP, **UDP**	Domain Name System (DNS)
67	**UDP**	BootPS; server protokolu Bootstrap (je využíván protokolem DHCPv4)
68	**UDP**	BootPC; klient protokolu Bootstrap (BootP) (je využíván protokolem DHCPv4)
69	**UDP**	Trivial FTP (TFTP)
80	TCP	HTTP (pro službu WWW)
110	TCP	Poštovní protokol - Post Office Protocol version 3 (POP3)
161	**UDP**	Simple Network Management Protocol (SNMP)
443	TCP	HTTPS (http secure)
520	**UDP**	Routing Information Protocol (RIP)

Porty dle použitého transportního protokolu

Skupina portů	*TCP porty*	*UDP porty*	*TCP/UDP společné porty*
Dobře známé porty 0 -1023	• 20, 21 – FTP • 22 - SSH • 23 – Telnet • 25 – SMTP • 80 – HTTP • 110 – POP3 • 194 – Internet Relay Chat (IRC) • 443 – Secure HTTP (HTTPS)	• 69 – TFTP • 520 – RIP	• 53 – DNS • 161 – SNMP • 531 – AOL Instant Messenger, IRC
Registrované porty 1024 - 49151	• 1863 – MSN Messenger • 8008 – alternativní HTTP • 8080 – alternativní HTTP	• 1812 – RADIUS Authentication Protocol • 2000 – Cisco SCCP (VoIP) • 5004 – RTP (Voice and Video Transport Protocol)	• 1433 – MS SQL • 2948 – WAP (MMS)

Cvičení

NETSTAT - utilita pro výpis aktivních síťových spojení, statistiky rozhraní, směrovací tabulky, spojení typu NAT a členství jednotlivých rozhraní ve skupinách (IP multicast).
netstat -a, netstat -s, netstat -r, netstat -g

```
c:\>netstat -a

Aktivní připojení

  Proto  Místní adresa              Cizí adresa                Stav
  TCP    3303-33:epmap              3303-33:0                  NASLOUCHÁNÍ
  TCP    3303-33:microsoft-ds       3303-33:0                  NASLOUCHÁNÍ
  <vynecháno>
   TCP     3303-33:1048               a195-113-232-80.deploy.akamaitechnologies.com:http
NAVÁZÁNO
  <vynecháno>
  TCP    3303-33:1049               mail.spse.pilsedu.cz:4156  TIME_WAIT
  <vynecháno>
  UDP    3303-33:microsoft-ds       *:*
  UDP    3303-33:isakmp             *:*
  <vynecháno>
```

- Výpis aktivních síťových připojení
- Protokol transportní vrstvy TCP nebo UDP
- Místní adresa: zdrojová IP adresa/doménové jméno : zdrojový port (aplikační protokol)
- Vzdálená cizí adresa: cílová IP adresa / doménové jméno : cílový port (aplikační protokol)
- Stav připojení

Volba, parametr	***Popis***
-a	Zobrazí všechna spojení a naslouchající porty.
-n	Zobrazí adresy a čísla portů v numerické formě.
5 (interval)	Opakovaně vypisuje statistiku každých 5 sekund. Pro ukončení vypisování stiskněte Ctrl+C.
-p	Zobrazí spojení pro specifikované protokoly (proto), lze použít TCP, UDP, TCPv6 nebo UDPv6. Pokud je použito spolu s parametrem –s, může být protokol kterýkoliv z: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP nebo UDPv6.
-an 30	Opakovaně zobrazuje všechna spojení a naslouchající porty každých 30 sekund.
-g	Členství v IPv4 skupinách
Bez volby (No options)	Zobrazuje **pouze otevřená spojení**. Pozor na to!

Stav připojení	***Popis připojení***
LISTEN NASLOUCHÁ[41]	Lokální připojení čeká na požadavek na připojení (spojení) nějakého vzdáleného zařízení.
ESTABLISHED SPOJENO NAVÁZÁNO	Spojení je otevřeno, data mohou být vyměňována pomocí tohoto spojení. Toto je normální stav spojení ve fázi přenosu dat.
TIME-WAIT	Lokální spojení čeká implicitní časovou periodu, potom co odeslalo požadavek na ukončení, před tím než spojení uzavře. V normálním stavu bude trvat mezi 30 - 120 sekundami.
CLOSE-WAIT	Spojení je uzavřeno, ale čeká na požadavek na ukončení od lokálního uživatele.
SYN-SENT	Lokální spojení čeká na odpověď po odeslání požadavku na spojení. Spojení by mělo přejít přes tento **přechodový stav** velmi rychle.
SYN_RECEIVED	Lokální spojení čeká na požadované potvrzení spojení. Spojení by mělo přejít přes tento přechodový stav velmi rychle. Mnohonásobná spojení ve stavu SYN_RECEIVED mohou indikovat útok typu TCP SYN.

IP adresy zobrazené pomocí příkazu **netstat** spadají do několika kategorií:

41 Konkrétní český překlad závisí na konkrétní verzi a typu operačního systému.

IP Adresa	***Popis***
Místní adresa	
Local Address	*Adresa lokálního zařízení*
127.0.0.1	Tato adresa odkazuje na lokálního hostitele (*local host*, *localhost*) neboli na tento počítač. (127.0.0.1 = localhost). Síťový provoz neopustí síťovou kartu počítače.
0.0.0.0	Globální adresa znamenající „jakákoliv“.
Cizí adresa	
Foreign Address	*Adresa vzdáleného zařízení, které je připojené k tomuto počítači.*

Segmentace a opětovné složení

Rozděl a panuj (*Divide and Conquer*), to už věděli i staří Římané (latinsky: *Divide et Impera*). Ve výpočetní technice metoda nezávislého řešení dílčích podproblémů.

Některé aplikace přenášejí velké objemy dat, v některých případech mnoho gigabajtů. Bylo by nepraktické všechna tato data v jednom velkém kusu. Žádný jiný síťový provoz by nemohl být přenášen dokud by byla vysílána tato data. Navíc, pokud by došlo k jakékoliv chybě, byla by ztracena všechna data a musela by být odvysílána znovu. Síťová zařízení nemají se tak velkou vyrovnávací paměť, aby mohly tato data ukládat během vysílání nebe příjmu. Omezení se mění v závislosti na použité síťové technologii nebo konkrétním přenosovém médiu.

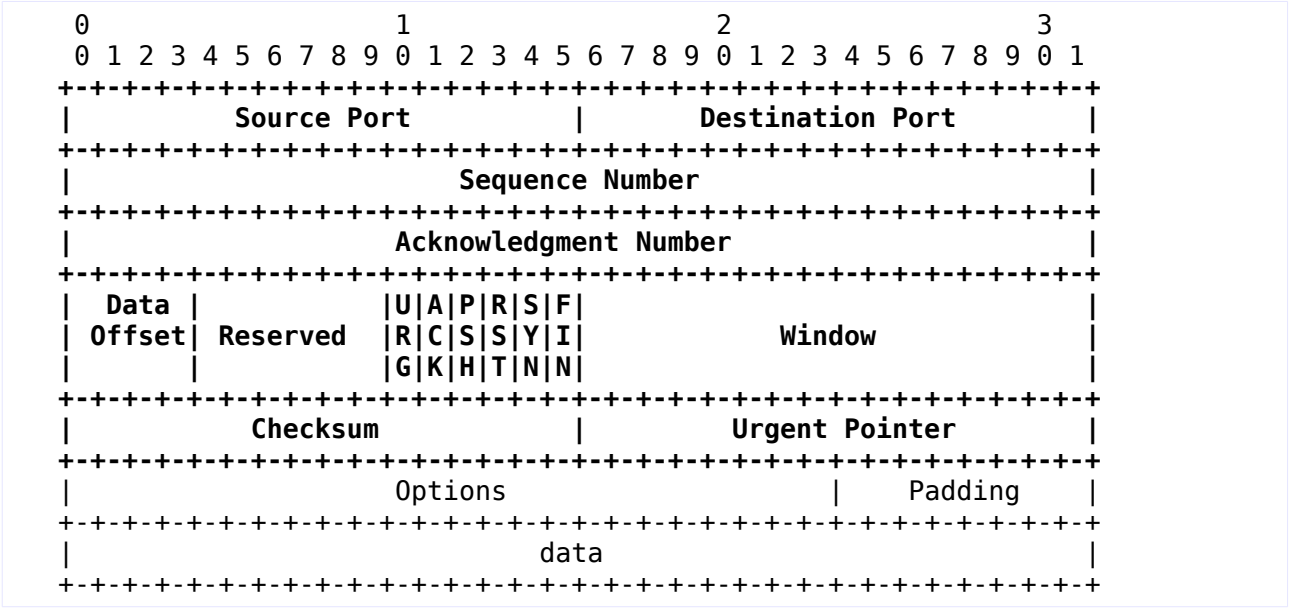
Rozdělení aplikačních dat do kousků zajistí, že jsou jednak data přenášena v rámci omezení příslušného přenosového média a jednak, že mohou být data z různých aplikací střídavě prokládána na toto sdílené médium (multiplexing).

TCP a UDP pracují se segmentací rozdílně.

V TCP záhlaví každého segmentu obsahuje pořadové číslo (*sequence number*). To pořadové číslo umožní na cílovém hostiteli znovu složit data do pořadí, v jakém byla odvysílána. Cílová aplikace má data v přesně takovém tvaru jak zamýšlel odesílatel.

Ačkoliv UDP také zajistí doručení mezi aplikacemi, nezajišťuje pořadí, ve kterém jsou informace vysílány ani neudržuje spojení. V záhlaví UDP není číslo pořadí. UDP je jednodušší protokol s menší režií a rychlejším přenosem dat. Informace ale mohou přijít jiném pořadí, protože jednotlivé pakety mohou jít jinou cestou v síti. Aplikace, používající UDP, tento fakt musí tolerovat.

TCP Segment



Pole	***Bitů***	***Popis***
Source Port	16	Vysílající (zdrojový) port, přiřazená první volná hodnota vyšší než 1023.
Destination Port	16	Přijímající (cílový) port, určuje aplikaci, proces nebo protokol vyšší vrstvy na vzdáleném hostiteli.
Sequence Number	32	Sleduje přenos bajtů. Pořadové číslo prvního bajtu aplikačních dat zapouzdřených v segmentu.
Acknowledgment Number	32	Potvrzuje přenos bajtů. Obsahuje pořadové číslo prvního bajtu očekávaných aplikačních dat v dalším segmentu. Dopředné (pozitivní, optimistické) potvrzování.
Data Offset (Header Length)	4	Počet 32-bitových slov v hlavičce. Délka hlavičky.
Reserved	6 - 2	Rezervováno - pro budoucí použití. Nastaveno na hodnotu 0.
Flags	6 + 2	Návěští (příznaky) – určuje správu relace a způsob zacházení se segmentem. *Synchronization* (**SYN**) – **synchronizace** – požadavek na synchronizaci – vytvoření relace před vlastním přenosem aplikačních dat, *Acknowledgement* (**ACK**) – **potvrzení** přijatých dat (číslo příštího očekávaného bajtu), *Finish* (**FIN**) – **ukončení** spojení, *Push* (PSH) - , *Urgent* (URG) – urgentní – prioritní, *Reset* (RST) – reset spojení.

		CWR – Congestion Window Reduced (CWR) nastaveno vysílajícím hostitelem, aby indikovalo, že byl přijat segment s nastaveným ECE (přidáno do hlavičky - RFC 3168). ECE - ECN-Echo – indikuje, že TCP má schopnost ECN během třícestného navázání spojení (přidáno do hlavičky - RFC 3168).
Window Size	16	Kolik bajtů je posíláno na jedno potvrzení (ale může být ve více segmentech). Velikost vstupní vyrovnávací paměti.
Checksum	16	Kontrolní součet za záhlaví a aplikační data. Vysílač generuje a přijímač kontroluje, aby viděl zda nebyly **hlavička a data z vyšší (aplikační) vrstvy** změněny nebo poškozeny během přenosu.
Urgent Pointer	16	Ukazuje na první bajt prioritních dat, tak jako Ctrl+Z značí konec prioritních dat. Použité pouze společně s návěštím URG.
Options	32	Volby musí být dorovnány do délky 32-bitů. Doplnění prázdných znak do této délky to zaručí.
Data	Násobky 32 bitů	Informace z vyšších vrstev.

Zdroj: RFC 793 http://www.ietf.org/rfc/rfc793.txt .

Cvičení

PacketTracer: otevření HTML stránky z WWW serveru www.seznam.cz (nastavte DNS). Prozkoumat obsah prvních segmentů TCP (pro http) a UDP (pro DNS).

Wireshark: Totéž v reálném provozu odposlechnout pomocí „čmuchacího“ programu (*sniffer*).

Navázání a ukončení spojení v TCP

Třícestné navázání spojení (*Three Ways Handshaking*):

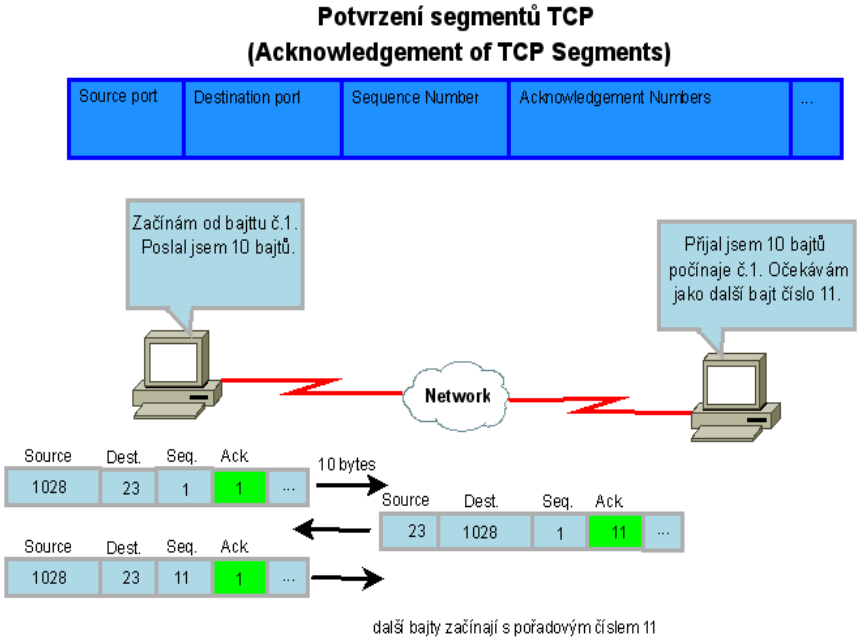
- -> TCP port zdroje (dynamicky přidělený) 1048 > port cíle (dobře známý) 80, Flags=SYN, seq = (x+)0 (relativní), windows size = 65536, (header) len = 0 (odchylka od standardní délky 28 bajtů), MSS (*Maximal Segment Size*) = 1460
- <- TCP 80 > 1048, Flags= SYN,ACK, seq = (y+)0, ack = (x+)1, windows size=5840, len =0, MSS=1460
- -> TCP 1048 > 80, Flags = ACK, seq = (x+)1, ack = (y+)1, windows size 65536, len =0

Tři kroky „třícestného“ navázání spojení (vytvoření relace) v TCP (v těchto 3 segmentech nejsou přenášená žádná „užitečná“ (= aplikační) data a slouží pouze pro vytvoření relace mezi koncovými aplikacemi):

1. Iniciující klient odesílá segment s návěstím SYN (synchronizuj čísla pořadí) obsahující počáteční (synchronizační) hodnotu čísla pořadí - *Initial Sequence Number* (ISN) (ta je pseudonáhodná vygenerovaná ze systémového času a slouží ke sledování toku dat ve vytvořené relaci, je to 32-bitové číslo – při „čmuchání“ ve WireSharku je toto číslo zobrazováno s relativní hodnotou 0). Zdrojový port je přiřazen jako první volný z rozsahu registrovaných portů

nebo u nových aplikací z rozsahu privátních portů. Cílový port je určen portem aplikačního protokolu. Tento segment slouží jako požadavek na server, aby se otevřelo sezení (relace).

2. Server odpovídá segmentem s návěštím SYN a ACK (synchronizace a platná odpověď = potvrzení), který obsahuje číslo potvrzení rovné přijatému číslu pořadí plus jedna (+ 1) = žádná přenesená data a navíc vlastní pseudonáhodnou hodnotu čísla pořadí. Hodnota čísla potvrzení je o jedničku větší protože zde nejsou žádná data, která by byla potvrzována (v analyzátoru síťových protokolů je zobrazena opět relativně jako 1). Tomuto potvrzení o jedničku většímu (říká mi, číslo pořadí segmentu, který očekávám, že příště přijmu) se říká **dopředné potvrzování** (někdy se také říká optimistické, pozitivní potvrzování). Případně nepotvrzené segmenty jsou odvysílány znovu. Celému tomuto mechanismu se říká **dopředné potvrzování a opětovné poslání** (*Positive Acknowledgment and Retransmission (PAR)*). Proti iniciujícímu segmentu je zdrojový a cílový port v segmentu odpovědi vzájemně přehozen. Hodnota čísla potvrzení svazuje odpověď s původním požadavkem posílaným na server.
3. Iniciující klient odpovídá s návěštím ACK a s číslem potvrzení o jedničku větším než bylo přijaté číslo pořadí ze serveru. V segmentu nejsou žádná uživatelská data. Čísla portů jsou stejná jako v kroku jedna. To dokončuje vytvoření relace (sezení, spojení).



Ukončení (obsahuje čtyři transakce):

- -> Flags=FIN, SEQ = x
- <- Flags=ACK; ACK = x + 1,
- <- Flags=FIN, ACK; SEQ = y, ACK = x + 1
- -> Flags=ACK, ACK = y+1

Uzavření relace je na čtyři kroky (FIN, ACK, FIN+ACK, ACK).

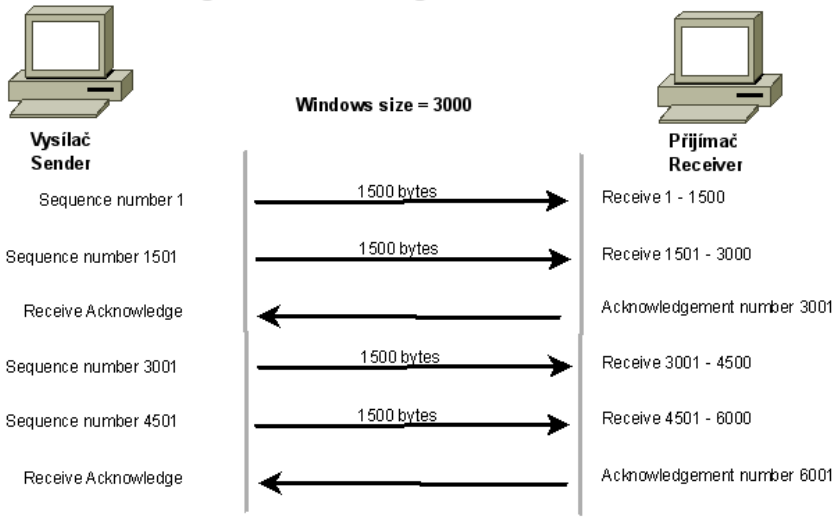
Řízení toku dat, správa zahlcení

Pokud mohou například k serveru nějaké služby neomezeně přistupovat klienti, může dojít na straně

serveru k jeho zahlcení (*congestion*) – server není schopen odpovídat a je třeba mu odlehčit. Podobně v důsledku nespolehlivosti linek se mohou některé segmenty na cestě „ztratit“ nebo mít příliš velké zpoždění a je vhodné data z vyšší vrstvy potvrzovat po menších blocích dat – tj řídit tok dat (*data flow control*). To se řeší mechanismem posuvného okénka (*sliding window*). Velikost okénka (*window size*) = množství přenesených dat (v bajtech) na jedno potvrzení (než vysílající strana začne čekat na potvrzení vyslaných dat jako přijatých ze strany příjemce).
Příklad komunikace (již po navázání spojení a synchronizaci – po vytvoření relace) přenos dat jedním směrem:
Řekněme, že velikost okénka je 3000 bajtů a do jednoho segmentu se vejde maximálně 1500 bajtů dat (zapouzdřený paket má velikost 1500 bajtů). Počáteční sekvenční číslo je relativní = 1.
První segment, SEQ=1, ACK=1, přeneseno 1500 bajtů
Druhý segment, SEQ=1501, ACK = 1, přeneseno 1500 bajtů,
Po přenesení 3000 bajtů (velikost okénka) je posláno potvrzení s číslem očekávaného bajtu ACK=3001. SEQ=1.
Třetí segment, SEQ=3001, ACK=1, přeneseno 1500 bajtů
Čtvrtý segment, SEQ=4501, ACK=1, přeneseno 1500 bajtů,
Po přenesení 3000 bajtů (velikost okénka) je posláno potvrzení s číslem očekávaného bajtu ACK=6001. SEQ=1 to znamená, že při potvrzování nejsou přenášena žádná data (rozuměj zapouzdřená z vyšší vrstvy) – slouží pouze pro potvrzení dat přijatých „z druhé strany“.

Potvrzení segmentu TCP a velikost okénka

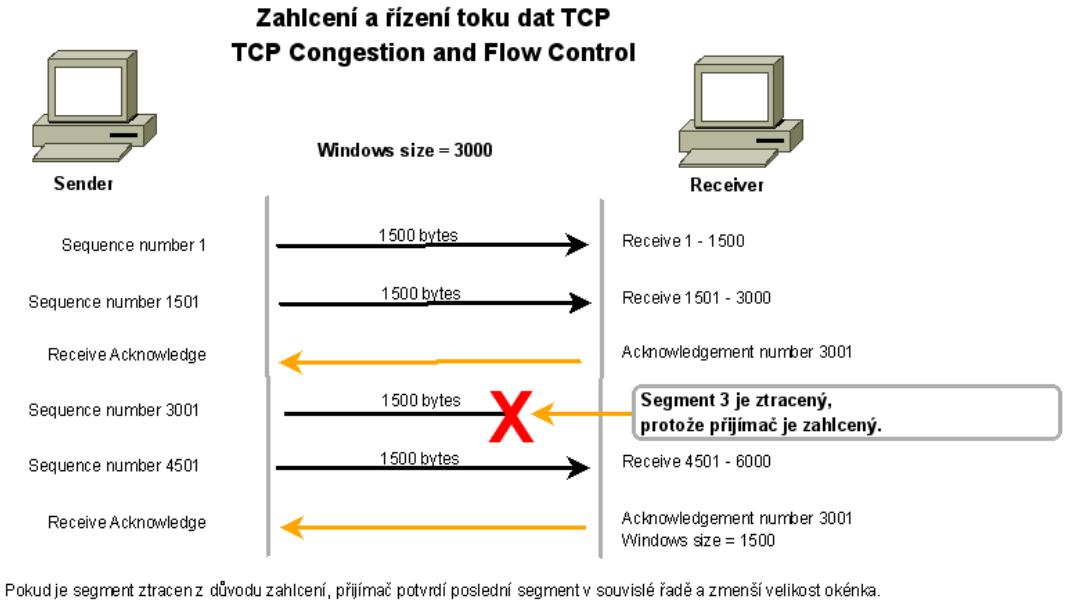
TCP Segment Acknowledgement and Windows Size



Velikost okénka (windows size) určuje počet bajtů před tím, než je očekáváno potvrzení.
Číslo potvrzení (acknowledgement number) je číslo následujícího očekávaného bajtu.

Nyní si představíme situaci, že třetí segment v předchozím případě **nedorazil do cíle v předem stanoveném čase nebo nemá správný kontrolní součet**. Potom se systém vrátí k poslednímu číslu potvrzení ACK (= 3001) a odvysílá znovu (od SEQ=3001) se zmenšenou velikostí okénka například na polovinu původní hodnoty.
V příštím přenosu budou data přenesena, dejme tomu, v pořádku a TCP hned zvětší velikost okénka. Protože se velikost okénka během přenosu dat neustále zvětšuje a zmenšuje, říká se tomuto mechanismu **posuvné (klouzající) okénko (*sliding window*)**.
Pokud není přijato potvrzení do předem dané doby, data jsou automaticky vysílající stranou znova

vyslána od sekvenčního čísla daného hodnotou posledního potvrzení ze strany příjemce.



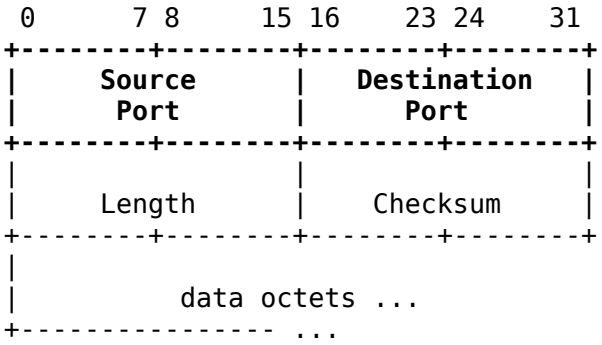
Pokud je segment ztracen z důvodu zahlcení, přijímač potvrdí poslední segment v souvislé řadě a zmenší velikost okénka.

Aplikační protokoly používající TCP

Spolehlivý přenos za cenu vyšší režie.

- FTP, SSH, , Telnet, SMTP, POP3, Internet Relay Chat (IRC), MSN Messenger, atd.

UDP Datagram



Pole	***Bitů***	***Popis***
Source Port	16	Vysílající (zdrojový) port
Destination Port	16	Přijímající (cílový) port
UDP Length	16	Délka: Data + hlavička
Checksum	16	Volitelné – Kontrolní součet (CRC) **záhlaví i dat** – pokud je 0, tak se nepočítá
Data	**Různě**	Informace z vyšších vrstev

Zdroj: RFC 768 http://www.ietf.org/rfc/rfc768.txt .

Poznámka

Datagramem rozumíme **nepotvrzovanou PDU**.

Aplikační protokoly používající UDP

Pro rychlý přenos s malou režií:

- Domain Name System (DNS) , Simple Network Management Protocol (SNMP) , Dynamic Host Configuration Protocol (DHCP) , Routing Information Protocol (RIP) , Trivial File Transfer Protocol (TFTP) , online hry, kontinuální video, VoIP, atd.

Poznámka

Způsob zabezpečení datové sítě (**firewall typu SPI** - *Stateful Packet Inspection* – stavová inspekce paketů):

- Potlačení vytváření libovolných relací TCP
- Vytváření relací je povoleno pouze pro určité předem definované služby
- Síťový provoz je povolen pouze jako součást již vytvořených relací (dovnitř sítě propuštěny pouze odpovědi na provoz zevnitř).
- Tím zabráníte vstupu potenciálně škodlivých transakcí do vaší sítě (např. Ping smrti, který se tváří jako ICMP *echo reply* na váš požadavek ICMP *echo request*).

Cvičení

Změna velikosti posuvného okénka a potvrzování při přenosu souboru během komunikace TCP:

1. spusťte odposlech ve WireShark,
2. v příkazové řádce operačního systému ze školního ftp serveru (jonatan.spse.pilsedu.cz, uživatel ftp, prázdné heslo) stáhněte větší soubor na lokální disk,
3. zjistěte přenosovou rychlost (v promptu (příkazové řádce) klienta FTP),
4. prozkoumejte změny velikosti posuvného okénka během přenosu (na nezatíženém lokálním serveru nebudou velké),
5. podívejte se, jak jsou data - přenášené jedním směrem – potvrzována (ACK=1),
6. Určete, zda se jedná o FTP přenosový režim aktivní či pasivní (dle čísel portů, pasivní nepoužívá port 20).

7. Stáhnutý soubor potom nezapomeňte smazat z lokálního disku!

Kontrolní opakovací otázky a odpovědi (kvíz):

1) K jednotlivým protokolům přiřaďte správná čísla portů:
   a) HTTP: 80 (nebo alternativní číslo 8080),
   b) Telnet: 23,
   c) FTP: v aktivním režimu 20 a 21, v pasivním režimu 21 a dynamicky přidělovaný.
   d) SMTP: 25,
   e) POP3: 110.
2) K jednotlivým protokolům přiřaďte jejich charakteristiky:
   a) UDP:
      i. nespolehlivý (ve smyslu malé režie či nepotvrzování a zaručení doručení),
      ii. nespojově orientovaný,
      iii. bez řízení toku dat,
      iv. přijatou zprávu neseřazuje do správného pořadí.
   b) TCP:
      i. spolehlivý,
      ii. spojově orientovaný,
      iii. na přijímajícím cílovém hostiteli zprávu seřadí do původního pořadí,
      iv. vše, co není doručeno (přijato na cíli) je odvysíláno znovu.
3) Jaký způsob řízení na transportní vrstvě je použit k předcházení přetečení (*overflowing*) vyrovnávací paměti přijímajícího hostitele?
   a) Řízení toku dat (*flow control*) – pomocí řízení velikosti posuvného okénka (*sliding window size*) v protokolu TCP.
4) Koncové systémy používají čísla portů k tomu, aby vybraly odpovídající aplikaci (protokol). Jaké je nejmenší číslo portu, které může být dynamicky přiřazeno hostitelským systémem?
   a) 1024.
5) Co je hlavní odpovědností přijímajícího hostitele během spolehlivého datového přenosu? (2 odpovědi)
   a) potvrzování přijetí,
   b) znovu složení do původního pořadí (*reassembly*).
6) Na které vrstvě modelu TCP/IP pracuje protokol TCP?
   a) Transportní.
7) Co určuje, kolik dat může vysílající stanice s protokolem TCP vyslat před tím, než očekává potvrzení?

a) Velikost okénka (*window size*).

8) Jaký je účel pořadového čísla (*sequence number*) v záhlaví protokolu TCP?
   a) Opětovné složení segmentů do původních dat
9) Jaký je účel čísel portů u protokolů TCP a UDP?
   a) Odlišení jednotlivých simultánních konverzací v síti (mezi správnými procesy).

Kapitola 5 - Síťová vrstva OSI

V této kapitole se naučíme:

- Identifikovat roli síťové vrstvy, jak popisuje komunikaci z jednoho koncového síťového zařízení na druhé koncové zařízení.
- Prozkoumat nejběžnější protokol síťové vrstvy Internet Protocol (IP) a jeho funkce pro poskytování nespojované služby „dělám co mohu“ (*best-effort service*).
- Pochopit principy použité k rozdělování nebo seskupování zařízení do jednotlivých sítí.
- Pochopit hierarchické adresování síťových zařízení a jak to umožňuje komunikaci mezi sítěmi.
- Rozumět základům cest, směrů (*routes*), adresám následujícího přeskoku (*next-hop addresses*) a posílání paketů (*packet forwarding*) do cílové sítě (*destination network*).

Shrnutí

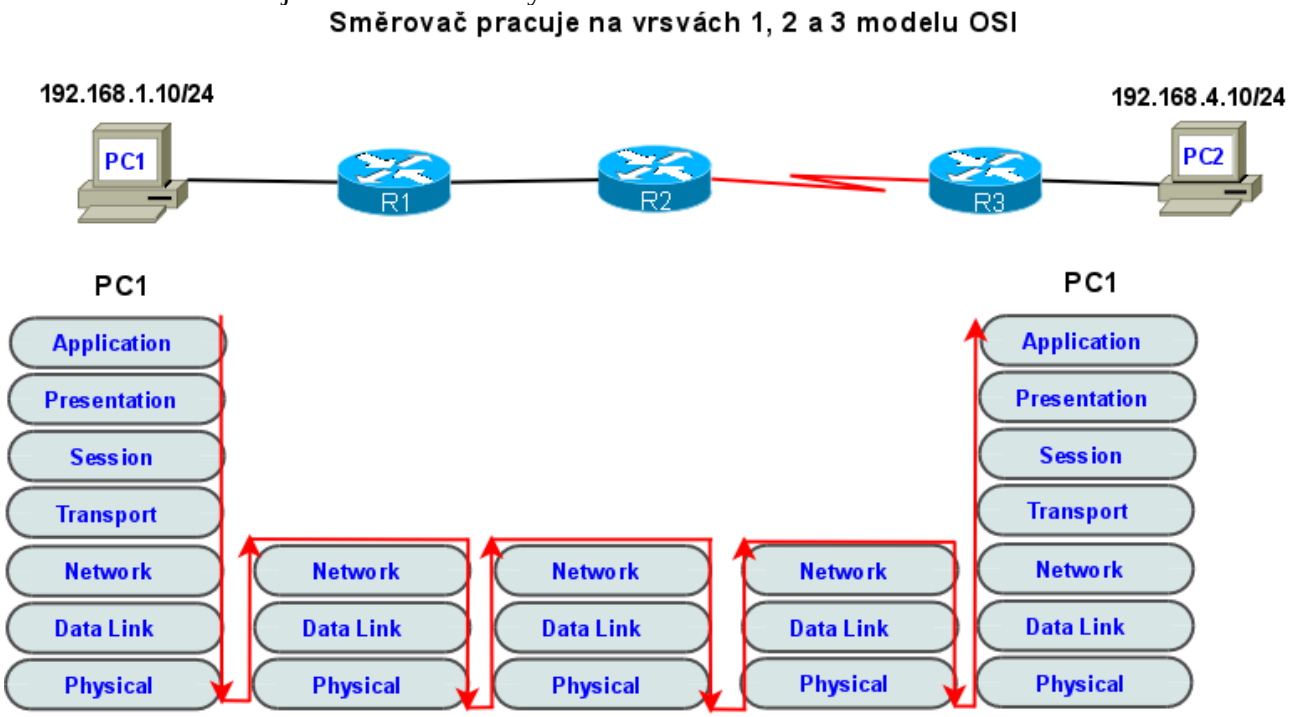
- Síťová vrstva **poskytuje své služby transportní vrstvě**.
  - Transportní vrstva slouží k propojování procesů (aplikací), když už data byla síťovou vrstvou dopravena na příslušná zařízení v síti (hostitele).
  - Data z transportní vrstvy jsou zapouzdřena do paketu (datagramu) na síťové vrstvě.
- **Síťová vrstva slouží k propojení – komunikaci - hostitelů – uzlů – zařízení v síti**.
- **Logické IP adresy** mají hierarchickou strukturu a jsou unikátní pro každé (koncové) zařízení v síti[42]. V sítích IPv4 je potom zařízení s přidělenou IP adresou nazýváno **hostitel** (*host*). Každý hostitel má ve své IP adrese obsaženu adresu sítě, ve které leží (= síťová část IP adresy).
- Zapouzdření segmentů do paketů na síťové vrstvě slouží k dopravě dat ze zdrojového do cílového síťového zařízení **s minimální režií**.
- Zapouzdření na L3 obsahuje mimo jiné **zdrojovou a cílovou IP adresu**.
- Hostitelé jsou rozděleni do **skupin (podle IP adres) = sítí**.
- Jednotlivé sítě jsou vzájemně **propojeny (nebo také odděleny) směrovači (routery)** – ty se také někdy nazývají **mezilehlé systémy (*intermediary system*)**
  - účelem – hlavní činností - routeru je **směrovat** (vybrat nejlepší cestu a znovu zabalit a přepnout paket zapouzdřený v rámci) – poslat data směrem k cíli).
  - směrovač pracuje na vrstvách L1, L2 a L3, protože nejvyšší vrstva na které pracuje je L3, říká se proto, že je to L3 zařízení.
- Výběru nejlepší cesty (*path*) (směru, trasy, *route*) a přeposílání paketu mezi sítěmi se říká **směrování (*routing*)**.
- Nejběžnější protokol na síťové vrstvě je **IP (*Internet Protocol*)**.
- Protokol síťové vrstvy definuje strukturu **paketu** a postup použitý k **přenosu dat z jednoho hostitele (*host*) do druhého hostitele (v jiné síti)**.

Čtyři základní činnosti na síťové (L3 OSI) vrstvě

1. **adresování** (*Addressing*) – použita logická IP adresa, když je IP adresa přidělena síťovému zařízení, toto zařízení se potom nazývá hostitel (*host*),

42 Pokud je IP adresa veřejná, je unikátní v celém internetu, pokud je adresa neveřejná, je unikátní v příslušné neveřejné síti. (Budeme brát později.)

2. **zapouzdřování** (*Encapsulation*) – data zapouzdřená v paketu, v záhlaví paketu musí být, mimo jiné cílová adresa (*destination address*) a zdrojová adresa (*source address*),
3. **směrování** (*Routing*) – vyhledání nejlepší cesty z jedné sítě do jiné cílové sítě a odeslání paketu směrem k cíli,
4. **odpouzdřování** (*Decapsulation*) – v paketu je zapouzdřen obsah z vrstvy L4, který umožňuje přenášet vícenásobné, paralelní, komunikace mezi hostiteli. Samotné doručení dat mezi hostiteli je věcí síťové vrstvy.



Protokoly na síťové vrstvě

V této chvíli nás zajímají takzvané **směrované protokoly** (*routed protocols*) (jsou v nich zapouzdřená aplikační data dopravovaná sítí):

- ***Internet Protocol version 4 (IPv4),***
- ***Internet Protocol version 6 (IPv6),***
- *Novell Internetwork Packet Exchange (IPX),*
- *AppleTalk,*
- *Connectionless Network Service (CLNS/DECNet)*

IP verze 4 a 6 jsou nejrozšířenější a budeme se věnovat hlavně jim. Diskuse ostatních protokolů bude minimální.

Základní charakteristiky IPv4

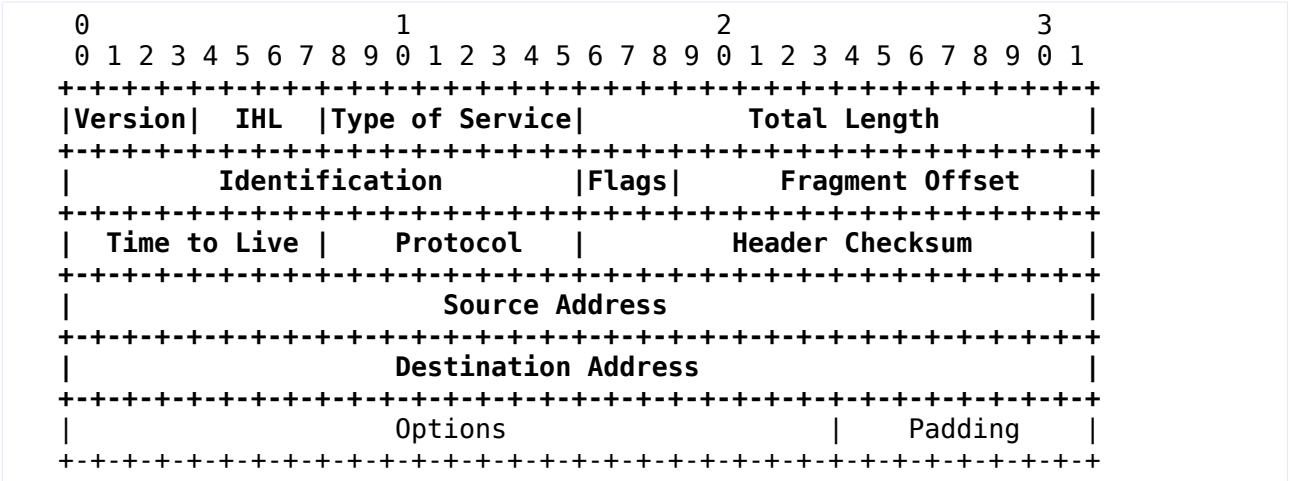
V současnosti je protokol Internet Protocol version 4 IPv4 nejpoužívanějším protokolem pro přenos dat prostřednictvím Internetu. Protokol IPv6 může fungovat paralelně s IPv4 a v budoucnu ho nahradí. IP protokol byl navržen jako protokol s nízkou režií. Má pouze takové funkce, které jsou nutné k doručení paketu ze zdroje do cíle přes vzájemně propojený systém sítí. Tento protokol není

navržen pro sledování (*track*) a správu toku paketů. Tyto funkce provádějí jiné protokoly na jiných vrstvách.

Základní charakteristiky IPv4:

- **Nespojovaný** (*Connectionless*) – není vytvářeno spojení (relace, sezení) před odesláním datových paketů => odesílatel neví: zda je přítomen příjemce, zda paket dorazil, zda příjemce mohl číst paket a příjemce zase neví kdy paket dorazí.
- **Nespolehlivý** (*Unreliable*) používá systém tzv **Nejlepší snaha** (*Best Effort*) to znamená, že žádná režie není použita pro zajištění doručení paketu => pojem „nespolehlivý“ (v datových sítích) jednoduše znamená, že
  - Paket je odeslán a:
    - Odesílatel neví: zda je příjemce přítomen, zda data došla, zda je příjemce může číst.
    - Příjemce neví: kdy data dorazí (zda má právě nějaká očekávat).
  - IP nemá žádnou schopnost řídit zotavení po nedoručení nebo po poškození paketů.
  - IP nezaručuje, že odeslaná data budou skutečně přijata, data se mohou po cestě ztratit (a směrovače na trase to neřeší).
  - Není žádné sledování cesty paketu a kontrola eventuální chyby. Ani možnost znovu odeslání.
  - Protože spolehlivost lze ale zařídit na vyšších vrstvách, může potom IP protokol pracovat **velmi efektivně a rychle**.
- **Nezávislý na médiu** (*Media Independent*) – pracuje nezávisle na médiu přenášejícím data.
  - Přesto, ale existuje charakteristika média, kterou je třeba brát v úvahu na síťové vrstvě a totiž maximální velkost PDU v bajtech, které může konkrétní médium přenášet - **Maximum Transmission Unit (MTU)**[43]. Z tohoto důvodu potom router někdy musí při přechodu na médium s nižším MTU paket rozdělit do menších kusů = fragmentů, to se nazývá **fragmentace**.

IPv4 paket - záhlaví



43 Například: Ethernet má MTU=1500 bajtů, Token Ring má MTU větší, PPP menší než Ethernet.

Pole	***Bitů***	***Popis***
Version	4	Verze protokolu IP - má vždy hodnotu 4
Internet Header Length (IHL)	4	Délka záhlaví / hlavičky - počet 32-bitových slov, max=15
Type of Service, ToS	8	Typ služby pro QoS (kvalitu služby) - pokud není toto pole používáno, je jeho hodnota 0, definuje jak má směrovač s paketem zacházet z hlediska **priorit** (precendence) a specifických kritérií v rámci kvality služby: zpoždění (delay), propustnost (throughput), spolehlivost (reliability) a cena (cost)) – **prakticky se nepoužívá**
Total Length	16	Celková délka datagramu (paketu) v oktetech, max=65535, délka je vždy násobkem 32 bitů
Identification	16	Identifikace – odkaz na původní paket před fragmentací (fragmentace paketu - z důvodu zavedených maximálních délek rámců (MTU) v různých síťových technologiích)
Flags	3	Příznaky, Návěsti – zda je nebo není paket fragmentován ● první bit zleva je vždy nulový – někdy se uvádí i **aprílové RFC**, kde byl tento bit (**„evil bit“**) použit pro označení „zlých paketů“ - určených pro nelegální činnosti v síti :-)) ● druhý bit = **DF (Do not fragment)**, pokud = 1, není fragmentování povoleno, ● třetí bit = **MF (More fragments follow)**, pokud = 1 následuje fragmentovaný paket (a je použit offset pro umístění fragmentu na správné místu v původním paketu), pokud = 0 další fragment už nenásleduje.
Fragment Offset	13	Odstup fragmentu – relativní posunutí vzhledem k začátku původního fragmentovaného paketu (dělené 8B=64 bity), jednoznačně určuje pořadí fragmentu v původním datagramu
Time to Live – TTL	8	Životnost - (zbývající) doba platnosti (života) paketu v hopech (maximálním počtu přeskoků, maximálním počtu směrovačů na cestě) – slouží k vyloučení nekonečného bloudění paketů v síti, **na každém směrovači se snižuje o jedničku, když dosáhne hodnoty 0, paket se již dál neposílá a na routeru se produkuje zpráva ICMP (Time-To-Live Exceeded)** Tím se předchází vzniku tzv. **Směrovacích smyček (routing loops)**, které zbytečně zatěžují provoz směrovačů. (Směrovací smyčka vznikne nesprávným obsahem směrovací tabulky směrovače.)
Protocol	8	Protokol, číslo protokolu – zapouzdřený protokol vyšší vrstvy v paketu ● **ICMP = 1**, ● IGMP = 2, ● **TCP = 6,** ● **UDP = 17**, ● EIGRP = 88, ● OSPF = 89 http://www.iana.org/assignments/protocol-numbers
Header Checksum	16	**Kontrolní součet záhlaví** / hlavičky (pro výpočet se nastaví hodnota kontrolního součtu na 0), pouze záhlaví a **nikoliv dat**
Source Address	32	Zdrojová IP adresa – adresa odesílajícího počítače (platná je pouze unicastová adresa)
Destination Address	32	Unicat, Broadcast nebo Multicast
Options	X	Volby (pokud jsou nějaké) – např. Zabezpečení – obvykle se nepoužívá
Padding	32 - X	Výplň - dorovnání voleb do 32 bitů

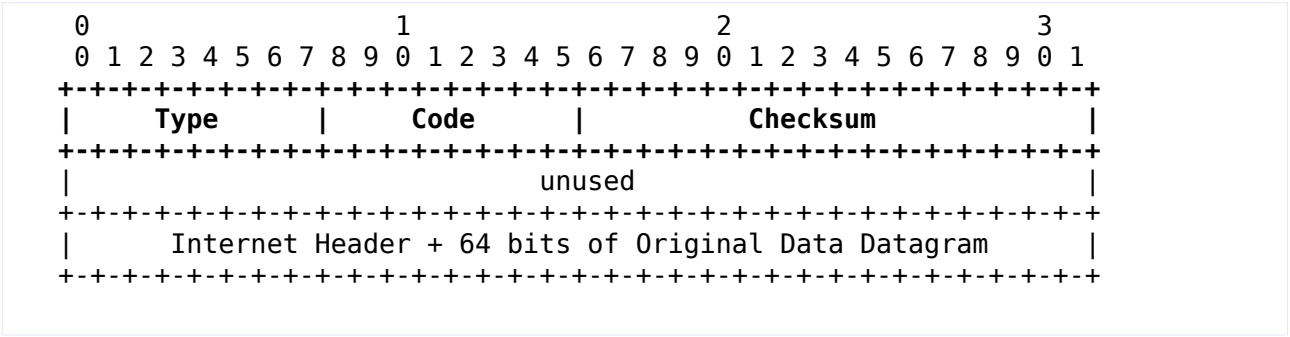
Zdroj: RFC 791 http://www.ietf.org/rfc/rfc0791.txt .

Zde se budeme zabývat hlavně těmito šesti poli:

- Zdrojová IP adrese (IP Source Address),
- Cílová IP adresa (IP Destination Address),
- Životnost (Time-to-Live (TTL)),
- Typ služby (Type-of-Service (ToS)),
- Číslo protokolu (Protocol),
- Odstup fragmentu (Fragment Offset).

ICMP zpráva

Internet Control Message Protocol (ICMP) – **protokol řídících zpráv Internetu**. Pracuje na síťové vrstvě a je přímo zapouzdřen v IP paketu (jako přenášená data).
Struktura zprávy je závislá na obsahu zprávy (typu zprávy):



Vždy obsahuje pole:

Pole	***Bitů***	***Popis***
Type	8	Typ zprávy – určuje typ zprávy
Code	8	Kód – návratový kód zprávy – specifické pro konkrétní kód zprávy
Checksum	16	Kontrolní součet pouze záhlaví
...		Další pole jsou závislá na typu zprávy.

Obsah polí protokolu ICMP (*ICMP Fields*) závisí na typu zprávy (*Type*), ke kterému patří určitý návratový kód (*Code*).

Příklady vybraných typů zpráv a jejich návratových kódů:

Type: 8 - žádost o odpověď (*echo request message*),
Type: 0 - odpověď na žádost (*echo reply message*)
Code: vždy je 0

Type: 3 - cíl je nedostupný (*Destination Unreachable Message*)
Code:

- 0 = síť nedostupná (*net unreachable*),
- 1 = hostitel nedostupný (*host unreachable*),
- 2 = protokol nedostupný (*protocol unreachable*)
- 3 = port nedostupný (*port unreachable*),

- 4 = potřebná fragmentace a DF nastaven (*fragmentation needed and DF set*)
- 5 = zdrojový směr selhal (*source route failed*).

Type: 11 – překročena doba (*Time Exceeded Message*)
Code:

- 0 = životnost překročena během přenosu (*time to live exceeded in transit*),
- 1 = překročena doba pro opětovné složení fragmentu (*fragment reassembly time exceeded*).

Další viz RFC.
Zdroj: RFC 792 http://www.ietf.org/rfc/rfc792.txt

Příkaz Ping

Zjišťuje dostupnost uzlu v síti (hostitele) z uzlu, na kterém se spustí.
Používá dvě zprávy ICMP:

- zpráva požadavek na odpověď *echo request* (typ zprávy = 8)
- odpověď na tento požadavek *echo reply* (typ zprávy = 0).[44]

Parametry:
-t neomezený počet ICMP zpráv za sebou
-i n nastavení TTL na hodnotu n (n je přirozené číslo)

Příkaz Tracert

Zjišťuje cestu (trasuje cestu, *trace route*) do uzlu v síti (hostitele) z uzlu, na kterém se spustí.

Ve Windows **tracert** používá protokol ICMP Nejprve s vyšle zpráva ICMP požadavek na odpověď (echo request), zapouzdřená v IP paketu s životností TTL = 1. Na prvním směrovači je TTL zmenšeno o 1 a nabývá hodnoty TTL = 0. Tím už takový paket není možno poslat dál a dochází k chybě. O této chybě je zdroji (odesílateli) zaslána zpráva o vypršení životnosti (*TTL exceeded*) a je možné vypsat první směrovač na cestě k cíli. Dále se pokračuje stejným způsobem pouze je ICMP zpráva zapouzdřena v paketu s TTL = 2. Tím „vytiká“ na druhém směrovači. Atd.

V Linuxu je pro tento účel použito UDP segmentu určeným na „nepravděpodobný“ port > 30000 (na zapouzdřeném IP paketu postupně nastavováno TTL= 1, 2, ...). I v Linux lze ale vynutit použití protokolu ICMP (parametr příkazu **traceroute -I**).

Cvičení

Odposlech ve WireShark provozu **zpráv protokolu ICMP** pro utility **ping** a **traceroute**.
Ping: je utilita využívající dvě zprávy: ICMP echo request, ICMP echo reply
Zároveň kontrolujte **obsah IP paketu.** U traceroute vzhledem k položce TTL – IP paket má postupně se zvětšující TTL od 1 do počtu routerů na cestě do cíle, klasický traceroute má navíc tento počet maximální TTL omezen hodnotou 30. Pole TTL potlačuje (zkracuje) směrovací smyčky vzniklé nesprávným obsahem směrovací tabulky.

- Vypište ping na určitou adresu s parametrem -i 1 a potom 2 atd.
- Porovnejte tento výstup s výstupem tracert.

44 Výpis příkazu ping a tracert je v kapitole 2.

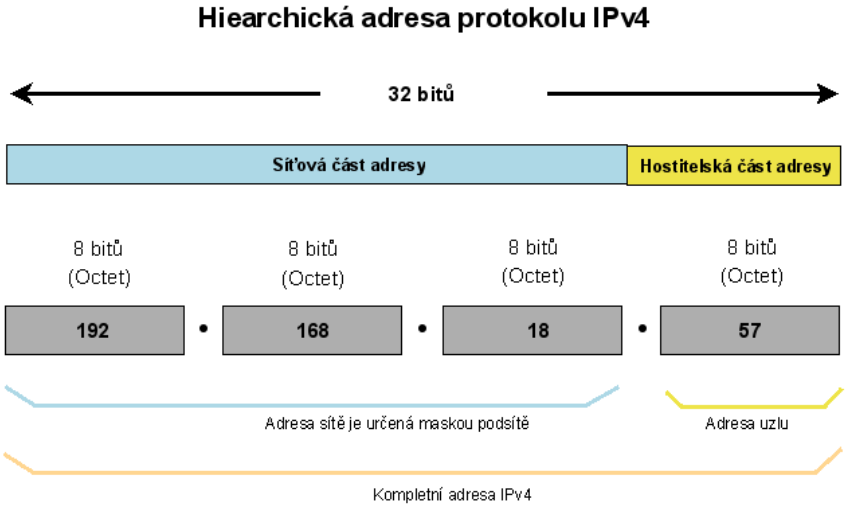
Sítě – rozdělení hostitelů do skupin

Sítě se vytvářejí na základě (podle):

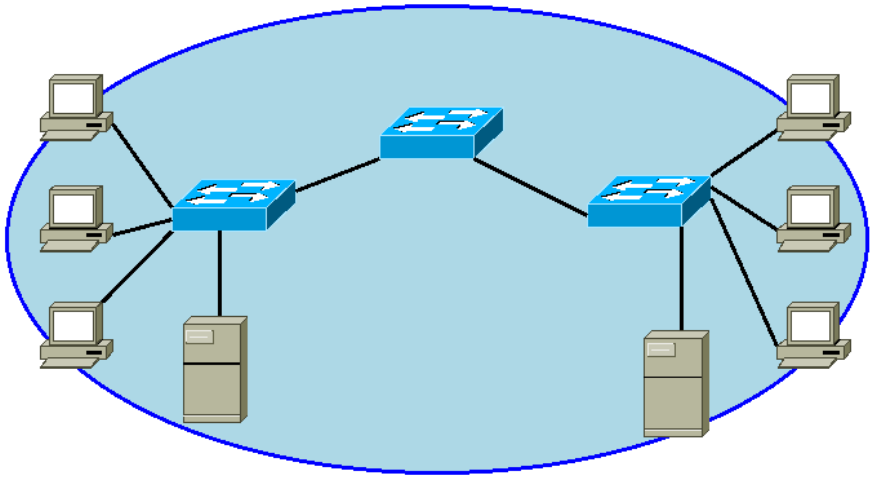
- geografického umístění (místností, pater budovy, oddělených budov, ...),
- specifického účelu (vývoj grafických aplikací – síť s velkým datovým provozem je vhodné oddělit od ostatních, ...),
- vlastnictví (odděleno z důvodu zabezpečení a odpovědnosti za síť, ...).

Proč se sítě dále rozdělují do menších (podsítí = *subnet*)?
Snažíme se **zmenšit obvyklé problémy rozsáhlých sítí:**

- **Pokles výkonnosti** (*Performance degradation*) - obecně platí: jedna síť je jedna **broadcastová doména**, nesměrové (všesměrové) vysílání zbytečně zatěžuje (*burden*) systémové zdroje, proto se broadcastovou doménu snažíme zmenšit (a snížit tak celkovou režii sítě), východ z jedné sítě se nazývá **brána (*gateway*)** => náhrada přepínače (*switch*) směrovačem (*router*). Směrovač segmentuje broadcastovou doménu,
- Problémy se **zabezpečením** (*Security issues*) => na směrovačích je možné realizovat **firewall** nastavením přístupových práv v tzv. **přístupových seznamech (ACL, Access Control List)** pomocí nich mohu **zakázat (*access deny*) nebo povolit (*access grant, permit*) síťový provoz** na určitých adresách a na určitých protokolech, nebo je možné vložit firewall jako samostatné propojovací zařízení,
- **Správa adres (*Address Management*)** – zmenšení jednotlivých sítí zmenší zbytečnou režii v celé síti. Pokud potřebujete z jedné LAN přistupovat do jiné (vzdálené) sítě, použijete zařízení zvané **brána (*gateway*)** což je směrovač, sloužící jako východ z naší sítě (a spojující tuto síť s jinou sítí).
- **Hierarchické adresování** – **IP adresa = adresa sítě (síťová část adresy *network portition*) + adresa hostitele v této síti (hostitelská část adresy *host portition*)**. (Síťovou část IP adresy určíme **odmaskováním (logický součin AND, anding)** IP adresy maskou podsítě.)



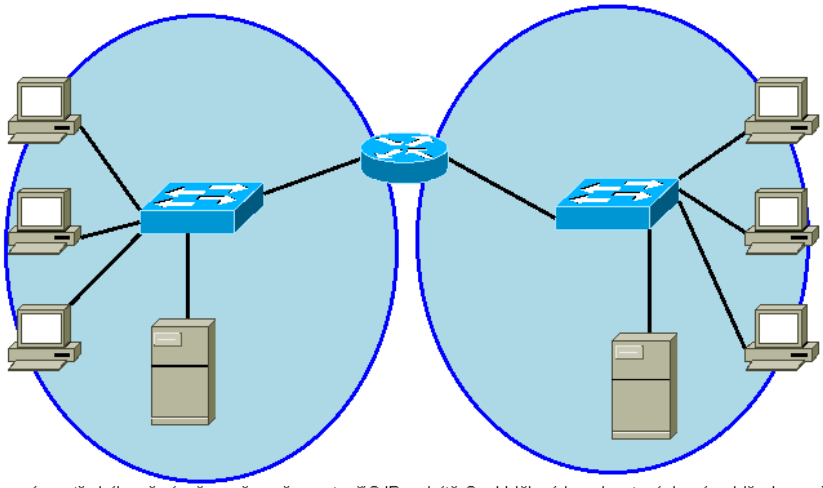
- => Oddělení hostitelů, kteří potřebují komunikovat hlavně mezi sebou, od ostatních. Vhodné například pro agregaci, sumarizaci, cest při směrování, atd.



Všechna zařízení v této síti jsou propojeny do jedné broadcastové domény, pokud jsou přepínače ve výchozím továrním nastavení. Pokud přepínače posílají broadcast standardně, bude broadcast doručen všem zařízením v této síti.

Jak se síť rozdělí do menších sítí, podsítí?

Náhrada přepínačů směrovači. Podsíťování IP adres (maska nové menší sítě tzv. podsítě (*subnet*) je delší než byla maska původní sítě (nadsítě, *supernet*).



Nahrazení prostředního přepínače směrovačem vytvoří 2 IP podsítě, 2 oddělené broadcastové domény. Všechna zařízení jsou propojena, ale lokální broadcast je oddělen.

Cvičení

ipconfig

- IP adresa,
- maska podsítě,
- implicitní (výchozí) brána,
- (primární a sekundární) DNS server.

Brána

Brána (Gateway) je východ z naší sítě. Žádný paket se ze sítě nedostane aniž má **na směrovači (bráně)** nastavenou **cestu (*route*)** ve **směrovací tabulce (*routing table*)**. Z klienta do jiné sítě **přes bránu** se paket dostane pouze v případě, že má klient nastavenou **implicitní bránu (*Default Gateway*)**.

Vytváření podsítí

Rozdělování **sítí (*network*)** do menších sítí - **podsítí (*subnet, subnetwork,* „subsíť“)** se nazývá **podsíťování (*subnetting*)**. Masky (podsítě) jsou vyjádřené **v lomítkovém (*slash*) tvaru** (/24) nebo v **kanonickém tvaru (*canonical form*)** (255.255.255.0). Propojování podsítí se provádí též **směrovačem (bránou)**. S výhodou lze použít hierarchie IP adres a určité činnosti (například sumarizaci, agregaci směrování) provádět za celou **nadsíť (*supernet,* „*supersíť*“)**.

Směrování

1. **Směrování je nalezení „nejlepší“[45] cesty / “nejlepšího“ směru do cílové sítě.** Směrování je hlavní činnost **směrovače**. Číselné vyjádření ceny cesty se nazývá metrika. Nejlepší cesta je nejlevnější cesta, tedy cesta s nejmenší metrikou.
2. Pokud se data dopravují pouze v rámci jedné sítě, není potřeba směrovač.
3. Pokud jsou data do jiné sítě (a to klient zjistí porovnáním síťové části své a cizí adresy), jsou data poslána na **bránu (*Gateway*) (= vstupní rozhraní směrovače)**.
4. Pokud je cílová síť:

   4.1. **přímo připojená, přilehlá (*Directly Connected*)**, jsou do ní data rovnou předána.

   4.2. Pokud **není síť přímo připojená je vzdálená (*remote network*)** a router potom hledá cestu (do dalšího směrovače ve směru k cílové síti) ve směrovací tabulce. (Ve skutečnosti se cesta hledá ve směrovací tabulce vždy, ale pro přímo připojené sítě, se nehledá žádná jiná (lepší) cesta. Protože přímo připojená síť má administrativní vzdálenost = 0. Cesta do přímo připojené síti se na směrovači vytvoří okamžitě potom, co administrátor nakonfiguruje příslušné rozhraní směrovače popřípadě celou linku do přilehlé sítě.)
5. Ve směrovací tabulce (*routing table*) se pro cílovou síť nalezne směr (*route*) (odchozí rozhraní aktuálního směrovače nebo vstupní rozhraní následujícího směrovače = další přeskok = *next hop* = *gateway*)[46], kam se má paket (zapouzdřený do příslušného rámce) přeposlat. Pokud je ve směru do cílové sítě zadána místo odchozího rozhraní adresa dalšího přeskoku (*next-hop*), paket je odeslán na výstupní rozhraní, do kterého je přímo připojena síť, ve které adresa dalšího přeskoku leží.

Směrovací tabulka

Jednotlivé řádky **směrovací tabulky**[47] (*routing table*) obsahují směry (cesty) (*route*) do cílové sítě.

45 Kritéria co je „nejlepší“, mohou být různá. Budeme probírat v příštím semestru.

46 Přesněji řečeno, k dalšímu přeskoku se musí ve směrovací tabulce ještě rekurzivně dohledat síť, ve kterém leží, a k ní příslušné odchozí rozhraní.

47 Někdy se také setkáte s termínem „routovací tabulka“.

Aby směrovač mohl směrovat (poslat data do určité cílové sítě) musí o této síti „vědět“, tzn. mít pro tuto síť řádku (*entry*) ve své směrovací tabulce. (Uvědomte si, že **směrovač ve směrovací tabulce zná pouze směr do cílové sítě** nikoliv celou konkrétní cestu (tj. směrovače, přes které se do cíle dostane).)

Obsah jednotlivé řádky může být získán třemi způsoby:

1. **přilehlé sítě** (řádky jsou automaticky vytvořené směrovačem při konfiguraci rozhraní a linky **přímo připojené sítě na směrovači**),
2. **statické směrování** (řádky ručně nastavil (vytvořil) **administrátor**),
3. **dynamické směrování** (řádky směrovací tabulky se dynamicky aktualizují pomocí **dynamických směrovacích protokolů** *(routing protocols)*).

Směry (cesty, trasy, *route*) do cílové sítě ve směrovací tabulce (*routing table*) mají **3 základní části**:

- Protokol, kterým byla řádka získána,
- **Cílová síť (*Destination network*),**
- Maska podsítě (*Subnet Mask*),
- **Odchozí rozhraní (*Outgoing interface, exit interface*),**
- Další přeskok - IP adresa vstupu do následujícího směrovače (*Next-hop* = *Gateway* (brána)),
- **Metrika (*Metric*)** (na Cisco routerech je ve tvaru **administrativní vzdálenost/metrika**). Metrika vyjadřuje „cenu“ cesty. Vybírá se „nejlepší“ = „nejlevnější“ cesta. **Administrativní vzdálenost (*administrative distance, AD*)** vyjadřuje „cenu“, kvalitu (důvěryhodnost) samotného směrovacího protokolu. (Nejlepší protokol je ten s nejmenší administrativní vzdáleností. Přímo připojená síť má AD = 0, statická cesta má AD = 1 atd..)

Směrovací tabulka může ještě, kromě cest (směrů, *route*) na konkrétní cílové sítě, obsahovat **implicitní cestu (*default route*)**, je to cesta do jakékoliv jiné sítě, která není explicitně uvedena ve směrovací tabulce = **cílová síť 0.0.0.0**[48] **s maskou 0.0.0.0**, tam se posílá vše co nebylo spárováno (*match*) ve směrovací tabulce. Protože se ve směrovací tabulce hledá, jako by řádky byly setříděny sestupně podle délky masky, prohledává se implicitní cesta jako poslední řádka a říká se jí také proto „brána poslední záchrany“ (*gateway of last resort*).

Výpis obsahu směrovací tabulky:

- na směrovači – výpis v IOS směrovačů Cisco: **#show ip route**
  - **přilehlé sítě** (automaticky vytvořené směrovačem při konfiguraci rozhraní a linky do k tomuto směrovači přímo připojené sítě),
  - **statické směrování** (ručně nastavil administrátor),
  - **dynamické směrování** (řádky směrovací tabulky se dynamicky aktualizují pomocí **směrovacích protokolů**).
- na hostitelském počítači – výpis: **netstat -r**, **route print (další parametry: add, delete, change).** (Každý klient má směrovací tabulku (i když má pouze jednu síťovou kartu), ta obsahuje implicitní výchozí bránu, implicitní cestu, loopback a vlastní IP adresu což východ z operačního systému do sítě.) Poznámka: Jak se z počítače stane směrovač? Má alespoň

48 Adresa 0.0.0.0 nesmí být přidělena žádné skutečně existující síti. Je to vyhrazená adresa znamenající „jakákoliv síť“.

dvě síťové karty a operační systém podporující směrování (IP protokol).

Směrovací tabulka na směrovači (Cisco)

```
A#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     172.16.0.0/24 is subnetted, 6 subnets
C       172.16.1.0 is directly connected, Serial0/1/1
D       172.16.2.0 [90/2681856] via 172.16.3.253, 00:00:14, Serial0/1/0
                   [90/2681856] via 172.16.1.254, 00:00:10, Serial0/1/1
C       172.16.3.0 is directly connected, Serial0/1/0
C       172.16.4.0 is directly connected, FastEthernet0/0
D       172.16.5.0 [90/2172416] via 172.16.1.254, 00:00:10, Serial0/1/1
D       172.16.6.0 [90/2172416] via 172.16.3.253, 00:00:14, Serial0/1/0
S*   0.0.0.0/0 is directly connected, Serial0/1/1
A#
```

Směrovací tabulka na hostiteli (Windows XP)

```
C:\>netstat -r

Směrovací tabulka
===========================================================================
Seznam rozhraní
0x1 ........................... MS TCP Loopback interface
0x2 ...00 06 5b a9 dd 0f ...... 3Com 3C920 Integrated Fast Ethernet Controller
(3C905C-TX Compatible) - Packet Scheduler Miniport
===========================================================================
===========================================================================
Aktivní směrování:
       Cíl v síti     Síťová maska            Brána        Rozhraní  Metrika
          0.0.0.0          0.0.0.0  192.168.105.254  192.168.105.34        20
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1         1
    192.168.105.0    255.255.255.0   192.168.105.34  192.168.105.34   20
   192.168.105.34  255.255.255.255        127.0.0.1       127.0.0.1   20
  192.168.105.255  255.255.255.255   192.168.105.34  192.168.105.34   20
        224.0.0.0        240.0.0.0   192.168.105.34  192.168.105.34   20
  255.255.255.255  255.255.255.255   192.168.105.34  192.168.105.34         1
Výchozí brána:   192.168.105.254
===========================================================================
Trvalé trasy:
   Žádné
```

Tentýž výpis získáte ve Windows též příkazem **route PRINT**.

Směrovací tabulka na hostiteli (Linux)

```
$netstat -r
Směrovací tabulka v jádru pro IP
Adresát         Brána           Maska           Přízn   MSS Okno    irtt Rozhraní
169.254.0.0     *               255.255.0.0     U         0 0          0 eth0
172.16.0.0      *               255.255.0.0     U         0 0          0 eth0
default         ns.spse.pilsedu 0.0.0.0         UG        0 0          0 eth0
```

Tentýž výpis získáte v Linux též příkazem **route**.

Cvičení

Ukázka: Packet Tracer (určit celkový počet sítí ze schématu sítě, ukázka směrovací tabulky, implicitní cesta). Vznik směrovací smyčky.

Směrování - postup

1. Směrování probíhá paket po paketu a směrovač po směrovači (*packet-by-packet and hop-by-hop*).
2. Každý paket je zpracováván nezávisle na každém dalším směrovači v průběhu cesty, pouze na základě směrovací tabulky na aktuálním směrovači.
3. Na každém směrovači se rámec odpouzdří (*decapsulate*) na paket. V paketu se zmenší TTL o jedničku. Pokud je TTL po odečtení rovné 0, paket se zahodí a do cíle je o tom odeslána zpráva ICMP (překročena doba života). Z paketu se separuje cílová IP adresa každého jednotlivého paketu a porovnává se se směrovací tabulkou pro určení cesty (na každé řádce směrovací tabulky se cílová adresa odmaskuje maskou v této řádce a porovná s adresou cílové sítě v této řádce).

Router potom udělá s paketem jednu ze tří věcí:

- Odešle (*forward*) ho přes odchozí rozhraní na další směrovač (*next hop*) (pro vzdálenou síť),
- Odešle (*forward*) ho do cílového hostitele (*destination host*) (pokud je hostitel v přímo připojené síti),
- Odloží ho (*drop it, discard it*) – pokud je cíl nedostupný. (V tomto případě směrovač odešle do zdroje paketu ICMP zprávu, že je cíl nedostupný.)

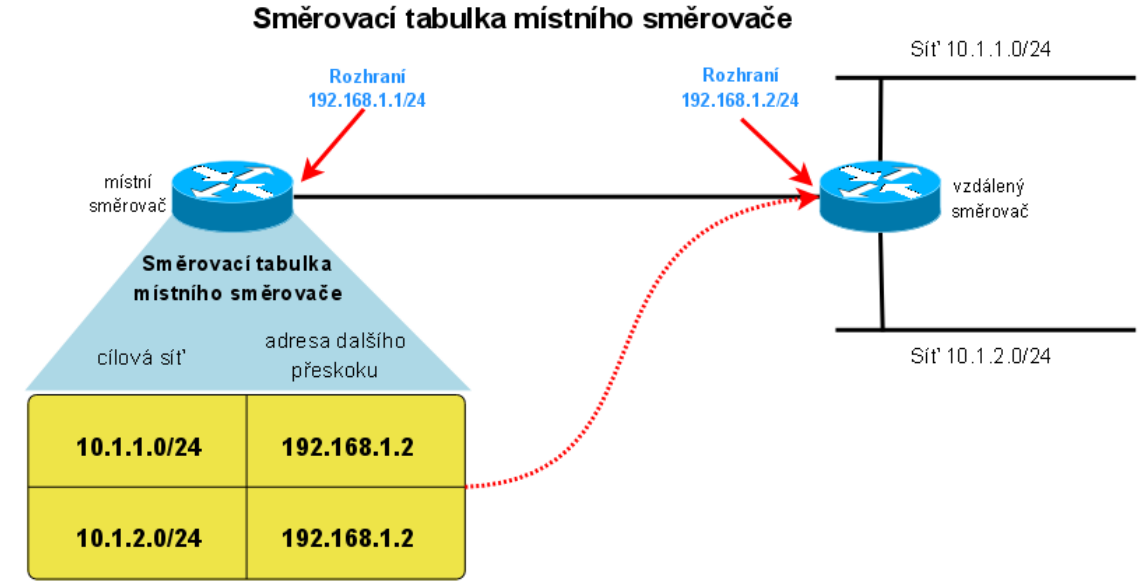
Protože paket na směrovač přichází zapouzdřený do L2 rámce, musí se rámec nejprve **odpouzdřit (*decapsulate*)**. Po určení cesty se na směrovači paket opět zapouzdří do nového L2 rámce a odešle směrem k cíli.

Pokud není směr do konkrétní cílové sítě nalezen a je zároveň nastavena implicitní cesta, pošle se zapouzdřený paket na směr implicitní cesty. **Implicitní cesta** je také známa jako ***Gateway of Last Resort (= brána posledního útočiště)***. Pokud není v tomto případě nastavena implicitní cesta paket se odloží, zahodí, (*drop it*) a je o tom informován zdroj paketu pomocí ICMP zprávy.

Postup:

1. Klient odesílá paket. Otestuje se zda je cílová adresa uvnitř (lokální) sítě (= po odmaskování zdrojové a cílové adresy maskou podsítě se obě adresy rovnají). Pokud ano (je uvnitř sítě), přepošle se na úrovni spojové (linkové) vrstvy. Pokud ne (je v jiné síti), odešle se na **implicitní výchozí bránu**.
2. Na **bráně (routeru)** se rozhoduje, zda je cíl přímo připojené, přilehlé, zařízení (leží v přímo připojené síti). Pokud ne, pošle se na další směrovač (router).
3. Na dalším směrovači se rozhoduje, zda je cíl přímo připojené zařízení (leží v přímo připojené síti). Pokud ne, pošle se na další směrovač (router). Atd.

4. IP paket dorazí do cíle. Z paketu se odstraní hlavička a TCP segment je postoupen do L4 na příslušném síťovém zařízení.
5. L2 PDU se vytváří vždy nová pro každý síťový segment (pro každou jednotlivou fyzickou síť).
6. L3 PDU se během své cesty sítí (jednotlivými směrovači) nemění (s výjimkou dekrementace (odečítání jedničky z) pole TTL a přepočtu CRC záhlaví).
7. L4 PDU se během své cesty sítí (jednotlivými směrovači) nemění.



Další přeskok pro obě sítě 10.1.1.0/24 a 10,1.2.0/24 z místního směrovače je 192.168.1.2

Směrovací protokoly

- **Směrovací protokoly** slouží k dynamickému sdílení směrovacích informací (o cestách do cílových sítí) mezi jednotlivými směrovači => **dynamické směrování**. Aktualizace směrovacích tabulek: Každý směrovač posílá informace jednak o svých přímo připojených (přilehlých) sítích, jednak o sítích, o kterých se dozvěděl z okolních směrovačů. To ovšem vyžaduje procesorový čas pro vzájemnou výměnu a aktualizaci informací.
- Jiná možnost je, aby směrovací informace směrovači ručně zadal administrátor => **statické směrování**. Statické směrování nemá žádnou režii.
- Přímo připojené, přilehlé, sítě vytvářejí řádky ve směrovací tabulce automaticky (po konfiguraci a zapnutí rozhraní do příslušné sítě na směrovači a zprovoznění linky).

Běžné (interní) směrovací protokoly jsou:

- Routing Information Protocol (RIP),
- Enhanced Interior Gateway Protocol (EIGRP),
- Open Shortest Path First (OSPF).

Internetová brána - Internet Gateway - RFC 823, http://www.ietf.org/rfc/rfc0823.txt

Porovnání statického a dynamického směrování

Vlastnost	*Statické směrování*	*Dynamické směrování*
Popis metody	● jedna cesta k cíli, zadaná správcem sítě, ● voleno především z bezpečnostních důvodů, ● vhodné tam, kde existuje pouze jediná cesta, ● jako rezerva pro selhání směrovacího protokolu	● směrovací protokol, ● metrika (počet hopů, propustnost zpoždění, spolehlivost, zátěž, maximální délka cena), ● směrovací algoritmy: ● vektor vzdáleností (*distance vector*), ● stav spojů (*link state*)
automatické reakce na změny v síti	ne	ano
možnost rozložit zátěž na několik cest	staticky lze (podle typu směrovače)	ano (některé protokoly)
potřeba správce pro manuální (re)konfiguraci	vysoká	malá
dohled nad používanými cestami	vysoký	malý
výměna směrovacích informací	žádná	ano
zátěž směrovače	minimální	střední až vysoká
zátěž paměti	minimální	střední až vysoká
zátěž sítě	žádná	střední (při běžné činnosti) až vysoká (při startu)

Cvičení

Příklad obsahu směrovací tabulky.
Máme dva směrovače R1 a R2. Mezi nimi je spojovací síť 10.1.1.0/24 na sériové lince. Ke každému směrovači je přes Ethernet připojena LAN s klienty (zleva sítě 172.16.1.0/24 a 172.17.1.0/24).
Obsah směrovací tabulky na směrovači R1:

***Popis** (ten ale není ve směrovací tabulce)*	***Protokol***	***Cílová síť/Maska***	***Odchozí rozhraní***	***Next hop,*** ***IP adresa vstupního rozhraní následujícího směrovače, Brána***	***Metrika*** ***(AD/Metrika)***
Přímo připojená síť (LAN)	C	172.16.1.0/24	E0	---	0/0
Přímo připojená síť (propojovací síť)	C	10.1.1.0/24	S0	---	0/0
Statická cesta do vzdálené sítě (LAN)	S	172.17.1.0/24	(S0)	10.1.1.254/24	1/0
Implicitní cesta (pro nenalezené cílové sítě)	S*	0.0.0.0/0	(S0)	10.1.1.254/24	1/0

C = přímo připojená síť (administrativní vzdálenost, *Administrative Distance*, AD = 0),

S = statická cesta (AD = 1).
* = kandidát na implicitní cestu
Administrativní vzdálenost určuje důvěryhodnost směrovacího protokolu. Čím nižší číslo, tím větší důvěryhodnost. Vidíte, že nejlepší je přilehlá (přímo připojená) síť a potom statická cesta.

Cvičení

Packet Tracer **cvičení 5.6.1.3** – najděte, co vše není nastaveno a zkuste nejprve bez návodu (už bychom měli vědět, co má být nastaveno) a potom podle návodu opravit. Kontrolujte nastavení IP adres rozhraní, masky a nastavení bran.

1. Bez návodu, byste měli sami najít, co vše chybí nastavit.
2. Bez návodu, byste měli určit i jaké konkrétní hodnoty, máte nastavit (s výjimkou jedné jediné, kterou **zatím** neumíme zjistit).
3. Nakonec použijte návod.

Kontrolní opakovací otázky a odpovědi (kvíz):

1) Který protokol zajišťuje nespojované (nespojově orientované) služby na síťové vrstvě?
   a) IP (Internet Protocol)
2) Který protokol je nespojovaný (z následujících: TCP, UDP, FTP, SMTP)?
   a) UDP
3) Která část adresy na síťové vrstvě je použita směrovačem při výběru nejlepší cesty do cíle?
   a) Síťová část (= adresa sítě)
4) Které síťové zařízení dokáže rozdělit síť do různých domén všesměrového vysílání (*broadcast domain*)?
   a) Směrovač (*router*)
5) Kterému problému na síťové vrstvě lze předejít nebo ho zmenšit použitím konzistentní adresace koncových zařízení (*end-to-end addressing*)?
   a) Omezení nepotřebného všesměrového vysílání.
6) Které dva příkazy mohou být (na klientu) použity pro výpis směrovací tabulky?
   a) route PRINT
   b) netstat -r
7) Které tři údaje (jaké informace) o příslušném směru lze nalézt ve směrovací tabulce?
   a) Adresa cílové sítě,
   b) adresa následujícího přeskoku (*next-hop*) – následující směrovač,
   c) metrika.
8) Které tři druhy problémů jsou způsobeny nadměrným provozem všesměrového vysílání v určité síti?
   a) Zvýšení režie (*overhead*) v síti,

b) spotřeba šířky pásma síťového média,

c) přerušení dalších funkcí klientů v síti (spotřebovává výkon jejich procesoru).

9) Které tři faktory byste měli vzít v úvahu při seskupování hostitelů do jedné společné sítě?

a) Účel,

b) geografické umístění,

c) vlastnictví.

Kapitola 6 – Adresování sítí IPv4

V této kapitole se naučíme:

- Vysvětlit strukturu IP adres a demonstrovat svou schopnost převádět mezi 8-bitovými binárními a decimálními čísly.
- Zadanou adresu IPv4 zařadit do jejího typu a popsat jak je použita v síti.
- Vysvětlit jak jsou adresy přiřazovány sítím poskytovatelem služeb (ISP) a administrátory uvnitř jednotlivých sítí.
- Určit síťovou část adresy hostitelského počítače a vysvětlit roli masky podsítě při rozdělování sítí.
- Při zadaných informacích a kritériích pro IPv4 adresy, vypočíst odpovídající komponenty pro adresaci sítě.
- Použít běžné testovací utility k ověření a testování síťového připojení a funkčního stavu protokolového zásobníku TCP/IP a hostitelského počítače.

Anatomie adresy IPv4

Tečkový dekadický tvar (= kanonický tvar, *canonical form***)** 32-bitové IP adresy se zavedl pro snazší práci člověka s IP adresou.

Binární tvar adresy 10101100000100000000010000010100 je v tečkovém dekadickém (kanonickém) tvaru 172.16.4.20.

Binární tvar adresy 00001010000010100000101000001010 je v kanonickém tvaru 10.10.10.10.

Postup převodu: Každý oktet (8 bitů) převedete na dekadické číslo a oddělíte tečkou.

IP adresa má **hierarchickou strukturu** (obrázek viz kapitola 5 – Síťová vrstva – protokol IPv4):

IP adresa = adresa sítě (síťová část adresy) + adresa hostitele v síti (hostitelská část adresy).

Hranice mezi síťovou a hostitelskou částí IP adresy je dána maskou sítě. Jedničky v binárním tvaru masky zleva určují na své pozici síťovou část IP adresy, nuly určují hostitelskou část.

Například:

Adresa hostitele:		192.168.1.15 /24	(kde /24 je prefix sítě, kolik bitů zleva v masce je binárně rovno jedničce, kolik bitů tvoří zleva síťovou část IP adresy)
Adresa sítě:		192.168.1.0	<= (192.168.1.15 AND 255.255.255.0) tzv. odmaskování
Hostitelská část adresy:		+ 0.0.0.15	
IP adresa hostitele:		192.168.1.15	Součet adresy sítě a hostitelské části dá opět původní rozkládanou adresu hostitele.

Převody mezi dvojkovou a dekadickou soustavou

Dvojková i dekadické číselná soustava jsou obě tzv. Poziční číselné soustavy (*Positional notation*). Hodnota každé číslice je dána její pozicí (řádem) v konkrétním čísle. Tato N-tá pozice, řád, určuje váhu číslice v čísle a je rovná N-té mocnině **základu** (*radix*) příslušné číselné soustavy. Tedy pro dvojkovou číselnou soustavu v rozsahu jednoho bajtu:

Řád pozice - N	***7***	***6***	***5***	***4***	***3***	***2***	***1***	***0***	
Váha pozice ***N-tá mocnina základu (radix) 2^N***	***128***	***64***	***32***	***16***	***8***	***4***	***2***	***1***	
Příklad	1	1	1	1	1	1	1	1	**= 255_D**
Příklad	0	0	0	0	0	0	0	0	**= 0_D**
Příklad	1	0	0	0	0	0	1	0	**= 130_D**

Odečítací metoda (převod dekadického čísla na binární v rozsahu 1 bajtu)

Pro binární soustavu jde při převodu z desítkové soustavy jednoduše o rozklad dekadického čísla na součet jednotlivých mocnin dvojky.

Příklad: $(172)_D$

172	
-128	Lze odečíst 128 => zapíši **na 7. řádu 1**
44	
-0	Nelze odečíst 64 => zapíši **na 6. řádu 0**
44	
-32	Lze odečíst 32 => zapíši **na 5. řádu 1**
12	
-0	Nelze odečíst 16 => zapíši **na 4. řádu 0**
12	
-8	Lze odečíst 8 => zapíši **na 3. řádu 1**
4	
-4	Lze odečíst 4 => zapíši **na 2. řádu 1**
0	
-0	Nelze odečíst 2 => zapíši **na 1. řádu 0**
0	
-0	Nelze odečíst 1 => zapíši **na 0. řádu 0**
0	

Výsledek je převodu $(172)_{10}$ je $(1010\ 1100)_2$.

Vyčíslení definičního polynomu (převod binárního čísla na dekadické):

Příklad: $(1000\ 0010)_2 = 1*128 + 0*64+0*32+0*16+0*8+0*4+1*2+0*1 = 128 + 2 = (130)_{10}$.

Typy adres v síti IPv4

- **Adresa sítě** – síťová část adresy (odkazuje na celou síť/podsíť). V hostitelské části adresy binární nuly. Tuto adresu nesmí mít žádné konkrétní zařízení v síti. Na adresu celé sítě se odkazujeme ve směrování do cílové sítě.
- **Adresa nesměrového vysílání** – v hostitelské části jsou binárně samé jednotky (nesměrové vysílání zasáhne všechny právě funkční stanice/hostitele v síti). Tuto adresu nesmí mít žádné konkrétní zařízení v síti. Na adresu posíláme zprávy, které přijmou všichni (zapnutí) hostitelé v síti.
- **Adresa hostitele v síti – hostitelská část adresy** - každý hostitel (uzel (*node*)) v síti má svou unikátní adresu.

V starší terminologii technologie **CIDR (*Classless Inter Domain Routing*)** je **prefix sítě** (= síťová část IP adresy) adresa sítě, zápis prefix/maska např. 172.16.0.0/16. **Délka síťového prefixu** v bitech je rovna počtu jednotkových bitů zleva v masce podsítě to znamená také číslu v masce v lomítkovém (*slash*) tvaru.

V nové terminologii **VLSM (*Variable Length Subnet Mask*)** se potom podsíť nazývá **adresní blok** a lomítkový tvar masky **síťový prefix**.

Maska podsítě v desítkovém kanonickém (*canonical*) tvaru 255.255.255.0 je v **lomítkovém (*slash*) tvaru (prefixu) rovna** /24.

Výpočty adres sítí, hostitelů a všesměrového vysílání

Typy komunikace

- ***Unicast* – jednosměrové (směrové) vysílání** - odesílá paket z jednoho hostitele do jiného jednotlivého hostitele. (Pokud nebude explicitně řečeno jinak, zabýváme se v tomto kurzu pouze jednosměrovým vysíláním.)
- ***Broadcast (B/C)* – všesměrové (nesměrové, všeobecné oběžníkové) vysílání** – speciální adresa, její použití odesílá paket z jednoho hostitele do všech právě aktivních hostitelů v této síti. Tuto adresu nesmí mít žádné konkrétní zařízení v síti.
    - Příklady použití B/C:
        - mapování adres vyšší vrstvy na adresu nižší vrstvy (ARP request),
        - vyžádání adresy (DHCP request na DHCP server),
        - výměna směrovacích informací směrovacími protokoly (RIP).
    - Jsou **dva typy nesměrového vysílání** (B/C):
        - ***directed broadcast* (směrovatelný B/C)** – určen všem hostitelům v určité **ne-**

lokální síti (ve vzdálené síti). Například: hostitel vně sítě komunikuje s hostitelem v síti 172.16.4.0 /24, cílová adresa paketu by byla 172.16.4.**255**. Ačkoliv směrovače tento *directed broadcast* implicitně nepřeposílají, lze je nakonfigurovat tak, aby ho přeposílaly.

- ***limited broadcast* (omezený B/C)** – omezen na všechny hostitele v jedné aktuální lokální síti – všeobecná adresa 255.255.255.255. Směrovač toto vysílání nepřeposílá do jiných sítí. Například hostitel s IP adresou 172.16.4.1 /24 v síti 172.16.4.0 /24 může všesměrově vysílat na všechny hostitele **v jeho síti** použitím paketu s cílovou **všeobecnou adresou 255.255.255.255**.

- ***Multicast* – skupinové vysílání (vícesměrové vysílání) –** je určeno pro úsporu přenosové kapacity sítě IPv4, redukuje síťový provoz tím, že odesílá paket z jednoho hostitele do vybrané skupiny hostitelů. (Při použití unicastové komunikace s více cílovými klienty musí vysílající hostitel posílat individuální paket pro každý cílový klient. Při multicastové komunikaci může zdrojový hostitel vyslat jeden paket, který dosáhne tisíce cílových hostitelských počítačů.)
  - Příklady použití skupinového vysílání:
    - distribuce videa a audia,
    - výměna směrovacích informací směrovacími protokoly (OSPF),
    - distribuce SW (UDPcast),
    - zpravodajství – tok datových novin (*News feeds*).

  - Definice skupin pro skupinové vysílání. Hostitelské počítače, které přijímají určitá multicastová data se nazývají multicastoví klienti (*multicast client*). Tito klienti používají služby vyvolané klientským programem, aby se stali členem multicastové skupiny (*multicast group*). Každá tato skupina je reprezentovaná jednou multicastovou cílovou adresou. Když je hostitelský počítač přihlášen do multicastové skupiny, počítač zpracovává pakety adresované do této multicastové adresy stejně jako pakety adresované do jeho unikátní unicastové adresy. Jak ještě uvidíme, IPv4 má stranou pro adresaci multicastových skupin speciální blok adres od 224.0.0.0 do 239.255.255.255.

Přiřazování adres v síti

Příklad

Zadaná IP adresa hostitele v síti: 172.16.1.1/24 a z ní určíme:

- **Síťová část adresy** je 172.16.1.0 (IP adresa hostitele odmaskovaná maskou (logický součin, AND), v hostitelské části jsou binárně samé nuly),
- **Broadcastová adresa**: 172.16.1.255 (síťová část adresy binárně doplněná v hostitelské části samými jedničkami),
- **Interval použitelných adres hostitelů** (ležící mezi adresou sítě a adresou všesměrového vysílání):
  - **první použitelná adresa hostitele**: 172.16.1.1
  - **poslední použitelná adresa hostitele**: 172.16.1.254.

Cvičení

Samostatně doplňte následující tabulku (*předvyplněno kurzívou*). Ke kanonickým tvarům (adres) si vždy dopište i jeho binární tvar a k lomítkovým tvarům masek (prefixům) si napište její kanonický tvar.

IP adresa/maska	*Počet možných adres v síti celkem*	*Počet adres hostitelů v síti*	*Adresa sítě*	*Adresa nesměrového vysílání v této síti*	*Rozsah povolených adres hostitelů - poslední bajt*
172.16.4.0/ 24	*2^8 = 256*	*2^8 – 2 = 254*	*172.16.4.0*	*172.16.4.255*	*.1 - .254*
172.16.4.0/ 25	*2^7 = 128*	*2^7 – 2 = 126*	*172.16.4.0*	*172.16.4.127*	*.1 - .126*
172.16.4.0/ 26	*2^6 = 64*	*2^6 – 2 = 62*	*172.16.4.0*	*172.16.4.63*	*.1 - .62*
172.16.4.0/ 27	*2^5 = 32*	*2^5 – 2 = 30*	*172.16.4.0*	*172.16.4.31*	*.1 - .30*
172.16.4.0/ 28	*2^4 = 16*	*2^4 – 2 = 14*	*172.16.4.0*	*172.16.4.15*	*.1 - .14*

172.16.4.0 AND 255.255.255.0 = 172.16.4.0 = **adresa sítě.**

Nesměrové vysílání = adresa následující sítě – 0.0.0.1 (172.16.5.0 – 0.0.0.0 = 172.16.4.255)

Příklad:

Spočtěte adresu sítě, adresu všesměrového vysílání a rozsah povolených adres klientů v dané síti pro IP adresu hostitele **157.47.143.90 /19.**

Nejprve **spočítejme v binárním tvaru** adresy sítě a B/C (podbarvené jsou síťové části adres):

Hostitel	**Host:**	**10011101**	**00101111**	**10001111**	**1011010**	**=> 157.47.143.90/19**
AND Maska	**Mask:**	**11111111**	**11111111**	**11100000**	**00000000**	**=> 255.255.224.0**
Adresa sítě	**Net:**	**10011101**	**00101111**	**10000000**	**00000000**	**=> 157.47.128.0/19**
Broadcast	**B/C:**	**10011101**	**00101111**	**10011111**	**11111111**	**=> 157.47.159.255/19**

Adresa hostitele		157.47.143.90/19
Maska	AND	255.255.224.0
Adresa sítě (po odmaskování IP adresy maskou)		**157.47.128.0/19**

Odmaskování IP adresy maskou je provedení logického součinu (operátor AND).

Pravdivostní tabulka pro operátor AND (Výsledek je pravdivý pouze a jen tehdy jsou-li pravdivé oba dva vstupní operandy):

1 **AND** 1 = 1

1 AND 0 = 0

0 AND 1 = 0

0 AND 0 = 0

Celkový počet adres v síti (včetně adresy sítě a broadcastu) = **velikost adresního bloku**:

bude pro délku prefixu /19 : $2^{(32-19)}=2^{(13)}=2^{(5+8)}=2^5*2^8$ = v kanonickém tvaru (**0.0.32.0)**, tzn., že adresa **následující sítě k řešené** bude vypočtena („z hlavy“):

Adresa sítě aktuální sítě	157.47.128.0/19
+ celkový počet adres v síti (= velikost adresního bloku)	**+ 0.0.32.0**
Součet je adresa následující sítě	**157.47.160.0**
-1 (broadcast aktuální sítě je adresa o jedničku menší než adresa následující sítě)	**- 0.0.0.1**
Broadcast aktuální sítě	**157.47.159.255/19**

Povolený rozsah klientů (hostitelů) leží mezi těmito dvěmi mezními adresami (Network a Broadcast, B/C) tedy:

157.47.128.1 až 157.47.159.255.

Upravený způsob výpočtu (když nepočítáte „z hlavy“)[49]:

1. Adres v síti je 2^{13} = 8 192
2. Poslední dva bajty adresy sítě převedené do dekadického tvaru: 128*256 + 0*1 = 32 768
3. Sečtená adresa sítě (pouze poslední dva bajty) a celkový počet adres v jedné síti dekadicky: 8 192 + 32 768 = 40 960
4. převedeno na kanonický tvar (pro poslední dva bajty): 40960/256 = 160 => 160.0

Pro snazší představu: kanonický tečkový tvar je „jakoby“ zápis v číselné soustavě o základu 256. (Například: $(192.168.2.0 – 0.0.0.1 = 192.168.1.255)_{256}$)

Příklad
Máte zadánu adresu a masku klienta v síti. Určete adresu sítě, ve které leží, adresu nesměrového vysílání v této síti a rozsah použitelných adres klientů v této síti.

IP adresa stanice	**192.**	**168.**	**130.**	**10**	**/20**	
AND Maska	255.	255.	240.	0		
= IP adresa sítě	192.	168.	128.	0		
+ Počet adres v jedné síti	0.	0.	16.	0		$2^{12}=2^4*2^8=(0.0.16.0)_{256}$
= IP adresa následující sítě	192.	168.	144.	0		
- 1	0.	0.	0.	1		
= IP adresa B/C sítě	192.	168.	143.	255		
Rozsah použitelných adres klientů						192.168.128.1 – 192.168.143.254

Příklad
Máte zadánu adresu a masku klienta v síti. Určete adresu sítě, ve které leží, adresu nesměrového vysílání v této síti a rozsah použitelných adres klientů v této síti.

49 Nezapomeňte, že inteligentní postup výpočtu „z hlavy“ je snazší než neinteligentní postup výpočtu s kalkulačkou v ruce.

IP adresa stanice	**10.**	**10.**	**10.**	**10**	**/10**	
AND Maska	255.	192.	0.	0		
= IP adresa sítě	10.	0.	0.	0		
+ Počet adres v jedné síti	0.	64.	0.	0		$2^{22} = 2^6 * 2^8 * 2^8 = (0.64.0.0)_{256}$
= IP adresa následující sítě	10.	64.	0.	0		
- 1	0.	0.	0.	1		
= IP adresa B/C sítě	10.	63.	255.	255		
Rozsah adres klientů						10.0.0.1 – 10.63.255.254

Příklad
Máte zadánu adresu sítě a adresu nesměrového vysílání v této síti, určete masku podsítě.

IP adresa nesměrového vys.	**172.**	**31.**	**255.**	**255**	**/?**	
- IP adresa sítě	172.	16.	0.	0	/?	
= Inverzní maska podsítě	0.	15.	255.	255		
=> Maska podsítě	255.	240.	0.	0		= /12

Inverzní maska je binární doplněk masky podsítě k „samým binárním jedničkám“. Inverzní maska se ve formě tzv. pseudomasky, zástupné masky (*Wildcard Mask*) používá mimo jiné při definici přístupových seznamů na směrovači (*Access Control List*, *ACL* což je Firewall) a při konfiguraci některých směrovacích protokolů. (Přesněji řečeno: pseudomaska není přímo z definice rovna inverzní masce, ale má obvykle její tvar.)

Samé binární jedničky	**255.**	**255.**	**255.**	**255**	
- Maska podsítě	255.	255.	192.	0	
= Inverzní maska podsítě	0.	0.	63.	255	**=> inverzní maska + 0.0.0.1** **= velikosti bloku v kanonickém tvaru**

Samostatně *doplňte*:

Příklad 1

Určete počet adres v adresním bloku pro zadaný prefix (zapište také v kanonickém tvaru):

/16: *16bitů hostitele adresuje celkem $2^{16} = (0.1.0.0)_{256}$ adres*

...

/30: *2 bity hostitele adresuje celkem $2^2 = (0.0.0.4)_{256}$ adres*

Příklad 2

Určete informace o adresním bloku pro IP adresu **172.16.1.209** *(částečně předvyplněno kurzívou):*

Vypočtěte / pro prefix:	/24	/25	/26	/27	/28	/29	/30
Adresa sítě	*172.16.1.0*						*172.16.1.208*
Velikost bloku	*0.0.1.0*						*0.0.0.4*
Hostitelé	*.1 - .254*						*.209 - .210*
Adresa B/C	*172.16.1.255*						*172.16.1.211*
Kanonický tvar masky	*255.255.255.0*						*255.255.255.252*
Inverzní maska	*0.0.0.255*						*0.0.0.3*

Rezervované rozsahy IPv4 adres

- **Hostitelské adresy**: 0.0.0.0 – 223.255.255.255 (RFC 790) – pro skutečné uzly sítě, reálná síťová zařízení s přidělenými IP adresami. (POZOR: v rámci jednoho adresního bloku je vždy první a poslední adresa (adresa sítě a adresa všesměrového vysílání) speciální rezervovaná adresa, která nelze přidělit reálným síťovým zařízením (hostitelským počítačům, rozhraním směrovačů atd.).
- **Skupinové adresy**: 224.0.0.0 – 239.255.255.255 (RFC 1700) – adresace skupiny zařízení pro multicastové vysílání
- **Experimentální adresy:** – 240.0.0.0 – 255.255.255.254 (RFC 1700, 3330) – pro výzkum a experimenty – v současné době je nelze použít pro adresy fyzických zařízení.

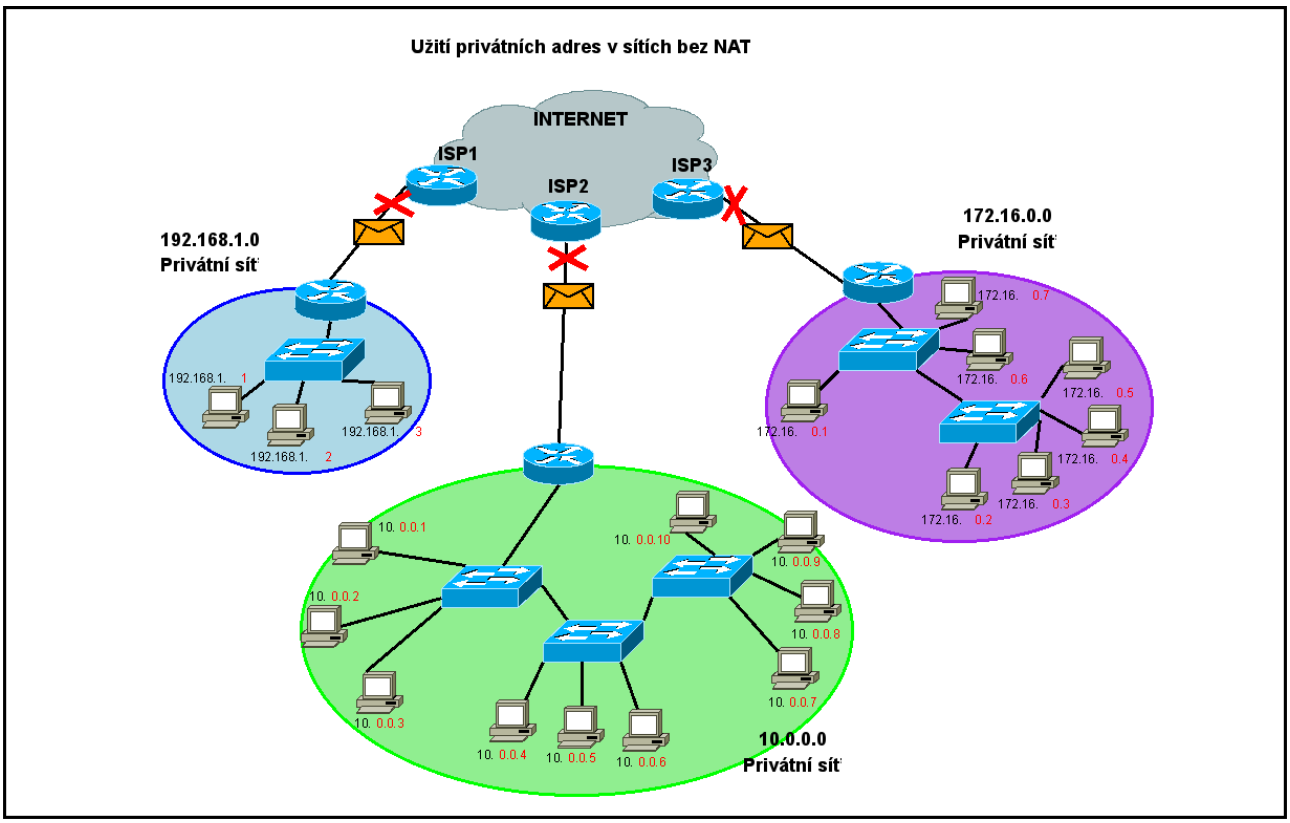
Veřejné a privátní IPv4 adresy

- **Veřejné (*public*) IP adresy** jsou unikátní v celém Internetu. Protože jsou ale postupně vyčerpávané, zavedli se tzv.:
- **neveřejné, privátní (*private*) IP adresy**, které jsou unikátní pouze v nějaké **neveřejné (privátní) síti** (skupině sítí/podsítí).
    - Pokud z těchto privátních sítí nepotřebujete přístup do Internetu, můžete je používat zcela volně.
    - Pokud potřebujete z neveřejné sítě přístup do veřejného Internetu, neveřejné IP adresy z privátní sítě jsou potom na hraničním směrovači překládány na jednu veřejnou adresu celé privátní sítě mechanismem **NAT (*Network Address Translation*)** někdy nazývaný též **IP maškaráda** (*IP masquerade*). NAT (jako funkce protokolu IP) se provozuje na zařízení oddělujícím privátní síť od veřejné (= na hraničním směrovači) a NAT jednotlivou komunikaci identifikuje podle **cílového a zdrojového socketu**. NAT zároveň blokuje přístup (= výskyt) neveřejných adres do veřejné sítě. NAT zároveň nepropustí do privátní sítě komunikaci, která není odpovědí na požadavek zevnitř sítě a slouží tedy jako firewall typu SPI. (Naopak, pokud potřebujete z privátní sítě nabízet veřejné služby, musíte buď použít demilitarizovanou zónu (DMZ) s veřejnou adresou, nebo použít PAT (*Port Address Translation*) známý též jako NAT Overload.)

Bloky privátních (neveřejných) adres (RFC 1918 – *Address Allocated for Private Internets***):**

- **10.0.0.0 až 10.255.255.255** (blok adres 10.0.0.0 /8)
- **172.16.0.0 až 172.31.255.255** (blok adres 172.16.0.0 **/12**)[50]
- **192.168.0.0 až 192.168.255.255** (blok adres 192.168.0.0 /16)

Všimněte si, že ve třídě A jde o jeden třídní blok, u třídy B o 16 bloků třídních adres B a u třídy C o 256 bloků adres v plné třídě C. Sloučení několika sítí do jedné větší nadřazené sítě (nadsítě, *super-net*) se nazývá vytváření nadsítí (*supernetting*) též agregace sítí[51]. Podobně jako se rozdělování jedné sítě na více menších sítí nazývá vytváření podsítí (*subnetting*).



Speciální IPv4 adresy

Některé adresy **nemohou být z různých důvodů přiřazeny konkrétním hostitelům**:

- **adresa sítě** a **adresa nesměrového vysílání** (první a poslední adresa v každé síti (adresním bloku)) (hostitelé – reálná síťová zařízení s IP adresou v jedné konkrétní IP síti jsou mezi tě-mito dvěma mezními vyhrazenými adresami)
- **implicitní cesta** (*default route*) (0.0.0.0 směr, který „bere všechno“ když nemáme směr do určité konkrétní sítě- adresní rozsah 0.0.0.0 – 0.255.255.255 (adresní blok 0.0.0.0/8)). Ve směrovací tabulce uváděné jako 0.0.0.0/0.

50 Tuto masku /12 musíme umět sami spočítat. (Rozdíl je 0.15.255.255 a binární doplněk 255.240.0.0 => /12.)
51 Agregaci sítí použijeme v příštím semestru pro úsporu počtu řádek ve směrovací tabulce.

- **loopback (místní smyčka, místní zpětná smyčka)** – 127.0.0.1 – ping na localhost (127.0.0.1) testuje instalaci protokolové sady TCP/IP (protokolu IP) na lokálním hostiteli a komunikaci na úrovni protokolu IP mezi operačním systémem počítače a síťovou kartou – adresní rozsah 127.0.0.0 – 127.255.255.255. (adresní blok 127.0.0.0/8). Loopback je speciální adresa, kterou hostitel použije k směrování (direct) provozu sám na sebe. Do sítě nejde žádný provoz, veškerý provoz je pouze na lokálním počítači.
- **Link-Local Addresses (adresy lokální linky)** - adresní rozsah 169.254.0.0 - 169.254.255.255 (adresní blok 169.254.0.0/16) adresa lokální linky automaticky přiřazená operačním systémem v prostředích, kde není dostupná konfigurace TCP/IP. Může být použito v malých sítích P2P, nebo když nemůže hostitel automaticky získat adresu z DHCP serveru. Adresa lokální linky **neposkytuje služby vně lokální sítě** LAN (i když mnoho aplikací bude s touto adresou pracovat korektně).
- **TEST-NET Addresses (adresy TEST-NET**) – adresní rozsah 192.0.2.0 až 192.0.2.255 (adresní blok 192.0.2.0 /24) je pro výukové a studijní účely. Na rozdíl od experimentálních adres, síťová zařízení tyto adresy akceptují. Používá se jako adresy uváděné v příkladech v jednotlivých RFC. Tyto adresy by se neměly objevit v Internetu.

Poznámka: Speciální adresy IPv4 - RFC3330: http://www.ietf.org/rfc/rfc3330.txt

Historické třídy sítí v IPv4 – alokace v plných třídách, třídní adresace[52]

Přidělování adres v **adresním prostoru plných tříd (*Classful allocation*), třídní alokace,** plýtvá s IP adresami v IPv4. Proto se přešlo na **beztřídní adresaci (*classless addressing*)**.

Toto dědictví (*legacy*) (= zastaralý způsob práce) je ovšem přesto třeba stále znát, protože se z něho stále vychází.

Třída	*1. bity prvního bajtu*	*Min hodnota 1. bajtu*	*Max hodnota 1. bajtu*	*Implicitní maska*	*Počet sítí vzorec*	*Počet sítí hodnota*	*Počet hostitelů v 1 síti*	*Počet hostitelů v 1 síti*
A	0	0*	127*	255.0.0.0	2^7 - 2*)	126	2^24 – 2	16 777 214
B	10	128	191	255.255.0.0	2^14	16 384	2^16 – 2	65 534
C	110	192	223	255.225.255.0	2^21	2 097 152	2^8 – 2	254
D	1110	224	239	-		1	2^28	268 435 456
E	1111	240	255	-		1	2^28	268 435 456

Nevýhodou třídní adresace (v celých třídách) (*classful addresing*) je rychlé vyčerpání dostupných adres. Jednotlivým firmám se původně přiděloval blok adres v rozsahu celé třídy. Poměr všech (i nepoužitelných) adres ve třídách A : B : C : D : E je 50% : 25% : 12,5% : 6,25% : 6,25%.

- Počet sítí: **2^(počet bitů v síťové části adresy – počet prvních fixních bitů).** *) Ve třídě A nelze použít sítě:
  - se samými binárními nulami v prvním bajtu **0.0.0.0/8 = implicitní cesta** (*default route*) při směrování a
  - samými binárními jedničkami v prvním bajtu **127.0.0.0/8 = lokální zpětná smyčka**

52 Třídní adresaci se též někdy říká *Fixed-Length Subnet Mask* (FLSM) v relaci s beztřídní (VLSM) – viz dále.

(*localhost, local loopback*).

- Počet hostitelů v jedné síti: **2^(počet bitů v hostitelské části adresy) – 2** (v síti se nemohou použít dvě speciální adresy:
  - samé **binární nuly v hostitelské části = adresa sítě**,
  - samé **binární jednotky v hostitelské části = adresa nesměrového vysílání**.)

My budeme používat pro další práci pouze směrové vysílání (*unicast*) třídy A, B, a C.

Beztřídní adresace

V současné době se používá **beztřídní adresace (*classless addressing*)**. V beztřídní adresaci jsou společnostem přidělovány adresní bloky bez ohledu na celou třídu. (Na směrovačích Cisco již je implicitně zapnuto příkazem *ip classless*.)

Vytváření podsítí - podsíťování (Subnetting)

CIDR (Classless Inter Domain Routing)

Vytváření podsítí k sítím v celé třídě A,B a C. Celá skupina podsítí má stejnou masku podsítě.

Adresy tříd A -E

Třída	***Vedoucí bity (Leading Bit Pattern)***	***První oktet (dekadicky)***	***Poznámky***
A	0xxxxxxx	0–127	0[53] je neplatná a 127 je rezervováno pro zpětnou smyčku
B	10xxxxxx	128–191	
C	110xxxxx	192–223	
D	1110xxxx	224–239	Rezervováno pro skupinové vysílání (*multicasting*)
E	1111xxxx	240–255	Rezervováno pro budoucí použití a testování

Adresa třídy A	**N**	H	H	H
Adresa třídy B	**N**	**N**	H	H
Adresa třídy C	**N**	**N**	**N**	H

Vysvětlivky

N = bity síťové části adresy (*network portition*)
H = bity hostitelské části adresy (*host portition*)
Samé 0 (nuly) v hostitelské části adresy = adresa sítě nebo podsítě
Samé 1 (jedničky) v hostitelské části adresy = adresa nesměrového (všesměrového) vysílání
Kombinace jedniček a nul v hostitelské části = platná adresa hostitele

53 Adresa sítě 0.0.0.0 je použita při směrování a znamená „jakákoliv síť“. Tato síť (0.0.0.0) fyzicky nesmí existovat.

Formule pro CIDR

Podsítě jsou tvořené k IP adrese v celé třídě a všechny podsítě z jedné sady mají stejnou masku – jsou stejně velké.

2^N kde N je rovné počtu zapůjčených bitů (k masce sítě, kterou podsíťujeme)	Celkový počet vytvořených podsítí
$2^N - 2$	Počet vytvořených platných podsítí (v CIDR)
2^H kde H je rovné počtu bitů hostitelské části adresy (host bits)	Celkový počet adres v jedné podsíti
$2^H - 2$	Počet adres hostitelů v jedné podsíti

Poznámka: $2^N - 2$ (nemohou se (neměli by se ve starší implementaci) používat 2 sítě:

1. sítě se samými nulami v síťové části adresy (tzv. nulová síť),
2. sítě samými jedničkami v síťové části adresy (tzv. broadcastová síť))

Jde o opatření z dob, kdy se používalo třídní směrování v celých třídách (*classful*) bez přenosu masky podsítě v aktualizacích směrování (směrovací protokol RIPv1). Nyní je na směrovačích již implicitně nastaven příkaz *ip subnet-zero* (i *ip classless*) a lze je potom použít.

Podsíťování sítě třídy C

Máme k dispozici adresní blok 192.168.100.0 /24 (privátní rozsah v plné třídě C). Chceme vytvořit 14 platných podsítí (v CIDR).

Vypočtěte masku podsítě:
Implicitní maska sítě ve třídě C je následující:

Dekadicky	Binárně
255.255.255.0	11111111.11111111.11111111.00000000

1 = Bity síťové části adresy

0 = Hostitelské bity

Vypůjčili jsme si 4 bity (adresuje celkem 16 podsítí, 2 neplatné), proto je maska podsítě následující:

11111111.11111111.11111111.**1111**0000	255.255.255.240

V jednom adresním bloku bude celkem $2^H = 2^4 = 16$ adres = (0.0.0.16) adres.

Adresní schéma bude následující:

Podsíť	***Adresa sítě (0000)***	***Rozsah adres hostitelů (0001–1110)***	***Adresa Broadcastu (1111)***
~~0 (0000) neplatná~~	~~192.168.100.**0**~~	~~192.168.100.1–~~ ~~192.168.100.14~~	~~192.168.100.**15**~~
1 (0001)	192.168.100.**16**	192.168.100.17– 192.168.100.30	192.168.100.**31**
2 (0010)	192.168.100.**32**	192.168.100.33– 192.168.100.46	192.168.100.**47**
3 (0011)	192.168.100.**48**	192.168.100.49– 192.168.100.62	192.168.100.**63**
4 (0100)	192.168.100.**64**	192.168.100.65– 192.168.100.78	192.168.100.**79**
5 (0101)	192.168.100.**80**	192.168.100.81– 192.168.100.94	192.168.100.**95**
6 (0110)	192.168.100.**96**	192.168.100.97– 192.168.100.110	192.168.100.**111**
7 (0111)	192.168.100.**112**	192.168.100.113– 192.168.100.126	192.168.100.**127**
8 (1000)	192.168.100.**128**	192.168.100.129– 192.168.100.142	192.168.100.**143**
9 (1001)	192.168.100.**144**	192.168.100.145– 192.168.100.158	192.168.100.**159**
10 (1010)	192.168.100.**160**	192.168.100.161– 192.168.100.174	192.168.100.**175**
11 (1011)	192.168.100.**176**	192.168.100.177– 192.168.100.190	192.168.100.**191**
12 (1100)	192.168.100.**192**	192.168.100.193– 192.168.100.206	192.168.100.**207**
13 (1101)	192.168.100.**208**	192.168.100.209– 192.168.100.222	192.168.100.**223**
14 (1110)	192.168.100.**224**	192.168.100.225– 192.168.100.238	192.168.100.**239**
~~15 (1111) neplatná~~	~~192.168.100.240~~	~~192.168.100.241–~~ ~~192.168.100.254~~	~~192.168.100.255~~

Rychlá kontrola	*Vždy sudé číslo*	*První platný hostitel je vždy liché číslo* *Poslední platný hostitel je vždy sudé číslo*	*Vždy liché číslo*

V kolikáté podsíti v tomto adresním schéma leží adresa 192.168.100.174?

Adresa sítě, kterou podsíťujeme = 192.168.100.0.

Adresa sítě, ve které leží zadaná adresa 192.168.100.174 AND 255.255.255.240 = 192.168.100.160.

Rozdíl je 192.168.100.160 - 192.168.100.0 = 0.0.0.160. Děleno velikostí bloku 0.0.0.160/0.0.0.16 = **10. (Je to také přímo hodnota ve čtyřech vypůjčených bitech nad implicitní masku: 1010_2 = 10_{10}.)**

=> Ve **vypůjčených bitech** (*borrowed bits*) (v IP adrese v bitech nad původní maskou podsíťované sítě a do nové masky podsítě nové podsítě) **je binárně pořadové číslo podsítě** vzhledem k původní síti. (Platí to obecně bez ohledu na třídu a adresní systém CIDR nebo VLSM.) Sítě jsou číslovány od nulté, první, atd.

Podsíťování třídy B

Máme k dispozici adresní blok 172.16.0.0 /16 (privátní rozsah v plné třídě B).Chceme vytvořit 14 platných podsítí (v CIDR):

Vypočtěte masku podsítě:

Implicitní maska sítě ve třídě B je následující:

Dekadicky	Binárně
255.255.0.0	11111111.11111111.00000000.00000000

1 = Bity síťové části adresy

0 = Hostitelské bity

Vypůjčili jsme si 4 bity (adresuje celkem 16 podsítí, 2 neplatné), proto je maska podsítě následující:

11111111.11111111.**1111**0000.00000000	255.255.**240**.0

V jednom adresním bloku bude celkem $2^H = 2^{12} = 2^4*2^8$ = 4096 adres = (0.0.16.0) adres.

Adresní schéma bude následující:

Podsíť	***Adresa sítě (0000 00000000)***	***Rozsah adres hostitelů***	***Adresa Broadcastu (1111 11111111)***
~~0 (0000) neplatná~~	~~172.16.0.0~~	~~172.16.0.1–172.16.15.254~~	~~172.16.15.255~~
1 (0001)	172.16.16.0	172.16.16.1–172.16.31.254	172.16.31.255
2 (0010)	172.16.32.0	172.16.32.1–172.16.47.254	172.16.47.255
3 (0011)	172.16.48.0	172.16.48.1–172.16.63.254	172.16.63.255
4 (0100)	172.16.64.0	172.16.64.1–172.16.79.254	172.16.79.255
5 (0101)	172.16.80.0	172.16.80.1–172.16.95.254	172.16.95.255
6 (0110)	172.16.96.0	172.16.96.1–172.16.111.254	172.16.111.255
7 (0111)	172.16.112.0	172.16.112.1–172.16.127.254	172.16.127.255
8 (1000)	172.16.128.0	172.16.128.1–172.16.143.254	172.16.143.255
9 (1001)	172.16.144.0	172.16.144.1–172.16.159.254	172.16.159.255
10 (1010)	172.16.160.0	172.16.160.1–172.16.175.254	172.16.175.255
11 (1011)	172.16.176.0	172.16.176.1–172.16.191.254	172.16.191.255
12 (1100)	172.16.192.0	172.16.192.1–172.16.207.254	172.16.207.255
13 (1101)	172.16.208.0	172.16.208.1–172.16.223.254	172.16.223.255
14 (1110)	172.16.224.0	172.16.224.1–172.16.239.254	172.16.239.255
~~15 (1111) neplatná~~	~~172.16.240.0~~	~~172.16.240.1–172.16.255.254~~	~~172.16.255.255~~

Rychlá kontrola – **v tomto případě**	Vždy (v tomto případě) 0	První platný hostitel je vždy liché číslo .1 Poslední platný hostitel je vždy sudé číslo .254	Vždy liché číslo .255

V kolikáté podsíti v tomto adresním schéma (tedy vzhledem k 172.16.0.0/16) leží adresa 172.16.174.1/20?

Adresa sítě, kterou podsíťujeme = 172.16.0.0.

Adresa sítě, ve které leží zadaná adresa: 172.16.174.1 AND 255.255.240.0 = 172.16.160.0.

Rozdíl je 172.16.160.0 – 172.16.0.0 = 0.0.160.0. Děleno velikostí adresního bloku 0.0.160.0 / 0.0.16.0 = **10.**

Pořadové číslo podsítě (počínaje nultou) je přímo hodnota ve vypůjčených bitech nad maskou původní podsíťované sítě (nadsítě)!!! (V předchozím příkladě: $1010_2 = 10_{10}$.)

Cvičení

1. Potřebujete vytvořit podsíť s 1000 klienty. Jaká je potřebná maska?
2. Potřebujete vytvořit podsíť s 500 klienty. Jaká je potřebná maska?
3. Máte IP adresu 172.17.10.10 k plné třídě vytvořte 10 podsítí. Jaká je potřebná maska podsítě?
4. Máte IP adresu 172.17.10.10 k plné třídě vytvořte 100 podsítí. Jaká je potřebná maska podsítě?
5. Převeďte masku podsítě 255.255.255.192 na lomítkový tvar masky.
6. Převeďte prefix /20 na kanonický tvar masky.
7. Máte IP adresu 192.168.10.0/29 spočtěte adresu broadcastu pro 2. podsíť vzhledem k plné třídě. (Začínáte od nulté.)
8. Máte IP adresu 172.16.0.0/28 spočtěte adresu sítě pro 30. podsíť vzhledem k plné třídě. (Začínáte od nulté.)

VLSM (Variable-Length Subnet Masking)

Formule pro VLSM

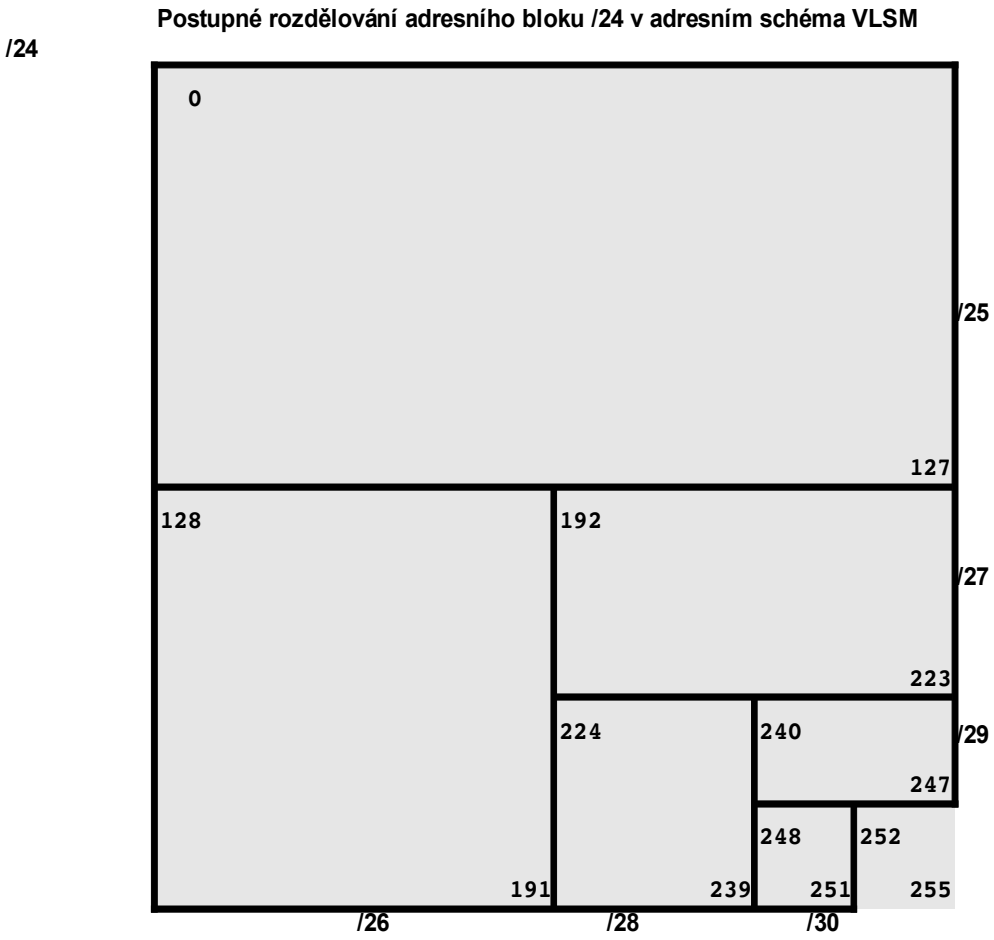
Vytváření **podsítí k podsítím**. Jednotlivé podsítě mohou mít různou masku – jsou různě veliké.

Velmi důležité u VLSM je, aby se použité adresní bloky vzájemně nepřekrývaly (*no overlap*).

2^N kde N je rovné počtu zapůjčených bitů (k masce podsítě, kterou podsíťujeme)	Celkový počet vytvořených podsítí
~~$2^N - 2$~~	~~Počet vytvořených platných podsítí~~ Ve VLSM se už nepoužívá a obě krajní podsítě lze na směrovači povolit příkazem **ip subnet-zero**.
2^H kde H je rovné počtu bitů hostitelské části adresy (host bits)	Celkový počet adres v jedné podsíti
$2^H - 2$	Počet adres hostitelů v jedné podsíti

Závislost velikosti bloku dat na masce (délce prefixu)

Prefix	Maska (binárně)	Maska	Inverzní maska (binárně)	Inverzní maska	Počet bitů hostitele	Velikost bloku	Velikost bloku (binárně)	Velikost bloku (kanonicky)
/8	11111111000000000000000000000000	255.0.0.0	00000000111111111111111111111111	0.255.255.255	24	16777216	00000001000000000000000000000000	1.0.0.0
/9	11111111100000000000000000000000	255.128.0.0	00000000011111111111111111111111	0.127.255.255	23	8388608	00000000100000000000000000000000	0.128.0.0
/10	11111111110000000000000000000000	255.192.0.0	00000000001111111111111111111111	0.63.255.255	22	4194304	00000000010000000000000000000000	0.64.0.0
/11	11111111111000000000000000000000	255.224.0.0	00000000000111111111111111111111	0.31.255.255	21	2097152	00000000001000000000000000000000	0.32.0.0
/12	11111111111100000000000000000000	255.240.0.0	00000000000011111111111111111111	0.15.255.255	20	1048576	00000000000100000000000000000000	0.16.0.0
/13	11111111111110000000000000000000	255.248.0.0	00000000000001111111111111111111	0.7.255.255	19	524288	00000000000010000000000000000000	0.8.0.0
/14	11111111111111000000000000000000	255.252.0.0	00000000000000111111111111111111	0.3.255.255	18	262144	00000000000001000000000000000000	0.4.0.0
/15	11111111111111100000000000000000	255.254.0.0	00000000000000011111111111111111	0.1.255.255	17	131072	00000000000000100000000000000000	0.2.0.0
/16	11111111111111110000000000000000	255.255.0.0	00000000000000001111111111111111	0.0.255.255	16	65536	00000000000000010000000000000000	0.1.0.0
/17	11111111111111111000000000000000	255.255.128.0	00000000000000000111111111111111	0.0.127.255	15	32768	00000000000000001000000000000000	0.0.128.0
/18	11111111111111111100000000000000	255.255.192.0	00000000000000000011111111111111	0.0.63.255	14	16384	00000000000000000100000000000000	0.0.64.0
/19	11111111111111111110000000000000	255.255.224.0	00000000000000000001111111111111	0.0.31.255	13	8192	00000000000000000010000000000000	0.0.32.0
/20	11111111111111111111000000000000	255.255.240.0	00000000000000000000111111111111	0.0.15.255	12	4096	00000000000000000001000000000000	0.0.16.0
/21	11111111111111111111100000000000	255.255.248.0	00000000000000000000011111111111	0.0.7.255	11	2048	00000000000000000000100000000000	0.0.8.0
/22	11111111111111111111110000000000	255.255.252.0	00000000000000000000001111111111	0.0.3.255	10	1024	00000000000000000000010000000000	0.0.4.0
/23	11111111111111111111111000000000	255.255.254.0	00000000000000000000000111111111	0.0.1.255	9	512	00000000000000000000001000000000	0.0.2.0
/24	11111111111111111111111100000000	255.255.255.0	00000000000000000000000011111111	0.0.0.255	8	256	00000000000000000000000100000000	0.0.1.0
/25	11111111111111111111111110000000	255.255.255.128	00000000000000000000000001111111	0.0.0.127	7	128	00000000000000000000000010000000	0.0.0.128
/26	11111111111111111111111111000000	255.255.255.192	00000000000000000000000000111111	0.0.0.63	6	64	00000000000000000000000001000000	0.0.0.64
/27	11111111111111111111111111100000	255.255.255.224	00000000000000000000000000011111	0.0.0.31	5	32	00000000000000000000000000100000	0.0.0.32
/28	11111111111111111111111111110000	255.255.255.240	00000000000000000000000000001111	0.0.0.15	4	16	00000000000000000000000000010000	0.0.0.16
/29	11111111111111111111111111111000	255.255.255.248	00000000000000000000000000000111	0.0.0.7	3	8	00000000000000000000000000001000	0.0.0.8
/30	11111111111111111111111111111100	255.255.255.252	00000000000000000000000000000011	0.0.0.3	2	4	00000000000000000000000000000100	0.0.0.4
/31	11111111111111111111111111111110	255.255.255.254	00000000000000000000000000000001	0.0.0.1	1	2	00000000000000000000000000000010	0.0.0.2



V materiálech Cisco je následující tabulka popisována jako tzv. Bobův trik (*Bob maneuvre*):

Maska podsítě	128	192	224	240	248	252	254	255
Mocnina 2^N	128	64	32	16	8	4	2	1
Pozice bitu (P)	8	7	6	5	4	3	2	1
Řád (N)	7	6	5	4	3	2	1	0
Počet platných podsítí (2^P - 2)		126	62	30	14	6	4	N/A

Adresní schéma VLSM pro poslední oktet

Prefix:	/25	/26	/27	/28	/29	/30
Počet bitů podsítě:	1	2	3	4	5	6
Počet podsítí:	2	4	8	16	32	64
Maska:	255.255.255.128	255.255.255.192	255.255.255.224	255.255.255.240	255.255.255.248	255.255.255.252
Počet bitů hostitele:	7	6	5	4	3	2
Velikost bloku:	128	64	32	16	8	4
Počet hostitelů:	126	62	30	14	6	2
.0	.0 (.1 - .126)	.0 (.1 - .62)	.0 (.1 - .30)	.0 (.1 - .14)	.0 (.1 - .6)	.0 (.1 - .2)
.4						.4 (.5 - .6)
.8					.8 (.9 - .14)	.8 (.9 - .10)
.12						.12 (.13 - .14)
.16				.16 (.17 - .30)	.16 (.17 - .22)	.16 (.17 - .18)
.20						.20 (.21 - .22)
.24					.24 (.25 - .30)	.24 (.25 - .26)
.28						.28 (.29 - .30)
.32			.32 (.33 - .62)	.32 (.33 - .46)	.32 (.33 - .38)	.32 (.33 - .34)
.36						.36 (.37 - .38)
.40					.40 (.41 - .46)	.40 (.41 - .42)
.44						.44 (.45 - .46)
.48				.48 (.49 - .62)	.48 (.49 - .54)	.48 (.49 - .50)
.52						.52 (.53 - .54)
.56					.56 (.57 - .62)	.56 (.57 - .58)
.60						.60 (.61 - .62)
.64		.64 (.65 - .126)	.64 (.65 - .94)	.64 (.65 - .78)	.64 (.65 - .70)	.64 (.65 - .66)
.68						.68 (.69 - .70)
.72					.72 (.73 - .78)	.72 (.73 - .74)
.76						.76 (.77 - .78)
.80				.80 (.81 - .94)	.80 (.81 - .86)	.80 (.81 - .82)
.84						.84 (.85 - .86)
.88					.88 (.89 - .94)	.88 (.89 - .90)
.92						.92 (.93 - .94)
.96			.96 (.97 - .126)	.96 (.97 - .110)	.96 (.97 - .102)	.96 (.97 - .98)
.100						.100 (.101 - .102)
.104					.104 (.105 - .110)	.104 (.105 - .106)
.108						.108 (.109 - .110)
.112				.112 (.113 - .126)	.112 (.113 - .118)	.112 (.113 - .114)
.116						.116 (.117 - .118)
.120					.120 (.121 - .126)	.120 (.121 - .122)
.124						.124 (.125 - .126)
.128	.128 (.129 - .254)	.128 (.129 - .190)	.128 (.129 - .158)	.128 (.129 - .142)	.128 (.129 - .134)	.128 (.129 - .130)
.132						.132 (.133 - .134)
.136					.136 (.137 - .142)	.136 (.137 - .138)
.140						.140 (.141 - .142)
.144				.144 (.145 - .158)	.144 (.145 - .150)	.144 (.145 - .146)
.148						.148 (.149 - .150)
.152					.152 (.153 - .158)	.152 (.153 - .154)
.156						.156 (.157 - .158)
.160			.160 (.161 - .190)	.160 (.161 - .174)	.160 (.161 - .166)	.160 (.161 - .162)
.164						.164 (.165 - .166)
.168					.168 (.169 - .174)	.168 (.169 - .170)
.172						.172 (.173 - .174)
.176				.176 (.177 - .190)	.176 (.177 - .182)	.176 (.177 - .178)
.180						.180 (.181 - .182)
.184					.184 (.185 - .190)	.184 (.185 - .186)
.188						.188 (.189 - .190)
.192		.192 (.193 - .254)	.192 (.193 - .222)	.192 (.193 - .206)	.192 (.193 - .198)	.192 (.193 - .194)
.196						.196 (.197 - .198)
.200					.200 (.201 - .206)	.200 (.201 - .202)
.204						.204 (.205 - .206)
.208				.208 (.209 - .222)	.208 (.209 - .214)	.208 (.209 - .210)
.212						.212 (.213 - .214)
.216					.216 (.217 - .222)	.216 (.217 - .218)
.220						.220 (.221 - .222)
.224			.224 (.225 - .254)	.224 (.225 - .238)	.224 (.225 - .230)	.224 (.225 - .226)
.228						.228 (.229 - .230)
.232					.232 (.233 - .238)	.232 (.233 - .234)
.236						.236 (.237 - .238)
.240				.240 (.241 - .254)	.240 (.241 - .246)	.240 (.241 - .242)
.244						.244 (.245 - .246)
.248					.248 (.249 - .254)	.248 (.249 - .250)
.252						.252 (.253 - .254)

Cvičení

Máme IP adresu 10.100.100.100 /12. Při podsíťování s prefixem /20 spočtěte:

1. Adresu sítě (výchozí sítě), ve které leží zadaná adresa.
2. Celkový počet podsítí vytvořených k prefixu /12 podsíťováním s maskou /20.
3. Velikost adresního bloku podsítě.
4. Adresu sítě (podsítě), ve které leží zadaná adresa.
5. V kolikáté podsíti (vzhledem k prefixu) leží zadaná adresa v podsíti /20.

Řešení:

1. *10.100.100.100 AND 255.240.0.0 = **10.96.0.0/12***
2. *20 -12 = 8; 2^8= **256***
3. *32 – 20 = 12; 2^12 = 2^4*2^8 = 4096 = **(0.0.16.0)***
4. *10.100.100.100 AND 255.255.240.0 = **10.100.96.0/20***
5. *10.100.96.0 – 10.96.0.0 = (0.4.96.0); 0.4.96.0/0.0.16.0 = **70***

Příklady na výpočty IP adres z binárního tvaru

Máte výchozí síť 172.16.48.0/20, vytvořte 4 podsítě.

Číslo podsítě	**Rozsah adres**	**Binární tvar: síťová část (vypůjčené bity) + hostitelská část IP adresy**
0.	172.16.48.0 – 172.16.51.255	10101100.00010000.001100**00.00000000** 10101100.00010000.001100**11.11111111**
1	172.16.52.0 – 172.16.55.255	10101100.00010000.001101**00.00000000** 10101100.00010000.001101**11.11111111**
2	172.16.56.0 – 172.16.59.255	10101100.00010000.001110**00.00000000** 10101100.00010000.001110**11.11111111**
3	172.16.60.0 – 172.16.63.255	10101100.00010000.001111**00.00000000** 10101100.00010000.001111**11.11111111**

Podtržené jsou **vypůjčené bity** k masce sítě (nebo podsítě), kterou podsíťujeme.
Cvičení:
Zadaná IP: 10.100.100.100/12 0000 1010 . 0110 **0100 . 0110** 0100 . 0110 0110
Odmaskováno maskou /12 0000 1010 . 0110 0000 . 0000 0000 . 0000 0000 => 10.96.0.0
Odmaskováno maskou /20 **0000 1010 . 0110 0100 . 0110** 0000 . 0000 0000 => 10.100.96.0
Pořadí = v zapůjčených bitech je hodnota 0100 0110 = 70.

Mějme síť (blok adres) 10.0.0.0/12, podsíťujte ji s maskou /20. Určete síťovou adresu 33. podsítě.
Podtržené jsou vypůjčené bity k masce /12 (8 bitů do masky /20).
Zadaná IP: 10.0.0.0/20 => 0000 1010 . 0000 0000 . 0000 0000 . 0000 0000
33. podstíť: 0000 1010 . 0000 **0010 . 0001** 0000 . 0000 0000 => 10.2.16.0

Mějme IP adresu 10.26.35.30/12 ležící v adresním bloku určeném maskou /12. Podsíťujte ji s maskou podsítě /20.
V jaké podsíti leží zadaná adresa (/20) vzhledem k původnímu adresnímu bloku (pořadí i adresa

sítě).

Zadaná IP: 10.26.35.30/12 0000 1010 . 0001 **1010 . 0010** 0011 . 0001 1110
Odmaskováno maskou /20 **0000 1010 . 0001 1010 . 0010** 0000 . 0000 0000 => 10.26.32.0
Pořadí = v zapůjčených bitech je hodnota 1010 0010 = 162.
Určete adresu sítě 15. podsítě.
V zapůjčených bitech je číslo 15 0000 1010 . 0001 **0000 . 1111** 0000 . 0000 0000 => 10.16.240.0

Spočtete totéž při podsíťování maskou /22:
Zadaná IP: 10.26.35.30/12 0000 1010 . 0001 **1010 . 0010 00**11 . 0001 1110
Odmaskováno maskou /22 **0000 1010 . 0001 1010 . 0010 00**00 . 0000 0000 => 10.26.32.0
Pořadí = v zapůjčených bitech je hodnota 10.10 0010 00 = 512 + 136 = 648.
Určete adresu sítě 15. podsítě.
V zapůjčených bitech je číslo 15 0000 1010 . 0001 **0000 . 0011 11**00 . 0000 0000 => 10.16.60.0

Nejvhodnější způsob výpočtu závisí na konkrétní situaci.
Lze použít i speciální podsíťové kalkulátory (*IP subnet calculator*) na webu, ale to jistě není hodné síťových specialistů.

Plánování adres v síti

Adresy nejsou uvnitř sítě předělovány náhodně, ale naopak na základě pečlivého návrhu vycházejícího z požadavků na síť kladených.

Přidělené adresy v síti by měly být plánovány a dokumentovány z následujících důvodů:

- **prevence duplikace adres** – každý hostitel uvnitř lokální sítě musí mít unikátní adresu. Bez vhodného plánování a dokumentace můžete jednu adresu přiřadit více než jednomu hostiteli.
- **poskytnutí a řízení síťového přístupu** - pokud některá zařízení poskytují své služby a zdroje uvnitř i vně lokální sítě, je bez plánování a dokumentace obtížné zajistit a spravovat zabezpečení (například blokování přístupu na server).
- **monitoring zabezpečení a výkonu sítě** – podobně potřebujeme monitorovat výkon a zabezpečení jednotlivých klientů i sítě jako celku – vhodně navržené adresy je snazší sledovat a administrovat.

Důležitou součástí plánu adresního schéma IPv4 adres je rozhodnutí, kdy a kde budou použité privátní adresy a kde veřejné adresy.

Součástí tohoto rozhodování je:

- Bude zde více do sítě připojených zařízení než máme přidělených veřejných adres od ISP?
- Budou tato zařízení dostupná z vnějšku lokální sítě?
- Jestliže zařízení s přidělenými privátními adresami vyžadují přístup do Internetu, je síť schopna poskytnout službu překladu síťových adres NAT (*Network Address Translation*)?

Jestliže máme více zařízení, než máme veřejných adres, veřejné adresy požadují pouze zařízení v lokální síti, která jsou dostupná z Internetu (jako jsou například web servery). Ostatní zařízení mohou použít službu NAT. Pokud máme pro tento účel dostatek veřejných adres je to v pořádku. Pokud není pro tento účel dostatek veřejných adres, je třeba použít službu **PAT (Port Address Translation)** na domácích (kategorie spotřebičů pro malé kanceláře a domácnost - SOHO) smě-

rovačích známo jako služba **virtuální server**.

Přiřazení adres uvnitř sítě

Hostitelé uvnitř jedné IPv4 sítě mají společnou síťovou část IP adresy. Uvnitř sítě jsou následující typy klientů (hostitelů):

- koncové zařízení pro uživatele,
- servery a síťové periferie,
- hostitelé přístupní z Internetu,
- směrovače.

Další kritéria výběru (přidělení) IP adresy jsou:

- umístění,
- oddělení, výrobní středisko,
- typ zařízení.

Statické versus dynamické přiřazení adres koncových zařízení

Statické přiřazení - ručně administrátorem. Minimální potřebné nastavení: IP adresa, maska podsítě a implicitní výchozí brána. Statické nastavení je vhodné pro směrovače, servery, síťové tiskárny (obecně je vhodné pro zařízení, které musí být přístupné ostatním zařízením v síti, a změna jeho IP adresy by činila ostatním zařízením potíže). Používá se též pro L3 adresy propojovacích zařízení (L3 switch[54]), které musí být predikovatelné.

Dynamické přiřazení – pomocí DHCP – je uzlu v síti propůjčena (na nějakou předem danou dobu) IP adresa (+ maska podsítě, implicitní výchozí brána, adresa DNS). Dynamické přiřazení je vhodné pro uživatelské počítače a mobilní zařízení (přenosná do jiných sítí). DHCP může přidělovat (propůjčovat) adresy:

- jako první volnou IP adresu z nějakého předem definovaného rozsahu (*pool*),
- na základě svojí MAC adresy má zařízení přidělovánu (staticky mapovánu) stále stejnou IP adresu (*static mapping*).

Přiřazování veřejných adres

Internet Assigned Numbers Authority (IANA) (http://www.iana.net) je hlavní držitel a registrátor IP adres. Skupinové adresy a adresy IPv6 přiděluje přímo IANA. Adresy IPv4 byly organizací IANA spravovány až do poloviny devadesátých let. V této době jsou zbývající IPv4 adresy přidělovány regionálními registrátory. Tito registrátoři se nazývají **Regional Internet Registries (RIRs)** a jsou v tabulce uvedeni podle jednotlivých regionů:

Název regionálního registrátora	***Region***	***Link***
Internet Assigned Numbers Authority (IANA)	Celosvětově	http://www.iana.net
AfriNIC (African Network Information Centre)	Afrika	http://www.afrinic.net

54 Administrativní rozhraní přepínače dostupné na všech jeho portech. L3 přepínače budeme brát ve třetím semestru.

Název regionálního registrátora	*Region*	*Link*
APNIC (Asia Pacific Network Information Centre)	Asie/Pacifik	http://www.apnic.net
ARIN (American Registry for Internet Numbers)	Severní Amerika	http://www.arin.net
LACNIC (Regional Latin-American and Caribbean IP Address Registry)	Latinská Amerika a některé karibské ostrovy	http://www.lacnic.net
RIPE NCC (Reseaux IP Europeans)	**Evropa**, Střední Východ a Střední Asie	http://www.ripe.net

Odkazy:

- Směrnice pro správu adresního prostoru IP: http://www.ietf.org/rfc/rfc1466.txt?number=1466 , http://www.ietf.org/rfc/rfc2050.txt?number=2050
- Alokace adres IPv4: http://www.iana.org/ipaddress/ip-addresses.htm
- Pod jakou IP adresou jsem vidět v Internetu (zde v Evropě, na stránkách registrátora IP adres pro Evropu): http://www.ripe.net

Cvičení

1. Nalezněte, pod jakou **veřejnou IP adresou** jste vidět na Internetu (na stránkách registrátora IP adres pro oblast Evropa: http://ripe.net/).
2. Nalezněte, komu RIPE přidělil adresní blok (Netname a Description), ve kterém se nachází server *jonatan.spse.pilsedu.cz*. Zjistěte adresní blok (inetnum), jeho velikost a kdo zodpovídá za zneužití (abuse) sítě pro tento blok (person, abuse-mailbox).
3. Prostudujte si „mapu“ školní sítě (schéma sítě spse.pilsedu.cz a okolí na Web serveru jonatan.spse.pilsedu.cz) najděte ***demilitarizovanou zónu (DMZ)***.

Poskytovatel služeb Internetu - ISP (Internet Service Provider)

Role ISP

Většina obchodních společností nebo organizací získává své adresní bloky IPv4 od ISP (*Internet Service Provider*) – Poskytovatele služeb Internetu. ISP obecně dodává malé bloky (6 nebo 14) použitelných adres IPv4 svým zákazníků jako součást svých služeb. Větší bloky adres je možné získat na základě oprávněných požadavků a za další poplatek.

ISP zapůjčuje nebo pronajímá tyto adresy organizaci. Jestliže se rozhodneme přesunout svoje připojení Internetu k jinému ISP, nový ISP nám přidělí nové adresy z rozsahu který poskytuje. Předchozí ISP IP adresy, které jsme měli dosud pronajaté, poskytne jinému zákazníkovi.

Služby ISP

Abychom získali přístup k službám Internetu, musíme připojit svoji datovou síť k Internetu prostřednictvím poskytovatele služeb Internetu (ISP).

ISP má svoje vlastní vnitřní datové sítě, aby mohl spravovat připojení k Internetu a poskytovat související služby. Mezi další služby, které ISP obvykle nabízí svým zákazníkům patří DNS, elektronická pošta, webová stránka. V závislosti na úrovni požadovaných a dostupných služeb, zákazníci používají různé vrstvy - úrovně (*tiers*) ISP.

Úrovně ISP (ISP Tiers)

ISP mají hierarchickou strukturu založenou na úrovni jejich připojeni k páteřní síti (*backbone*) Internetu. Každá nižší úroveň se k páteři připojuje prostřednictvím vyšší úrovně ISP.

Úroveň 1 - Tier 1

Na vrcholu hierarchie je ISP první úrovně. Tyto ISP jsou velké národní nebo mezinárodní ISP s přímým připojením k páteři Internetu. Zákazníky ISP první úrovně jsou také velké společnosti a organizace. Protože jsou na vrcholku připojení Internetu dosahuje vysoké spolehlivosti připojení i služeb. Mezi technologie použité k zajištění této spolehlivosti patří vícenásobná připojení k páteři Internetu.

Hlavní výhodou zákazníků ISP první úrovně je spolehlivost a rychlost. Protože tito zákazníci mají pouze jedno připojení z páteře Internetu, je zde málo příležitostí pro selhání nebo úzké místo pro provoz sítě. Nevýhodou jsou vysoké náklady.

Úroveň 2 -Tier 2

ISP druhé úrovně získává služby Internetu od ISP první úrovně. Zaměřuje se na podnikové zákazníky. Obvykle nabízí více služeb než zbývající dvě úrovně ISP. Zaměřuje se hlavně na to, aby měl zdroje, které zajišťují jeho vlastní služby jako jsou DNS, server elektronické pošty, web servery. Jiné nabízené služby jsou vývoj s správa webových stránek, elektronický obchod (*e-commerce/e-business*) a hlasové služby (*VoIP, Voice over IP*).

Hlavní nevýhodou druhé úrovně vzhledem k první úrovni je pomalejší přístup k Internetu. Protože ISP druhé úrovně mají více než jedno přípojení z páteře Internetu (ISP na stejné úrovni mohou být vzájemně propojeni = peering), mají menší spolehlivost než ISP první úrovně.

Úroveň 3 -Tier 3

ISP třetí úrovně nakupují své služby Internetu od jednotlivých ISP druhé úrovně. Zaměřují se na koncový prodej a domácnosti v jejich lokalitě. Jejich zákazníci obvykle nepotřebují tolik služeb jako zákazníci ISP druhé úrovně. Jejich hlavní potřebou je připojení a podpora.

Tito zákazníci mají často málo nebo žádné zkušenosti s počítači nebo sítěmi. IPS často své služby nabízí v balíčku služeb (síťové připojení a servis počítače). Ačkoliv mají omezenou šířku pásma, přenosovou kapacitu (*bandwidth*) a menší spolehlivost než ISP první a druhé úrovně, jsou často dobrou volbou pro malé nebo střední společnosti.

Poznámka: někdy je páteřní síť Internetu označována jako nultá úroveň ISP.

Několik příkladů rozvrstvení ISP v ČR:

tier0 – úroveň 0 *Páteřní ISP (USA)*	*tier1 – úroveň 1* *Nadnárodní ISP*	*tier2 – úroveň 2* *Národní ISP*	*tier3 – úroveň 3* *Lokální ISP*
Sprint	Global One	Bohemia.Net	CL-NET
Sprint	Global One	PVT Net	-
Sprint	Teleglobe	SPT Telecom	Internext 2000
MCI WorldCOM	EBONE (GTS Retail Services)	CESNET	-
MCI WorldCOM	-	Inway	-
AT&T Unisource	-	LUKO Czech Net	Sever NET

Propojení (*peering*) ISP na národní (i mezinárodní) úrovni probíhá přes IXP (Internet eXchange Point) - v ČR přes NIX.CZ (NIX.CZ – Neutral Internet eXchange).

Testování na síťové vrstvě

- Testování vždy provádíme postupně po jednotlivých vrstvách OSI modelu odspodu nahoru – to znamená od 1. vrstvy do 7. vrstvy. (Tedy nejprve testujeme kabely a pak nakonec funkci aplikací. Zatím známe pouze utility pracující na L3.)
- **Ipconfig /all** – otestuje přítomnost kabelu v síťové kartě i **funkci a nastavení síťové karty**.
- **Ping 127.0.0.1** – pinknutí na adresu lokální zpětné smyčky – test korektní lokální instalace a funkce sady TCP/IP (funkce protokolu IP) a komunikace síťové karty s OS počítače.
- **Ping <adresa implicitní brány>**, eventuálně pinknutí na jiného lokálního hostitele (v LAN) - test propojení uvnitř LAN – zapojený a fungující switch v přepínané síti.
- **Ping <adresa vzdáleného hostitele>** - propojení z LAN do jiné (vzdálené) sítě, správná konfigurace bránového směrovače, funkce celé trasy na cestě do cílového zařízení.
- **Traceroute <adresa vzdáleného hostitele>** – tracert – výpis směrovačů na cestě do vzdáleného zařízení.
- Kontrola obsahu zprávy ICMP.

Cvičení

Laboratorní cvičení (Lab) 6.7.5 + jeho realizace v Packet Traceru (úplně vše od počátku)

Varianta cvičení - adresní schéma CIDR

Cílem tohoto cvičení není naučit se jak se nastavuje směrovač, ale co vše se musí minimálně nastavit. Nejprve si vypočtěte potřebnou masku podle zadaný požadavků (**je stejná pro všechny sítě => CIDR**) a adresy portů vyhovující zadání. Potom v PT na plochu (*Logical Workspace*) vyberte potřebné aktivní prvky, přidejte do nich (ve vypnutém stavu!) zásuvné moduly s potřebnými rozhraními (použijte modul WIC-2T, *Cisco 2 Serial Port **W**AN **I**nterface **C**ard, WIC = WAN Interface Card*) a propojte odpovídajícími kabely. Zatím neumíme nastavení sériové linky (na straně DCE

musí být nastaveny hodiny). Nastavte statické směrování na R1 a R2. Ověřte funkčnost. Prohlédněte si použité protokoly na L2 (Ethernet II a HDLC).

Před začátkem každé práce v Packet Traceru (i v reálné síti) si vždy:

1. **dejte dohromady všechny požadavky kladené na síť a zásady (politiky) pro přidělování adres v dané firmě,**
2. **vypočtěte a vyplňte tabulku přiřazených IP adres k jednotlivým rozhraním,**
3. **nakreslete schéma topologie sítě, kde doplňte názvy jednotlivých rozhraní, IP adresy a masky jednotlivých rozhraní a čísla (adresy) celých sítí podle zadání.**
4. **zapojujte pečlivě podle tohoto diagramu. Pozor na špatné zapojení kabelů v nesprávných (tj. jiných než si myslíte) portech.**

Zadané požadavky:
Máte pro návrh vaší sítě zadán adresní prostor 192.168.1.0/24 (privátní rozsah, síť). Síť se skládá z následujících segmentů (podsítí):

- Síť připojená ke směrovači R1 bude požadovat dostatek adres pro 15 hostitelů.
- Síť připojená ke směrovači R2 bude požadovat dostatek adres pro 30 hostitelů.
- Spojení mezi směrovači R1 a R2 požaduje IP adresy pro oba konce linky.

Přiřazení adres podsítí do schéma topologie:
Podsíť 1 je přiřazena k síti připojené k R1.
Podsíť 2 je přiřazena k propojovací lince mezi R1 a R2.
Podsíť 3 je přiřazena k síti připojené k R1.
Určení IP adres rozhraní:
Rozhraní LAN na R1 – první platná adresa hostitele v podsíti 1.
PC1 – poslední platná adresa hostitele v podsíti 1.
Rozhraní WAN na R1 – první platná adresa hostitele v podsíti 2.
Rozhraní WAN na R2 – poslední platná adresa hostitele v podsíti 2.
Rozhraní LAN na R2 – první platná adresa hostitele v podsíti 3.
PC2 – poslední platná adresa hostitele v podsíti 3.

Nejprve určíme potřebnou masku:
Kolik je podsíti? =>3+2=5 je nutno vypůjčit 3 bity k masce /24 (s tím pokryjeme 6 podsítí, 8-2=6).
Kolik je hostitelů v největší podsíti: 30 (+2) => 32 = 2^5 - je nutno mít pro jejich adresaci 5 bitů nad maskou podsítě.
Z toho vychází (32-5) maska */27 = 255.255.255.224.*
Adresy sítí a všesměrového vysílání pro jednotlivé sítě odleva:

- *192.168.1.32 – 192.168.1.63,*
- *192.168.1.64 – 192.168.1.95,*
- *192.168.1.96 – 192.168.1.127.*

Ze zadání je potom možné vyplnit (*zobrazeno kurzívou*) následující tabulku:

Zařízení *Device*	*Rozhraní* *Interface*	*IP adresa* *IP Address*	*Maska podsítě* *Subnet Mask*	*Výchozí brána* *Default Gateway*
R1	Fa0/0	*192.168.1.33*	*255.255.255.224*	*N/A*
	S0/0/0	*192.168.1.65*	*255.255.255.224*	*N/A*
R2	Fa0/0	*192.168.1.97*	*255.255.255.224*	*N/A*
	S0/0/0	*192.168.1.94*	*255.255.255.224*	*N/A*
PC1	NIC	*192.168.1.62*	*255.255.255.224*	*192.168.1.33*
PC2	NIC	*192.168.1.126*	*255.255.255.224*	*192.168.1.97*

Postup práce:

Použijte následující aktivní prvky: Switch 2950-24, Router 1841, generic PC.

Do každého routeru přidejte (ve „vypnutém“ stavu) zásuvný modul WIC-2T se **dvěma synchronními sériovými porty**.

Propojení proveďte následujícími kabely:

- router (sériový port) - router (sériový port) = **sériový (serial) kabel** (POZOR - je nesymetrický na straně DCE („samice“ (*Female)* konektoru V.35) je třeba nastavit hodiny),
- switch - PC a switch - router (dvě logicky různá zařízení DCE – DTE) = **přímý UTP (straight) kabel**,
- router – PC (dvě logicky stejná zařízení DTE – DTE) = **překřížený (crossover) UTP kabel**.

Na klientu je třeba nastavit IP adresu síťové karty, masku podsítě a implicitní bránu.

Na směrovači je třeba nastavit IP adresu a masku rozhraní a rozhraní zapnout. Na straně DCE sériového kabelu je třeba na sériovém rozhraní nastavit hodiny (= takt hodin, *clock rate*).

Na každém směrovači je třeba dále nastavit statickou cestu pro vzdálenou síť (podsíť) (= *remote network*), která není přímo připojená (*directly connected*), router o této síti „neví“. (Přímo připojené sítě musíte při správném nastavení vidět ve směrovací tabulce (**Inspection**).)

Nastavení statické cesty:

Statické směrování (hodnoty pro levý směrovač R1):

- adresa cílové sítě *(192.168.1.96)*,
- maska podsítě *(255.255.255.224)*,
- next hop (= IP adresa vstupního portu do následujícího směrovače na cestě (route) ve správném směru (*direction*) do cílové sítě *(192.168.1.94)*.

Po nastavení (konfiguraci sítě) VŽDY OVĚŘTE:

- **na každém směrovači ve směrovací tabulce opravdu vidíte všechny sítě z celé skupiny sítí. (Pokud nejsou vidět – nejsou ve směrovací tabulce, nebude to fungovat!)**
- **před nastavením směrování musíte na každém směrovači ve směrovací tabulce vidět všechny přímo připojené sítě (*directly connected*).**
- **Otestujete dosažitelnost vzdálených hostitelů: ping, tracert a prozkoumejte v simulačním režimu protokoly na vrstvě L2.**
- **Pokud nefunguje – ověřte zapojení kabelů (L1) a dále postupujte nahoru po jednotlivých vrstvách OSI modelu: L1, L2, L3 a L7.**

Podívejte se na „fyzické“ zapojení racků a stohovacích routerů a switche = **Physical Workspace**.

Rozšířená varianta předchozího cvičení (VLSM)

Stejné schéma zapojení. Použijeme VLSM (tedy různé masky a velikosti podsítí). Máme všechny

adresy přidělovat v bloku privátních adres 192.168.0.0/16. Spojovací síť má obsahovat pouze 2 klienty (dva konce sériové linky) a mají to být nejnižší použitelné adresy. Určete adresu sítě/masku a rozsah adres klientů. *(192.168.0.0/30, 192.168.0.1 – 192.168.0.2)* Síť připojená ke směrovači R2 má obsahovat 30 klientů. Určete totéž. *(192.168.0.32/27, 192.168.0.33-192.168.0.62)* Síť připojená ke směrovači R1 má obsahovat 250 klientů. Určete totéž. *(192.168.1.0/24, 192.168.1.1-192.168.1.254).* ***POZOR: bloky adres se nesmějí vzájemně překrývat!!!***

Navrhněte statické směrování a zapište si obsah směrovacích tabulek.

Po dokončení uvažte následující: přes R2 a další sériovou linku se připojíme do Internetu. Potom provoz uvnitř privátní sítě funguje, ale provoz do Internetu ne. Kde je problém? Co je je ještě třeba?

1. *Nastavit implicitní cestu do odchozího portu do Internetu.*
2. *Nakonfigurovat na směrovači R2 „IP maškarádu“ = NAT.*

IPv6 – stručný přehled

Na počátku devadesátých let začalo být Internet Engineering Task Force (IETF) znepokojené vyčerpáním adres IPv4, a začalo připravovat náhradu tohoto protokolu. Tyto aktivity vedly vytvoření toho, co je dnes známo jako IPv6.
Hlavní motivací pro vývoj nového protokolu bylo **rozšíření adresního prostoru**. Dále byly při vývoji vzaty do úvahy ještě další aspekty jako jsou:

- zlepšení manipulace s pakety,
- zvýšená rozšiřitelnost a dlouhodobá použitelnost,
- kvalita služeb (QoS),
- integrované zabezpečení.

Za tímto účelem IPv6 nabízí:

- 128-bitovou hierarchickou adresaci – **rozšíření adresního prostoru**,
- zjednodušení formátu záhlaví – zlepšení manipulace s pakety,
- podpora rozšíření a volitelných nastavení – zvýšení rozšiřitelnosti a dlouhodobé použitelnosti, zlepšení manipulace s pakety,
- návěsti pro řízení toku dat – jako mechanismus zajišťující kvalitu služeb (QoS) rozdělováním služeb do tříd a řazením do front,
- autentizace a utajení dat – integrované zabezpečení.

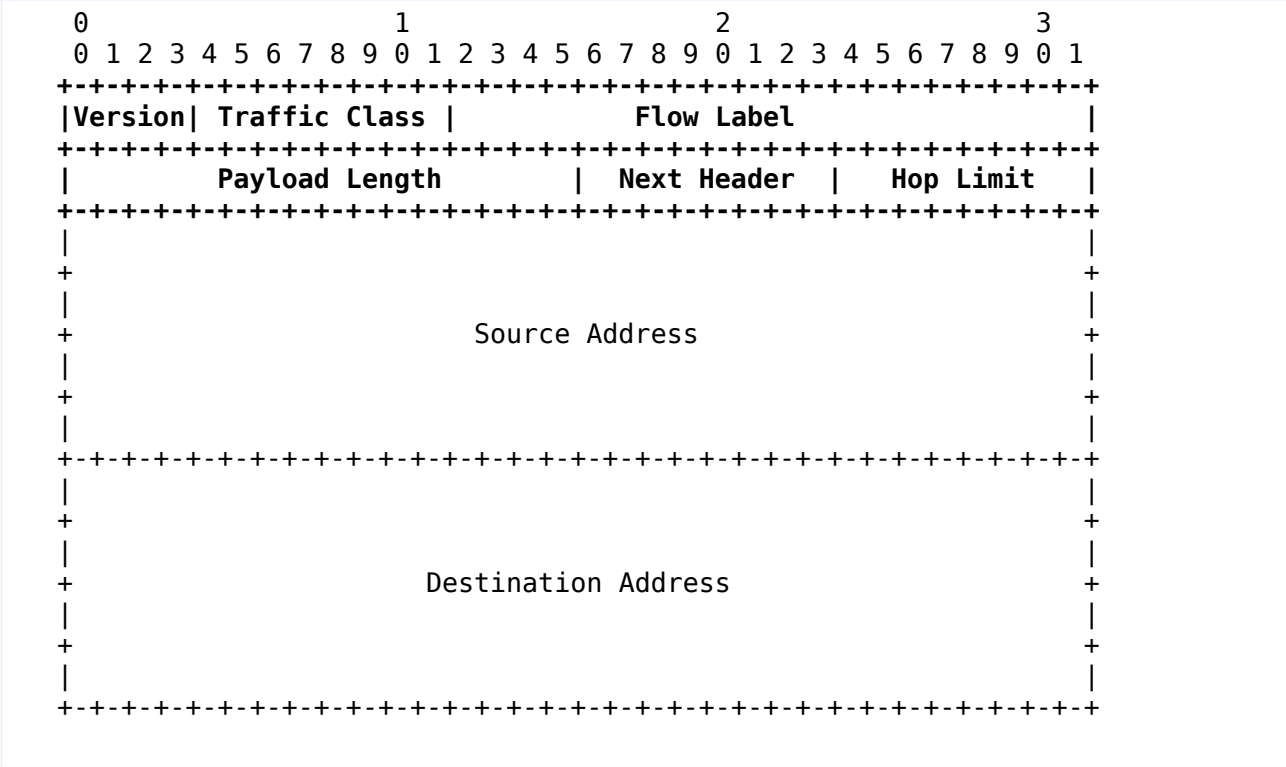
IPv6 není pouze nový L3 protokol – je to nová protokolová sada. Obsahuje protokoly různých vrstev: Je zde nový protokol zpráv (ICMPv6) a nové směrovací protokoly. Protože se zvětšila velikost záhlaví má to vliv i na síťovou infrastrukturu.

Přechod na IPv6

Jak jste viděli, je IPv6 navržen pro dlouhodobé použití v rozvíjejících se sítích. Nicméně IPv6 se implementuje pomalu a pouze na vybraných sítích. Kvůli lepším nástrojům, technologiím a lepší správě adres v posledních několika letech zůstává IPv4 stále široce rozšířen a pravděpodobně ještě zůstane po nějaký čas i v budoucnosti. Avšak IPv6 může eventuálně nahradit IPv4 jako dominantní protokol Internetu.

Linky:
IPv6: http://www.ietf.org/rfc/rfc2460.txt?number=2460
IPv6 addressing: http://www.ietf.org/rfc/rfc3513.txt?number=3513
IPv6 security: http://www.ietf.org/rfc/rfc2401.txt?number=2401
IPv6 security: http://www.ietf.org/rfc/rfc3168.txt?number=3168
IPv6 security: http://www.ietf.org/rfc/rfc4302.txt?number=4302
ICMPv6: http://www.ietf.org/rfc/rfc4443.txt?number=4443

IPv6 - hlavička



- **Version** - 4-bitové pole Číslo verze Internet Protocol = 6,
- **Traffic Class** - 8-bitové pole Priorita (priorita vzhledem k datagramům ze stejného zdroje - QoS),
- **Flow Label** - 20-bitové Označení datového toku,
- **Payload Length** – 16-bitové pole Délka dat v datagramu (v oktetech),
- **Next Header** – 8-bitové pole Následující záhlaví, identifikuje typ záhlaví bezprostředně následující za povinným záhlavím IPv6,
- **Hop Limit** - 8-bitové pole Maximální počet směrovačů, povolený počet zbývajících směrovačů na cestě, obdoba TTL u Ipv4, který každý směrovač na cestě sníží o jedničku (pokud dospěje k hodnotě 0, nesmí datagram předat dál a musí vygenerovat zprávu ICMP),
- **Source Address** - 128-bitová Zdrojová adresa datagramu,
- **Destination Address** - 128-bitová adresa zamýšleného příjemce paketu (v některých případech se nemusí jednat o cílovou stanici, pokud se používá rozšířené směrovací záhlaví).

Zdroj: RFC 2460.

Adresa IPv6 je 128-bitové binární číslo (16 oktetů) obvykle zapsané jako osm skupin čtyř hexadeci-

málních znaků = 16-ti bitů (jako např. **2001:0db8:0000:0000:0000:0000:1428:57ab**). Dvě dvojtečky (::) mohou nahradit skupinu po sobě následujících nul (např.: **2001:db8::1428:57ab**). V jedné adrese může být pouze jedna dvojitá dvojtečka (jinak je adresa neplatná).
Adresní prostor je 2^{128} = $3.4x10^{38}$ unikátních adres. Poznámka pro představu: Tolik má např. $30km^3$ železa přibližně celkem elementárních částic.

Kontrolní opakovací otázky a odpovědi (kvíz):

1) Dva rozdíly mezi binárními a dekadickými čísly:
   a) Binární čísla jsou založena na mocninách 2 a dekadická na mocninách 10.
   b) Počítače používají binární číselnou soustavu a lidé obvykle desítkovou.
2) Dva počítače s adresami 192.168.100.105/26 a 192.168.100.99/27, připojené k jednomu přepínači, se vzájemně „nedopinknou“. Jaká je možná příčina?
   a) Chybně vložené masky podsítě (=> jsou různé masky a počítače mají být v jedné síti, protože je mezi nimi switch)
3) Administrátor úspěšně pinknul na adresu 127.0.0.1. Co je to za typ adresy?
   a) Loopback (= lokální zpětná smyčka)
4) Jakou část IP adresy reprezentuje prefix?
   a) Síťovou část IP adresy
5) Co je pravda ohledně adresy sítě?
   a) Všechny hostitelské bity jsou nastaveny na 0.
6) Jaký typ adresy má všechny hostitelské bity nastaveny na 1?
   a) broadcast (všesměrové (oběžníkové) vysílání)
7) Kolik binárních číslic má adresa v protokolu IPv6?
   a) 128
8) Jaký je primární důvod zavádění protokolu IPv6?
   a) Rozšíření adresního prostoru (počtu adres)
9) Následující adresy leží v jedné podsíti: 192.168.223.99, 192.168.223.107, 192.168.223.117 a 192.168.223.127. Tři pravdivá tvrzení[55]:
   a) mají 27 společných bitů odleva,
   b) odpovídající maska je 255.255.255.224,
   c) 192.168.223.127 je všesměrová adresa pro danou síť.
10) Spárujte IP adresu a její popisek:
   a) 192.168.16.192/30 = dvě použitelné adresy v jedné podsíti s maskou /30,
   b) 172.16.64.98/23 = celkem 512 adres v jedné podsíti,

55 Rozdíl hodnot v posledním bajtu 127-99=28 nejbližší mocnina 2 je $32=2^5$ => 32 - 5 = /27, velikost bloku 0.0.0.32.

c) 172.16.125.6/20 = 4 vypůjčené bity nad implicitiní masku třídy B /16 (z třídní podsítě),

d) 192.168.1.1/24 = síť v plné třídě (*classful network*),

e) 172.31.16.128/19 = 8 podsítí sítě v plné třídě.

Kapitola 7 – Spojová vrstva

V této kapitole se naučíme:

- Vysvětlit roli protokolů spojové (linkové) vrstvy při přenosu dat.
- Popsat jak spojová vrstva připravuje data pro přenos přes síťové médium.
- Popsat rozdílné metody řízení přístupu k médiu.
- Identifikovat jednotlivé běžné logické topologie sítí a popsat jak logická topologie určuje metodu přístupu k médiu pro tuto síť.
- Vysvětlit účel zapouzdřování paketů do rámců k zajištění přístupu k médiu.
- Popsat strukturu rámce na druhé vrstvě a identifikovat všeobecně používaná pole.
- Vysvětlit roli klíčových polí záhlaví a zápatí, včetně adresních, QoS, typu zapouzdřeného protokolu a kontrolního součtu rámce (FCS).

Rekapitulace:

- Aplikační vrstva poskytuje rozhraní uživateli.
- Transportní vrstva odpovídá za rozdělení a řízení komunikace mezi procesy běžícími na dvou koncových systémech.
- Protokoly síťové vrstvy organizují komunikující data tak, aby mohly cestovat mezi propojenými sítěmi (*internetworks*) ze zdrojového do cílového hostitelského počítače.

Pakety (ze třetí vrstvy) přenášené ze zdrojového hostitele do cílového hostitele musí procházet různými fyzickými sítěmi. Tyto fyzické sítě se skládají z různých druhů fyzických (přenosových) médií, jako jsou měděné dráty, mikrovlny, optická vlákna nebo satelitní linky. Pakety síťové vrstvy nemají žádný způsob přímého přístupu k těmto různým přenosovým médiím.

Role spojové vrstvy OSI:

- připravit pakety ze síťové vrstvy (L3) pro přenos médiem (zapouzdření (framing) paketu do rámce, přidání záhlaví (*header*) a zápatí (*trailer*) k přenášeným (*payload*) datům) => oddělení vyšších vrstev, konkrétně síťové vrstvy, od konkrétní síťové technologie a přenosového média (IP paket zůstává cestou mezi sítěmi nezměněn (nemění se cílová ani zdrojová IP adresa, pouze se zmenšuje doba života a kontrolní součet záhlaví).
- a řízení přístupu k fyzickému (přenosovému) médiu.

Spojová vrstva – podpora služeb vyšších vrstev – přístup k médiu

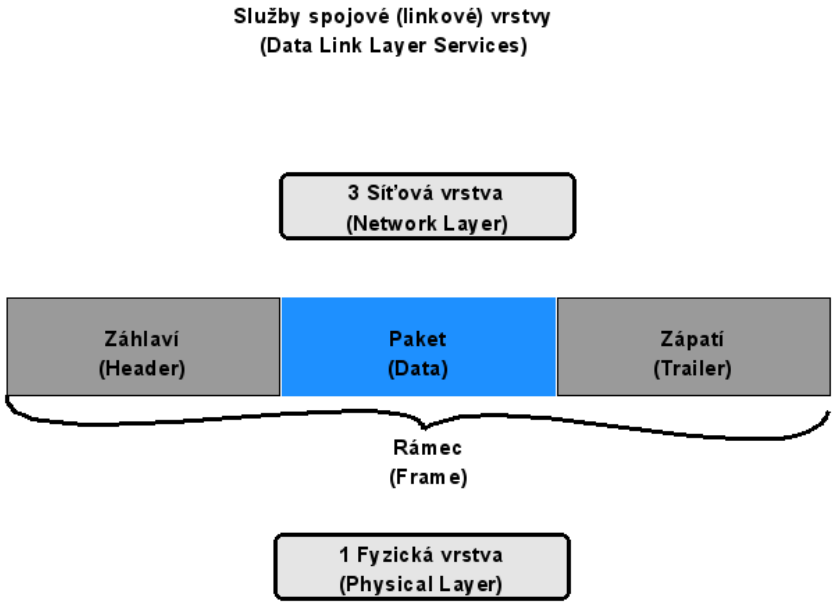
Spojová (linková) vrstva[56] (*Data Link Layer*) zajišťuje prostředky pro výměnu dat přes sdílené lokální přenosové médium.

Spojová vrstva poskytuje **dvě základní služby**:

- dovoluje vyšším vrstvám přistupovat k médiu pomocí **zapouzdřování do rámce (*framing*)**,

56 Používá se též termín spojová vrstva.

- **řídí předávání a přijímání dat na a z média**, použitím technik jako jsou:
  - **řízení přístupu k médiu** (*media access control*),
  - **detekce chyb** (*error detection*).



Termíny specifické pro L2:

- **Rámec (*Frame*)** – L2 PDU,
- **Uzel (*Node*)** – L2 označení pro síťové zařízení připojené ke sdílenému médiu (common medium),
- **(Fyzické) (*přenosové*) médium**[57] **(*Media/medium (physical)*)** – fyzické prostředky pro přenos informací mezi dvěma uzly.
- **(Fyzická) síť (*(physical) network*)**[58] – dva nebo více uzlů připojené na sdílené médium.

Spojová vrstva je odpovědná za výměnu rámců (*Frames*) mezi uzly (*Nodes*) prostřednictvím přenosového média fyzické sítě (síťového segmentu).

57 Je důležité si uvědomit význam slova **médium** v kontextu této kapitoly. Zde to odkazuje na materiál, který skutečně přenáší signály, které reprezentují přenášená data. Médium je fyzický měděný kabel, optické vlákno nebo atmosféra, přes které signály cestují. V této kapitole médium (média) neodkazují na programový obsah dat jako audio, animace, TV a video jak jsou použita, když se odkazuje na digitální obsah a multimédia.

58 Fyzická síť se liší od logické sítě. Logická síť je definována na síťové vrstvě soustavou hierarchického adresního schéma. Fyzická síť je reprezentována propojením zařízení na společném sdíleném médiu, Někdy se také fyzické síti říká **síťový segment** (*network segment*).

Spojová vrstva – řízení přenosu dat přes přenosové médium

Metody přístupu k médiu (přístupové metody) (*media access control methods*), které jsou popsány protokoly spojové (linkové) vrstvy, definují procesy pomocí kterých mohou síťová zařízení přistupovat k přenosovému médiu a přenášet datové rámce v různých síťových prostředích.

Například obsah rámce (v jednom protokolu spojové vrstvy) ze sítě LAN je na směrovači „rozbalen“ do paketu a opětovně zapouzdřen do rámce (v jiném L2 protokolu) pro přenos v síti WAN.

Vytvoření rámce na spojové vrstvě

Popis formátu rámce je klíčovým prvkem každého protokolu spojové vrstvy. Spojová vrstva připravuje data v paketu pro přenos přes lokální přenosové médium. K přenášeným datům (data) (=L3 paketu) je při zapouzdření na spojové vrstvě přidáno záhlaví (*header*) a zápatí (*trailer*).

Protokol spojové vrstvy požaduje pro svou činnost určité řídicí informace, které mu řeknou:

- které uzly (*nodes*) spolu komunikují,
- kdy komunikace mezi jednotlivými uzly začíná a kdy končí,
- které chyby se vyskytly během komunikace uzlů,
- které uzly budou komunikovat příště (v následující komunikaci).

Na rozdíl od jiných PDU, které jsme diskutovali v tomto kurzu, rámec spojové vrstvy obsahuje:

- **Data** – paket ze síťové vrstvy,
- **Záhlaví (*header*)** – obsahuje řídící informace jako jsou adresace, typ zapouzdřené L3 PDU, ... je umístěno na začátku PDU,
- **Zápatí (*trailer*)** – obsahuje kontrolní informace přidané na konec PDU.

Formátování dat před přenosem

Data jsou pro přenos pře médium konvertována do toku bitů (*bit stream*), nul a jedniček. Když uzel přijímá dlouhý proud bitů, jak určí, kde rámec začíná a končí, kde začíná adresa?

Seskupování bitů (*framing*) rozkládá jednolitý tok do dešifrovatelných skupin, s řídicími informacemi vloženými do záhlaví a zápatí jako hodnoty různých polí. Tento formát určuje fyzické signály struktury, které mohou být přijaty uzly a dekódovány do paketů v místě určení (cíli).

Typické typy polí rámce:

- Pole indikující začátek a konec (*Start and stop indicator fields*) – začátek a konec vymezující rámec (jde o, pro daný formát rámce, specifickou posloupnost bitů (*bit pattern*)),
- Jmenná nebo adresní pole (*Naming or addressing fields*),
- Pole typu (*Type field*) – typ PDU, který je přenášen v rámci,
- Kvalita (*Quality*) – pole pro řízení (přenosu, kvality),
- Pole Data – přenášená data (*payload data*) v rámci (L3 paket).

Pole na konci rámce vytváření zápatí (*trailer*). Tato pole jsou použita pro detekci chyb (pomocí

kontrolního součtu CRC) a označují konec rámce (opět jde o specifickou posloupnost bitů).

Kontrolní součet je z rámce vypočten před vysíláním a vložen do zápatí přenášeného rámce, po jeho přijetí je kontrolní součet znovu stejným způsobem vypočten a potom porovnán s hodnotou kontrolního součtu vloženého do zápatí rámce. Pokud obě tyto hodnoty nejsou stejné, je rámec odložen (zahozen).

Ne všechny protokoly obsahují všechna tato pole. Standardy pro konkrétní protokol spojové vrstvy definují skutečný formát rámce. Na konci kapitoly budou diskutovány příklady formátů rámců.

Síťová karta

Vlastní připojení vyšších vrstev k přenosovému médiu je prostřednictvím (v případě použití technologie Ethernet - Ethernetové) **síťové karty (*Network Interface Card – NIC*)**. NIC funguje na obou vrstvách L1 i L2. Spravuje přístup k médiu, zapouzdřuje L3 do rámce na L2, adresuje na fyzické adrese L2, rámec zakóduje a vysílá na přenosové médiu. Na druhém (cílovém) uzlu provede opětné dekódování a odpouzdření do L3.

Síťová karta má v paměti EPROM zapsánu svoji (L2) **hardwarovou fyzickou adresu (MAC adresu)**. MAC adresa je 48-mi bitová, obvykle zobrazovaná v hexadecimálním tvaru jako 6 bajtů (00-04-75-F1-A3-C1). První tři bajty zleva tvoří Organizationally Unique Identifiers (OUI), což je identifikátor výrobní organizace registrovaný IEEE.

Poznámka:

- ***MAC adresa má plochou strukturu,** z MAC adresy, kromě kódu výrobce (OUI) nevyčtete žádnou další informaci jako je například konkrétní LAN, umístění atd. Na rozdíl od IP adresy.*
- ***IP adresa má hierarchickou strukturu**, určitá síť je podsítí nadřazené sítě, hostitelé v jedné síti mají stejnou síťovou část IP adresy. Síťovou část IP adresy určíte odmaskováním (logický součin = AND) maskou podsítě.*

Cvičení

Určete výrobce síťové karty z MAC adresy. V příkazové řádce **ipconfig /all**. **První 3 oktety MAC adresy** zadejte do databáze OUI (na stránkách IEEE). Odkaz: http://standards.ieee.org/regauth/oui/index.shtml Například pro OUI= 00-04-75 zjistíme výrobce: 3 Com Corporation.

ARP

Adress Resolution Protocol. V rámci lokální sítě (síťového segmentu) se data přesouvají na úrovni druhé vrstvy (MAC adresy). Při použití IP adresy musí systém nejdříve převést IP adresu na MAC adresu pomocí ARP protokolu. Uzel vydá žádost *ARP request* jako broadcast. Uzel z požadovanou IP adresou jako unicast zašle zpět svoji MAC adresu. Tyto překlady jsou na uzlu uloženy ve vyrovnávací paměti ARP cache v RAM. Výpis v příkazovém řádku:

- klient: **arp -a**,
- směrovač: **Router#show arp**.

Cvičení

Vypište vyrovnávací paměť pro protokol ARP: v příkazové řádce **arp -a**. Zjistěte MAC adresu svého souseda v síti. (Při znalosti jeho IP adresy.)

Spojová (linková) vrstva – podvrstvy

Protože podporuje široké spektrum síťových funkcí je spojová vrstva obvykle rozdělena do dvou podvrstev. Horní podvrstva definuje SW procesy, které poskytují služby protokolům síťové vrstvy. Spodní podvrstva definuje HW procesy pro přístup k fyzickému přenosovému médiu. Rozdělením spojové vrstvy na dvě podvrstvy umožňuje jednomu typu rámce, definovanému na vyšší podvrstvě přistupovat k různým typům média na spodní podvrstvě. Jako je tomu v mnoha technologiích LAN, včetně Ethernet.

Dvě obvyklé **podvrstvy spojové vrstvy** LAN jsou:

- ***Logical Link Control (LLC)*** – identifikuje v rámci, který protokol síťové vrstvy bude použit pro tento rámec. Zapouzdřuje L3 paket do L2 rámce a tak umožňuje různým síťovým (L3) protokolům (jako jsou IP a IPX) použít stejnou síťovou kartu a přenosové médium.
- ***Media Access Control (MAC)*** – poskytuje L2 (fyzickou) adresaci (adresuje rámec) a vymezuje data (označuje začátek a konec dat) v závislosti na požadavcích fyzického přenosu dat konkrétním médiem a na typu použitého L2 protokolu. Rámec je zakódován do signálu pro přenos fyzickým přenosovým médiem.

Spojová vrstva – standardy

Některé z těchto standardů zahrnují vrstvy L2 i L1.

Standardizační organizace	Standard
International Organization for Standardization (ISO)	**HDLC** (High Level Data Link Control)
Institute of Electrical and Electronics Engineers (IEEE)	802.2 (LLC) **802.3 (Ethernet)** **802.5 (Token Ring)** **802.11 (WLAN)**
International Telecommunication Union (ITU)	Q.922 (**Frame Relay** L2 Standard) Q.921 (ISDN L2 Standard) HDLC (High Level Data Link Control)
American National Standards Institute (ANSI)	3T9.5 ADCCP (Advanced Data Communication Control Protocol)

Linky:

http://www.iso.org

http://www.ieee.org

http://www.ansi.org

http://www.itu.int

Přístupové metody

Regulace umísťování datových rámců na přenosové médium je známa jako řízení přístupu k přenosovému médiu (media access control).
Metoda řízení přístupu k médiu závisí na:

- **sdílení média** – jestli a jak uzly sdílí médium,
- **topologii** – jak se spojení mezi uzly jeví spojové vrstvě (=> logická topologie).

Přístupové metody ke sdílenému médiu

V některých síťových topologiích je médium sdíleno více uzly. V jedné chvíli může být více uzlů, které se pokoušejí vysílat a přijímat dat prostřednictvím média.
Existují dvě základní metody řízení přístupu ke sdílenému médiu:

- Řízený přístup (deterministická) – každý uzel má svůj čas přístupu k médiu.
- Konkurenční přístup (nedeterministická) – všechny uzly soutěží o použití média.

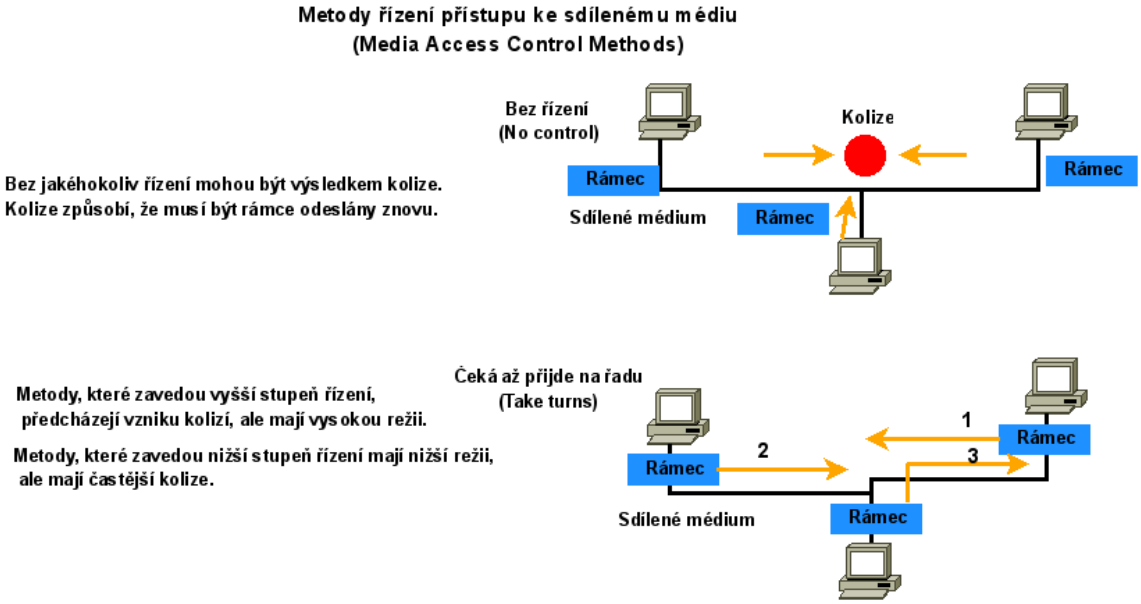
Přístupová metoda	***Charakteristiky***	***Příklad***
Deterministická (řízený přístup) (*deterministic/controlled*)	V jedné chvíli může vysílat pouze jedna stanice. Stanice, která chce vysílat, musí počkat na to, kdy přijde na řadu (*take turn*). Nejsou kolize. Některé deterministické sítě používají metodu *token passing* (= předávání tokenu/známky/žetonu/peška).	Token Ring FDDI
Nedeterministická (soupeření o přístup) = náhodná (*random/stochastic*)	Stanice mohou vysílat kdykoliv. (Nebo se o to pokusit.) Vznikají kolize. Soupeření je řešeno metodou: • CSMA/CD[59] (Ethernet) • CSMA/CA (WLAN) Jsou efektivnější, mají menší režii, než deterministické metody.	Ethernet WLAN (WiFi)

Přístupové metody pro nesdílené přenosové médium

Pro médium, které není sdíleno, není třeba žádné (nebo je třeba jen velmi malé a jednoduché) řízení přístupu. To nastává v případě topologie dvoubodového spojení (*point-to-point*). V tomto případě k médiu přistupují pouze dva uzly.[60]

59 Carrier Sense Multiple Access / Collision Detection – Metoda naslouchání nosné, vícenásobného přístupu a detekce kolizí používaná Ethernetem. Ve WiFi je přístupová metoda (v Ethernet CSMA/**CD**) upravena na CSMA/**CA** = Collision Avoidance – předcházení kolizím.

60 Například při použití přepínaného Ethernetu switch (přepínač) vytváří pro konkrétní rámec virtuální dvoubodové spojení mezi uzly a je možné použít (při současném vypnutí přístupové metody CSMA/CD) plný duplex (full-duplex).



Full Duplex a Half Duplex

- ***Half Duplex*** – Poloviční duplex - obě zařízení mohou buď vysílat nebo přijímat data, ale nikoliv ve stejné chvíli (ne simultánně). Stanice musí s vysíláním rámce počkat, dokud neskončí vysílání dat z jiné stanice. Například technologie Ethernet má vytvořené pravidla (přístupová metoda CSMA/CD) pro řešení konfliktů vyplývajících z pokusu více než jedné stanice vysílat ve stejný čas.
- ***Full Duplex*** – Duplexní (plný duplex) - obě zařízení mohou zároveň vysílat a přijímat data. Není nutné žádné vyjednávání o médiu. (Virtuální dvoubodové spojení = **mikrosegmentace na přepínači** (*switch*)). Lze použít pouze na přepínači a nikoliv na rozbočovači. Při zapnutí plného duplexu se vynutí vypnutí přístupové metody (CSMA/CD) na síťové kartě.

Logická topologie versus fyzická topologie

Topologie sítě je uspořádání nebo vztah síťových zařízení a propojení mezi nimi. Topologie sítě mohou být nahlíženy na fyzické nebo na logické úrovni.

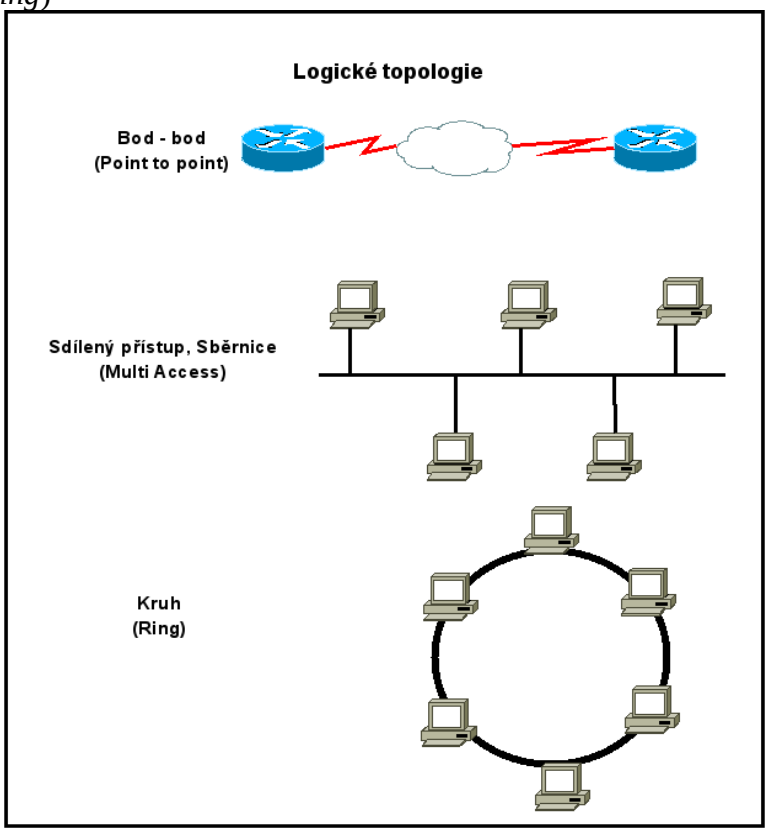
- **Fyzická topologie** je uspořádání uzlů a fyzického propojení mezi nimi. („Jak jsou zapojeny dráty.“) Například: dvoubodový spoj (*point to point*), hvězda (*star*), lineární sběrnice (*bus*), topologie s nadbytečnými (redundantními) spoji (*mesh*).
- **Logická topologie** je způsob, jak síť přenáší rámce z jednoho uzlu na další. Toto uspořádání závisí na **virtuálních spojeních mezi uzly** a **je nezávislé na jejich fyzickém uspořádání**. Tyto logické cesty signálu jsou definovány protokoly spojové vrstvy. Spojová vrstva „vidí“ logickou topologii sítě, když řídí přístup dat na přenosové médium. (Logická topologie je složena z jednotlivých virtuálních dvoubodových spojů.) Je to logická topologie, která má vliv na to, který typ rámců a přístupové metody je použit.

Fyzická (nebo kabelová) topologie v jedné konkrétní síti nejpravděpodobněji **není stejná** jako její

logická topologie[61].

Logické a fyzické topologie typicky používané v sítích jsou:

- **Dvoubodové spojení** (*Point-to-Point*)
- **Vícenásobný přístup** (*Multi-Access*) = lineární sběrnice (*Bus*) = sdílené médium (*shared physical medium*)
- **Kruhová** (*Ring*)



Topologie dvoubodového spojení (point to point)

Topologie *point-to-point* (dvoubodové spojení) **spojuje přímo pouze dva uzly**. Potom může být přístupová metoda velmi jednoduchá (s malou režií). Rámce mohou totiž skončit pouze na druhém konci přenosového média u druhého uzlu (v rámci okruhu – obvodu point to point).

- Jestliže ve dvoubodovém spojení mohou data téci v jedné chvíli pouze jedním směrem, pracuje jako linka **poloviční duplex (*half-duplex*)**.
- Pokud mohou data téci oběma směry simultánně, jde o linku **plný duplex (*full-duplex*)**.

V případě logické topologie point to point je vytvářeno **virtuální dvoubodové spojení (okruh)**.

Topologie vícenásobného přístupu (multi access)

Sdílené médium.Více uzlů sdílí přenosové médium (topologie lineární sběrnice). S ohledem na to je

61 Příklad rozdílu logické a fyzické topologie: technologie FFDI, logicky (z pohledu L2) dvojitý kruh, fyzicky („drátově“) je zapojené do hvězdy na centrální zařízení nazývané MAU. Přepínaný Ethernet (zapojení switche) – fyzická topologie je hvězda, logická topologie je virtuální dvoubodové spojení.

třeba přístupová metoda, která reguluje přístup dat na médiím tak, aby nedocházelo ke kolizím (*collisions*) mezi různými signály (rámci) na lince.
Typické přístupové metody jsou CSMA/CD, CSMA/CA, ale lze použít i metodu token passing (= předávání tokenu). Přístupové metody hledají vhodný poměr mezi řízením rámce, ochranou rámce a režií sítě.

Topologie kruhová

V logické kruhové topologii každý uzel, který je na řadě (*in turn*), přijme rámec. Pokud není rámec určen tomuto uzlu, přejde na další uzel v řadě. To umožňuje používat techniku řízeného přístupu k médiu nazývanou *token passing* (= předávání tokenu, žetonu). Každý uzel vyjme rámec z kruhu, prozkoumá adresu, a pokud to není adresa tohoto uzlu, pošle rámec po médiu dále.
Existuje vícero přístupových metod, které mohou být použity v logické kruhové topologii, v závislosti na úrovni požadovaného řízení. Například: pouze jeden rámec je obvykle přenášen přes médium v jedné chvíli. Jestliže nejsou žádná („užitečná“) data, která by měla být přenášena, může být na médium umístěn signál (nazývaný *token*) a uzel pouze umístí datový rámec na médium, když má (když přijal) token.
Nezapomeňte, že když spojová vrstva „vidí“ logickou kruhovou topologii, skutečná fyzická (kabelová, „drátová“) topologie může být jiná.

Rámce jednotlivých protokolů

V kurzu CCNA jsou **postupně** popisovány následující protokoly a jejich PDU - rámce (*frames*):

- **Ethernet** – protokol pro technologii LAN umožňující sdílené médium,
- **Point-to-Point Protocol (PPP)** – protokol pro dvoubodové připojení,
- **High-Level Data Link Control (HDLC)** – protokol pro sériovou linku (proprietární Cisco),
- **Frame Relay** – protokol technologie přepínání paketů WAN,
- **Asynchronous Transfer Mode (ATM)** – technologie přepínaných „buněk“ stejné velkosti, postupně nahrazovaný GigaEthernetem.

Každý protokol používá specifickou přístupovou metodu pro specifickou L2 logickou topologii. To znamená, že množství různých síťových zařízeních funguje jako uzly na spojové vrstvě, když implementujete tyto protokoly. Tyto zařízení zahrnují síťové karty (NIC) v počítačích, síťová rozhraní ve směrovačích (routerech) a L2 switche (přepínače).

L2 protokol používaný pro konkrétní síťovou topologii je určen technologií použitou pro implementaci této topologie. Technologie je určena:

- velikostí sítě (jednak počtem hostitelů a jednak geografickou rozlehlostí),
- službami, které mají být poskytovány v síti.

Technologie LAN

Lokální síť LAN (Local Area Network) používá typicky technologie **s velkou šířkou pásma, velkou přenosovou kapacitou** (*high bandwidth*[62]), které jsou schopné podporovat velké množství

62 Bandwidth = (analogová) šířka pásma = (digitální) přenosová rychlost = přenosová kapacita komunikačního kanálu = maximální teoretický počet přenesených bitů v daném médiu/technologii v bitech za sekundu (*bps*, b/s).

hostitelů. LAN pracuje v relativně malém geografickém území (jedna budova nebo několik málo budov – školní areál = *campus*) s vysokou hustotou uživatelů a to činí tuto technologii nákladově efektivní (relativně levnou).

Technologie WAN

Bohužel, použití technologie velké šířky pásma obvykle není levné v **rozlehlé síti WAN (Wide Area Network)**, která pokrývá geograficky velká území (například město, několik měst). Cena fyzických linek na velké vzdálenosti a technologie použité pro přenos signálů na velké vzdálenosti typicky vyúsťuje do použití nízké šířky pásma – nízké přenosové rychlosti.

Rozdíly v šířce pásma normálně vyúsťují do použití různých protokolů pro LAN a pro WAN.

Protokol Ethernet pro LAN

Ethernet je rodina síťových technologií definovaných standardy IEEE 802.2 a 802.3. Standardy Ethernet definují obojí L2 a technologie L1. Ethernet je nejrozšířenější používaná technologie LAN a podporuje datové šířky pásma 10, 100, 1000 a 10,000 Mbps (megabitů za sekundu).
Základní formát rámce a IEEE podvrstvy vrstev L1 a L2 O modelu zůstávají shodné ve všech formách Ethernetu. Avšak metody detekce a umístění dat na médiu se mění s různými implementacemi.
Ethernet poskytuje nepotvrzované nespojované služby na sdíleném médiu při použití přístupové metody CSMA/CD. Sdílené médium požaduje, aby byly použity L2 adresy identifikující zdrojový a cílový uzel. Ve většině protokolů LAN jsou tyto adresy označovány jako MAC adresy uzlu. MAC adresa Ethernetu je 48-mi bitová a všeobecně se uvádí v hexadecimálním formátu.
Rámec Ethernetu má šest políček, uvedených na obrázku. Na spojové vrstvě je struktura rámce téměř stejná pro všechny rychlosti Ethernetu. Avšak na fyzické vrstvě umisťují různé verze Ethernetu bity na médium různým způsobem.
Ethernet II je rámec Ethernetu používaný v sítích TCP/IP.
Ethernet je důležitou částí datových sítí, a je mu věnována zvláštní kapitola. Také je používán v příkladech v celé sérii kurzů CCNA. Jsou dva základní formáty rámců Ethernet.

Ethernet II

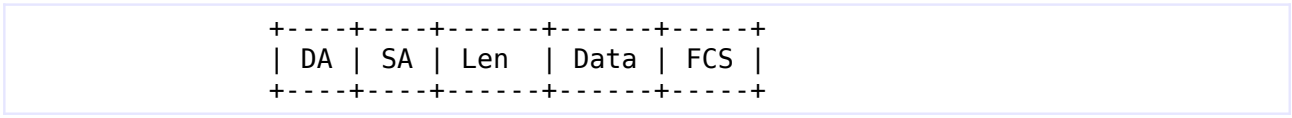
```
+----+----+------+------+-----+
| DA | SA | Type | Data | FCS |
+----+----+------+------+-----+
```

První pole rámce je **Preambule** (*Preamble*)[63] (8 bajtů) pro synchronizaci začátku rámce na síťové kartě.

63 Preambule (celkem 8 bajtů): sedm bajtů 10101010 a nakonec jeden bajt 10101011.

DA	Destination MAC Address – cílová MAC adresa	(6 bytes)
SA	Source MAC Address – zdrojová MAC adresa	(6 bytes)
Type	Protocol Type – typ protokolu (L3)[64]	(2 bytes)
Data	Protocol Data – data protokolu – přenášená (*payload*) data	(46 - 1500 bytes)
FCS	Frame Checksum Sequence – kontrolní součet (CRC)	(4 bytes)

IEEE 802.3 (revize) a jeho odvozeniny

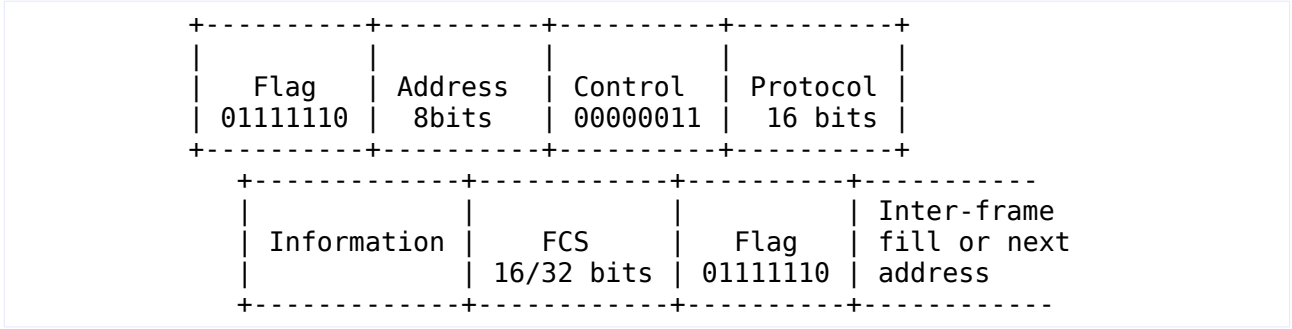


První dvě pole rámce jsou **Preambule** (*Preamble*) (7 bajtů) s **Start Frame Delimiter** (1 bajt) určené pro synchronizaci začátku rámce. Obsahově jsou totožné s obsahem pole **Preamble** v normě Ethernet II.

DA	Destination MAC Address – cílová MAC adresa	(6 bytes)
SA	Source MAC Address – zdrojová MAC adresa	(6 bytes)
Len	Length of Data field – délka datového pole	(2 bytes)
Data	Protocol Data – data protokolu – přenášená (*payload*) data	(46 - 1500 bytes)
FCS	Frame Checksum Sequence – kontrolní součet (CRC)	(4 bytes)

Zdroj: www.ietf.org

Formát rámce Point-to-Point Protocol (PPP)



Obrázek neobsahuje start a stop bity (pro asynchronní linky). Pole jsou přenášena zleva doprava.

- **Flag** – Návěští – jeden bajt, který identifikuje začátek nebo konec rámce. Pole obsahuje binární sekvenci 01111110,
- **Address** – Adresa – jeden bajt, který obsahuje standardní PPP **broadcastovou adresu** (11111111). PPP nepřiřazuje adresy individuálním stanicím (ve dvoubodovém spojení nemá L2 adresace smysl),
- **Control** – řízení – jeden bajt, který obsahuje binární sekvenci 00000011, která žádá o vysílán uživatelských dat v neseřazeném rámci,

64 Hexadecimální hodnota 0x0800 znamená, že je zapouzdřen paket IPv4.

- **Protocol** – protokol – 2 bajty, které identifikují zapouzdřený protokol v datovém poli, nejaktuálnější čísla protokolů jsou uveřejněna v nejnovějším (aktuálním) RFC - Assigned Numbers: RFC1700 viz: http://www.faqs.org/rfcs/rfc1700.html .
- **Information** = Přenášená data – zapouzdřená data jsou proměnné délky,
- **FCS (Frame Check Sequence)** – kontrolní součet, normálně 16 bitů (2B), po předchozí odsouhlasené dohodě může být dlouhý 32 bitů (4B).

Zdroj: RFC2171, RFC1549

Protokoly pro bezdrátovou LAN (WLAN)

(WLAN = Wireless LAN.) **IEEE 802.11** je rozšíření standardů IEEE 802. Používá stejné 802.2 LLC a 48-bitové adresní schéma (MAC) jako ostatní LAN založené na standardu IEEE 802. Nicméně je zde mnoho rozdílů na podvrstvě MAC a na fyzické vrstvě. V bezdrátovém prostředí je však třeba brát v úvahu zvláštní požadavky dané samotným prostředí. Není zde definované fyzické připojení, a tak mohou vnější vlivy interferovat s přenášenými daty a je zde obtížné řídit přístup k médiu. Aby tyto problémy (*challenges*) vyřešily, přidala se do bezdrátové technologie další řízení.
Standard IEEE 802.11, běžně označovaný jako ***Wi-Fi** (WiFi – Wireless Fidelity)*, je systém založený na soutěži (*contention-based system*), který používá jako metodu řízení přístupu k médiu **Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)**. CSMA/CA definuje **náhodnou odmlku** (backoff) na všech uzlech (na každém jinou), kterou čekají před vysíláním. Nejpravděpodobnější příležitost pro úspěšnou soutěž o médium je bezprostředně po tom, co se médium stalo dostupným. Odmlka po náhodnou dobu na jednotlivých uzlech velmi snižuje možnost vzniku kolize.
Sítě 802.11 také používají **potvrzování na spojové vrstvě**, aby ověřily, že byl rámec úspěšně přijat. Jestliže vysílací stanice nedetekuje **potvrzující rámec**, buď proto že původní datový rámec nebo že rámec s potvrzením nebyl přijat nedotčený, je datový rámec znovu odvysílán. Toto explicitní potvrzování zvítězí nad interferencemi a dalšími problémy souvisejícími s přenosem elektromagnetických vln.
Další služby podporované 802.11 jsou autentizace, asociace (připojení bezdrátového zařízení) a utajení dat (šifrování).

Poznámka:
*Protože **detekce kolize je u bezdrátového vysílání problematická**[65], přináší metoda CSMA/CA (CA = Collisin Avoidance = předcházení kolizí) proti CSMA/CD (CD = Collision Detection = detekce kolizí) virtuální naslouchací mechanismus (= rezervaci). Jednotlivé zprávy (rámce) protokolu CSMA/CA:*

- ***RTS – Request To Send** – žádost o rezervaci – stanice, které chce vysílat vyšle RTS, který definuje zdroj, cíl a předpokládanou dobu přenosu,*
- ***CTS – Clear To Send** – potvrzení rezervace – cílová stanice vyšle CTS s dobou trvání přenosu,*
- ***ACK – Acknowledge** – potvrzení přijetí rámce.*

Všechny stanice slyšící RTS nebo CTS musí chápat médium po celou inzerovanou dobu jako obsazené.

Rámec technologie Wi-Fi IEEE 802.11 obsahuje následující pole (velikost polí je v bajtech):

- **Frame Control** - Řídicí pole rámce (2B) se skládá z následujících skupin bitů a bitů (v

65 Problém skrytého uzlu (*hidden node problem*). (Při komunikaci mezi dvěma počítači z bezdrátové síťové karty přes AP sice z jedné síťové karty „vidím“ AP, ale již nikoliv nutně druhou síťovou kartu na druhém počítači.)

jednotkách bit):

- **Protocol Version** (2b) – verze používaného rámce 802.11,
- **Type** (2b) a **Subtype** (4b) – identifikuje jednu ze tří funkcí (řízení, data a správa) a podfunkcí (RTS, CTS, ACK) rámce
- **To DS** (1b)– nastavení na 1 v datovém rámci ho adresuje do distribučního systému (zařízení v bezdrátové struktuře),
- **From DS** (1b) - nastaveno na 1 v datovém rámci z distribučního systému,
- **More Fragments** (1b) - nastaveno na 1 v rámci, který má další fragment,
- **Retry** (1b) - nastavení na 1 v rámci, který je znovu odvysíláním předcházejícího rámce,
- **Power Management** (1b) - nastavení na 1 indikuje, indikuje, že uzel bude v úsporném režimu,
- **More Data** (1b) - nastavení na 1 indikuje uzlu v úsporném režimu, že je ve vyrovnávací paměti více rámců pro tento uzel,
- **Wired Equivalent Privacy (WEP)**[66] (1b) - nastavení na 1 v datovém rámci, jestliže rámce obsahuje šifrované WEP informace pro zabezpečení,
- **Order** (1b) - nastavení na 1 v datovém rámci, který používá servisní třídu „Strictly Ordered“ (a tedy nepotřebuje seřazení do správného pořadí),

- **Duration/ID** (2B) – závisí na typu rámce, reprezentuje buď čas v mikrosekundách, potřebných k přenosu rámce nebo identitu asociace (AID) pro stanici, která vysílala rámec,
- **Destination Address (DA)** (6B) - MAC adresa konečného cílového uzlu v síti,
- **Source Address (SA)** (6B) - MAC adresa uzlu, který inicializoval rámec,
- **Receiver Address (RA)** (6B) - MAC adresa, která identifikuje bezdrátové zařízení, které je bezprostředním příjemcem rámce,
- **Transmitter Address (TA)** (6B) - MAC adresa, která identifikuje bezdrátové zařízení, které vysílalo tento rámec,
- **Sequence Control (2B)** – řízení pořadí rámců a jejich fragmentů, se skládá ze dvou skupin bitů:
  - **Sequence Number** (12 bitů) – označuje pořadové číslo přiřazené rámci, znovu odvysílaný rámec je identifikován duplikovaným pořadovým číslem,
  - **Fragment Number** (4 bity) – označuje číslo každého fragmentu rámce,
- **Frame Body** (0 – 2312 bajtů) – obsahuje přenášená data, pro datový rámec, typicky IP paket,
- **FCS (Frame Check Sequence)** (4B) – obsahuje 32 bitový kontrolní součet (CRC) rámce.

Aktivní prvky sítí na druhé vrstvě (L2) v Ethernetu

- **Můstek (*Bridge*)** – dvouportové zařízení, které rámec z jednoho portu zesílí a na na základě obsahu přepínací tabulky (*bridge table*) buď předá druhému portu, nebo ho zahodí.
- **Přepínač (*Switch*)** – víceportový můstek – rámec z jednoho portu zesílí a na základě obsahu přepínací tabulky (*switch/bridge table*) tento rámec buď předá na jeden jiný konkrétní port, nebo ho zahodí, nebo jím zaplaví (*flooding*) všechny ostatní porty. (Podrobněji viz Kapitola 9 – Ethernet).

66 Je třeba si uvědomit, že WEP (Wired Equivalent Privacy) není zajištění bezpečného přenosu dat, ale pouze přenos dat bezpečností ekvivalentní s nezabezpečeným drátovým Ethernetem. Lepší zabezpečení je WAP, WAP2.

Souvislosti

1. Účelem spojové vrstvy je oddělit síťovou vrstvu od konkrétní síťové technologie a přenosového média (na vrstvách L2 a L1). Tím může L3 paket zůstat při své cestě propojenými sítěmi nezměněn. Nemění se cílová ani zdrojová IP adresa, pouze se zmenšuje doba života (TTL) a kontrolní součet záhlaví paketu.
2. Spojová vrstva dopravuje L2 rámce pouze v rozsahu jednoho síťového segmentu (= jedné fyzické sítě).
3. Adresy na druhé vrstvě se mění v každém síťovém segmentu, protože je rámec na každém síťovém segmentu vytvářen znova a znova. (Z rámce je na L2 směrovače odpouzdřen (vybalen) paket a po nalezení nejlepší cesty je opět zapouzdřen do nového L2 rámce.).
4. Adresy na L2 jsou potřeba pouze u logické topologie sdíleného média a kruhové. V logické topologii dvoubodového spoje nejsou L2 adresy potřeba. (Například HDLC ani PPP nemá ve svém rámci zdrojovou ani cílovou adresu, ale pouze jednu broadcastovou, všesměrovou, adresu. Data se mohou přenést pouze na druhý konec dvoubodového spoje.)
   POZOR: IP adresy jsou ale ve dvoubodovém spoji třeba!!!
5. Kontrolní součet v rámci se na každém segmentu sítě počítá dvakrát, poprvé při vytvoření rámce a podruhé při jeho přijetí příjemcem.
6. Konkrétní síťová technologie je daná použitým přenosovým médiem a logickou topologií (zda je médium sdíleno, či nikoliv). Každá síťová technologie má svůj vlastní formát rámce. Každá technologie používá určitou konkrétní přístupovou metodu (= metodu řízení přístupu k přenosovému médiu).

Tok dat přes propojené sítě

Popis činnosti vzájemně propojených sítí z pohledu L2 i L3. Uvědomit si funkci nastavení klienta v síti (IP adresa, maska, implicitní výchozí brána). Rozhodnutí na kterou IP (resp. MAC) adresu budou datové rámce zasílány. Překlad IP adresy na MAC adresu, přes kterou se adresuje uvnitř lokální sítě pro fyzický přenos dat (funkce a činnost ARP: *ARP request*, *ARP response*, *ARP cache*). Výpočet CRC a vložení kontrolního součtu do pole FCS v zápatí rámce na zdrojové síťové kartě, výpočet CRC na cílové síťové kartě (v jednom síťovém segmentu) a kontrola proti vloženému FCS v zápatí. Pokud nesouhlasí je rámec odhozen. (Ethernet je nepotvrzovaný a nespojovaný protokol.) Rozbalení rámce do paketu na vstupním portu směrovače. Odečtení jedničky z pole TTL. Směrování do cílové sítě na základě cílové IP adresy v paketu a masky podsítě v řádce směrovací tabulky. Výběr správného směru do cílové sítě => výstupní port tohoto směrovače (*outgoing interface*) nebo vstupní port dalšího směrovače v příslušném směru (*next hop*). Přepnutí rámce = znovu zapouzdření paketu do rámce příslušné síťové technologie na odchozím portu ze směrovače.
Viz animace 7.4.1.2:
Jak to tedy všechno funguje dohromady?

- Sledujeme data procházejících sítí - přenos dat mezi dvěma hostiteli ve třech propojených sítích.
- Ze zdrojového **hostitelského počítače PC** (IP: 10.1.1.1) připojenému **Ethernetem (10Mb/s)** ke **směrovači A** (Router A), který je spojen **WAN sériovou linkou** s druhým **směrovačem B** (Router B) propojovací (tranzitní) sítí 192.168.1.4/30. K druhému směrovači je přes **FastEthernet (100Mb/s)** připojen cílový **webový server** (IP: 192.0.3.7 a přidělené

doménové jméno).

- Pro příklad je použit požadavek na stažení webové stránky **GET request** mezi klientem a serverem. V následujícím přehledu je vynecháno mnoho prvků, které se vyskytují v reálném provozu v síti. V každém kroku se zaměřujeme pouze na v té chvíli klíčové prvky. (Například jsou vynechána různá, v této chvíli, nepodstatná pole z hlaviček PDU.)
  - Předpokládáme, že směrovací tabulky jsou zkonvergované a tabulky ARP jsou úplné.
  - Dále předpokládáme, že spojení mezi klientem a serverem na úrovni TCP je již plně navázáno (je vytvořena relace (*session*)).
  - Dále předpokládáme, že vyhledání v DNS pro dané doménové jméno již bylo také provedeno a výsledek je uložen ve vyrovnávací paměti na klientu.
  - Na WAN lince mezi směrovači předpokládáme vytvoření relace v protokolu PPP.

Čtete následující kroky pozorně:

1. **Web klient (browser) požaduje data z web serveru.** Uživatel v lokální síti LAN požaduje přístup k webové stránce na web serveru umístěném ve vzdálené síti. Uživatel začne s aktivací spojení s webovou stránkou.
2. **Aplikační vrstva zdroje začíná s inicializací přenosu dat.** Browser iniciuje **požadavek GET**. Aplikační vrstva přidá záhlaví k PDU L7 k identifikaci aplikace a protokolu. (Aplikace: Web Browser, Protokol: GET.)
3. **Transportní vrstva zdroje vytváří relaci mezi zdrojem a cílem.** Transportní vrstva identifikuje službu vyšší vrstvy jako klienta World Wide Web (WWW). Transportní vrstva potom přiřadí tuto službu k protokolu TCP a nastaví čísla portů. Použije náhodně vybraný zdrojový port, který je přidružený s touto vytvořenou relací (12345). (*Poznámka: přesněji: použije první volné dynamické číslo portu poskytnuté službou operačního systému.*) Cílový port (80) je přiřazen ke službě WWW. Záhlaví TCP ještě dále obsahuje číslo potvrzení Ack # =154647, pořadové (sekvenční) číslo Seq # = 7332 a **návěští (*flags*)** SYN=0 a ACK=1.
4. TCP posílá číslo potvrzení (Ack #), které říká www serveru, jaké číslo sekvence (pořadové číslo, Seq #) očekává že přijme v příštím segmentu. Sekvenční číslo určuje, kde je segment umístěn v řadě na sebe navazujících segmentů. Návěští jsou také odpovídajícím způsobem nastavena pro vytvoření relace (respektive pro pokračování již jednou vytvořené relace).
5. **Na síťové vrstvě je vytvořen IP paket**, aby identifikoval zdrojové a cílové hostitele. Jako cílovou adresu použije hostitelský počítač IP adresu (192.0.3.7), kterou má přiřazenou k doménovému jménu web serveru a uloženou ve vyrovnávací paměti v tabulce hostitelů. Jako zdrojovou IP adresu použije svoji vlastní (10.1.1.1). Síťová vrstva dále identifikuje zapouzdřený protokol vyšší vrstvy jako TCP.
6. Protože je cílová IP adresa v jiné IP síti než je zdrojový hostitelský počítač (klient to zjistí odmaskováním zdrojové a cílové IP adresy maskou podsítě), **použije na spojové vrstvě** klient **vyrovnávací paměť protokolu ARP** pro zjištění **MAC adresy vstupního rozhraní směrovače (= výchozí brány z lokální sítě)**. Tato adresa je použita jako **cílová adresa** při **vytvoření rámce Ethernet II**, ve kterém je zabalen paket IP4 pro přenos lokálním přenosovým médiem. Jako **zdrojová L2 adresa v rámci** je použita MAC adresa ze síťové karty (NIC) klienta. (Zdrojová MAC adresa: 00-05-9A-3C-78-00, cílová MAC adresa: 00-08-A3-B6-CE-04.)
7. V rámci je též indikován zapouzdřený protokol vyšší vrstvy (pro protokol IPv4 má rámec v poli **Typ** hexadecimální hodnotu 0x0800). Rámec začíná hodnotou pole **Preambule**

(sedmkrát 10101010 a potom 10101011). Rámec je zakončen hodnotou **kontrolního součtu** (*CRC, Cyclic Redundance Check*) v poli **Frame Check Sequence** (kontrolní sekvence rámce) pro detekci výskytu chyb v rámci. Pro řízení umístění (přístupu) rámce na přenosové médium je použita **přístupová metoda CSMA/CD**. Použitý protokol pro podvrstvy LLC/MAC je IEEE 802.2/802.3.

8. **Fyzická vrstva** začne kódovat rámec na přenosové médium bit po bitu. Fyzická vrstva transportuje data přenosovým médiem. Síťový segment mezi směrovačem B a zdrojovým hostitelem je segment 10Base-T (Ethernet, šířka pásma, přenosová rychlost 10Mb/s), z tohoto důvodu jsou bity kódovány s použitím **Manchesterského diferenciálního kódování** (*Manchester Differential encoding*) (viz následující kapitola Fyzická vrstva). Směrovač B načítá jednotlivé bity, tak jak jsou přijímány, do své vyrovnávací paměti.
9. **Směrovač B na spojové vrstvě** prozkoumává bity v **preambuli** rámce a hledá dva za sebou následující jedničkové bity, které indikují, že je synchronizace u konce a začíná obsah rámce. Směrovač potom začíná ukládat bity do vyrovnávací paměti jako část jednoho rekonstruovaného rámce. Po načtení spojová vrstva vypočte **kontrolní součet rámce** a porovná ho s hodnotou **FCS** uloženou v zápatí rámce. (Pokud by hodnoty nesouhlasily, rámec by byl zahozen.)
10. **Sítová vrstva**[67] porovnává **cílovou adresu** IPv4 se **směry (cestami) do cílových sítí ve směrovací tabulce**. Je nalezena odpovídající hodnota cílové sítě a s ní asociovaná adresa dalšího přeskoku, k této adrese je pak nalezeno příslušné odchozí rozhraní tohoto směrovače (s0/0/0). Paket je potom zevnitř směrovače předán do elektronických obvodů rozhraní s0/0/0.

Cílová síť	***Další přeskok (Next-hop)***	***Odchozí rozhraní***
10.1.1.0/24	C = přímo připojená síť	Fa0/0
192.0.3.0/24	192.168.1.6	S0/0/0
192.168.1.4/30	C = přímo připojená síť	S0/0/0

11. **Spojová vrstva**. Směrovač vytvoří **rámec PPP** (*point-to-point protocol*) pro přenos dat přes síť WAN. Do záhlaví PPP je přidáno návěstí s hodnotou 01111110 pro označení začátku rámce. Pole adresy má hodnotu 11111111, znamenající oběžníkové, všesměrové, (B/C) vysílání určené všem stanicím - uzlům v síti. S ohledem na to, že jde o dvoubodový spoj mezi dvěma uzly (*point to point*), nemá tato adresa v PPP rámci žádný význam.
12. Rámec PPP také obsahuje pole Protokol s hexadecimální hodnotou 0x0021, který indikuje, že je zapouzdřen paket IPv4. Zápatí rámce končí v poli *Frame Check Sequence* (FCS) kontrolním součtem pro detekci chyby. Hodnota návěští 01111110 indikuje, že se jedná o rámec PPP.
13. **Fyzická vrstva** (s vždy mezi směrovači vytvořeným obvodem a relací PPP) začne kódovat rámec bit po bitu na přenosové médium. Přijímající směrovač ukládá přijaté bity bit po bitu po vyrovnávací paměti. Způsob kódování a reprezentace bitů je závislý na konkrétní použité technologii WAN.
14. **Směrovač A na spojové vrstvě** prozkoumává bity v návěští, aby identifikoval začátek rámce. Směrovač potom začne bity ukládat jako část rekonstruovaného rámce. Když je přijat celý rámec, což je indikováno návěštím na konci rámce, směrovač vypočte kontrolní součet

67 Navíc ještě zmenší o jedničku hodnotu pole TTL. Pokud by potom byla nulová, je paket zahozen. To v našem příkladě nehrozí.

(CRC) celého rámce. Jestliže souhlasí s hodnotou kontrolního součtu v poli FCS na konci přijetého rámce, je potvrzeno, že rámec byl přijat nedotčený. Jestliže je takto potvrzeno, že je rámec v pořádku, je odstraněno záhlaví rámce a paket je vystrčen do síťové vrstvy.

15. **Síťová vrstva** porovnává cílovou adresu IPv4 se směry (cestami) ve směrovací tabulce. Odpovídající síť je nalezena jako přímo připojená k rozhraní Fa0/0. Paket je potom předán do rozhraní Fa0/0.

Cílová síť	***Další přeskok (Next-hop)***	***Odchozí rozhraní***
10.1.1.0/24	192.168.1.5	S0/0/0
192.0.3.0/24	C = přímo připojená síť	Fa0/0
192.168.1.4/30	C = přímo připojená síť	S0/0/0

16. **Spojová vrstva** se podívá do vyrovnávací paměti protokolu ARP, aby zjistila MAC adresu rozhraní web serveru. Tato adresa je potom použita **v ethernetovém rámci** určenému pro přenos dat v lokálním přenosovém médiu do web serveru. Jako **zdrojová adresa** je v něm použita MAC adresa rozhraní fa0/0 směrovače a jako **cílová adresa** je použita MAC adresa web serveru. V rámci je též indikován zapouzdřený protokol vyšší vrstvy (pro protokol IPv4 má rámec v poli Typ hexadecimální hodnotu 0x0800). Rámec začíná hodnotou **pole Preambule** (sedmkrát 10101010 a potom 10101011). Rámec je zakončen hodnotou **kontrolního součtu (CRC, *Cyclic Redundance Check*)** v poli **FCS (*Frame Check Sequence*)** pro detekci výskytu chyb v rámci. Pro řízení umístění (přístupu) rámce na přenosové médium je použita přístupová metoda CSMA/CD.
17. **Fyzická vrstva** začne kódovat rámec na přenosové médium bit po bitu. Síťový segment mezi směrovačem A a cílovým web serverem je segment 100Base-T (FastEthernet, 100Mb/s), a proto jsou bity kódována **blokovým kódem 4B/5B** (viz následující kapitola Fyzická vrstva). Server ukládá přijaté bity do vyrovnávací paměti.
18. **Web server na spojové vrstvě** prozkoumává bity v **preambuli** a hledá dva za sebou následující jedničkové bity, které indikují, že je **synchronizace** u konce a začíná obsah rámce. Směrovač potom začíná ukládat bity do vyrovnávací paměti jako část rekonstruovaného rámce. Když je přijat celý rámec, server vygeneruje kontrolní součet rámce a porovná ho s hodnotou v poli **FCS**. Pokud jsou hodnoty shodné, znamená to, že rámec byl přijat nedotčený.
19. Když je rámec shledán v pořádku, je **v síťové kartě serveru** na spojové vrstvě porovnána cílová MAC adresa v rámci s MAC adresou síťové karty. Protože jsou shodné, je odstraněno záhlaví a a zápatí a **paket** je přesunut do síťové vrstvy.
20. **Na síťové vrstvě** je prozkoumána **cílová IP adresa z paketu**, aby se určil **cílový hostitel**. Protože tato IP adresa odpovídá vlastní IP adrese je tento paket zpracováván přímo v serveru. Síťová vrstva identifikuje zapouzdřený protokol vyšší vrstvy jako TCP, a tak předá vybalený (odpouzdřený) **segment** ke zpracování službě TCP na transportní vrstvě. (Paket IPv4: Zdrojová IP adresa: 10.1.1.1, Cílová IP adresa: 192.0.3.7, Vyšší vrstva: TCP.)
21. **Na transportní vrstvě serveru** je prozkoumán **TCP segment**, aby se **určila relace** (*session*), do které data obsažená v segmentu patří. To se zjistí prozkoumáním zdrojového a cílového portu (12345 a 80). Unikátní dvojice portů určuje existující relaci jako webovou službu serveru. Pořadové číslo (*sequence number*) umožní dát data do správného pořadí a odeslat je nahoru do aplikační vrstvy. (Ack#: 154647, Seq#: 7332, Flags: SYN:0 a ACK: 1.)
22. **Na aplikační vrstvě** je **požadavek htpp GET** (jako záhlaví a data PDU na L7) doručen **démonu služby webového serveru** (d). Tato služba pak může zformulovat odpověď na za-

daný požadavek.

Cvičení

1. Zachytávání rámců různých síťových technologií v PT (dva směrovače propojené sériovou linkou a také Ethernetem dvěmi propojovacími sítěmi 192.168.1.0/30 a 192.168.1.4/30 i také v realitě.
2. Protokol ARP v síti, zjištění MAC adresy výchozí brány.

Kontrolní opakovací otázky a odpovědi (kvíz):

1) Které pole rámce je vytvořeno zdrojovým uzlem a je použito na cílovém uzlu k zjištění zda přenášený datový signál nebyl změněn interferencí, ztrátou nebo zkreslením signálu?
   a) FCS (*Frame Check Sequence Field*) – kontrolní součet rámce
2) Jaké adresní schéma spojové vrstvy je použito v topologii dvoubodového spoje (*point-to-point topology*)?
   a) V této topologii není L2 adresa třeba (signál jde pouze na druhý konec „drátu“)
3) K čemu používají síťoví hostitelé adresy spojové vrstvy?
   a) K doručení uvnitř jedné aktuální lokální sítě
4) Které tři základní části mají všechny rámce na spojové vrstvě společné? (3 odpovědi)
   a) záhlaví (*header*),
   b) datové pole (*data*),
   c) zápatí (*trailer*).
5) Dvě charakteristiky řízené metody přístupu k přenosovému médiu (*controlled media access method*):
   a) jsou známé jako deterministické metody,
   b) pokud je tato metoda použita, nevyskytují se kolize
6) Z jakých dvou podvrstev se skládá spojová vrstva?
   a) LLC – Logical Link Control
   b) MAC – Media Access Control
7) Dvě charakteristiky zapouzdřování na spojové vrstvě:
   a) je přidáno záhlaví a zápatí
   b) paket je zabalen do rámce
8) Co je dosaženo při procesu zapouzdření na spojové vrstvě?
   a) Paket je zapouzdřen (vložen) do rámce
9) Přiřaďte odpovídající charakteristiky k oběma typům přístupových metod:
   a) řízený přístup:
      i. deterministické,

   ii. v jedné chvíli může vysílat pouze jedna stanice,
   iii. nejsou kolize,
   iv. metoda předávání žetonu (tokenu) (*token passing*).

b) soutěžní přístup (neřízené):
   i. nedeterministické,
   ii. stanice mohou vysílat kdykoliv (nebo se o to alespoň pokusit),
   iii. efektivnější využití šířky pásma (přenosové kapacity) přenosového kanálu,
   iv. používá ji Ethernet v přenosovém režimu poloviního duplexu (*half-duplex*).

10) Přiřaďte odpovídající charakteristiky k jednotlivým typům síťových topologií:

a) point-to-point (dvoubodový spoj):
   i. spojuje pouze dva uzly,
   ii. logický virtuální obvod (v případě přepínaného Ethernetu při použití switche).

b) Multi-acces (vícenásobný přístup = sdílené médium):
   i. sdílené médium,
   ii. CSMA/CD.

c) Ring (kruhová topologie):
   i. deterministická přístupová metoda,
   ii. token passing.

Kapitola 8 – Fyzická vrstva

V této kapitole se naučíme:

- Vysvětlit roli protokolů a služeb fyzické vrstvy v podpoře komunikace prostřednictvím datových sítí.
- Popsat účel kódování signálů na fyzické vrstvě a jak jsou použity v sítích.
- Popsat roli signálů použitých k reprezentaci bitů když je rámec přenášen přes lokální přenosové médium.
- Určit základní charakteristiky měděných a optických kabelů i bezdrátových přenosových médií.
- Popsat běžné použití měděných a optických kabelů i bezdrátových přenosových médií.

Účel fyzické vrstvy (L1): poskytuje prostředky pro přenos jednotlivých bitů rámce (L2 ho do nich zakóduje) přes síťové přenosové médium.

Tato vrstva přijímá kompletní rámec ze spojové vrstvy a zakóduje ho do série signálů, které jsou přenášeny na lokálním médiu. Zakódované bity na médiu (= signály), ze kterých se skládá rámec jsou přijaty koncovým zařízením nebo propojovacím zařízením.

Doručení rámce přes lokální médium vyžaduje následující prvky fyzické vrstvy:

- fyzická média a konektory,
- reprezentace bitů na médiu,
- kódování dat a řídicích informací,
- vysílací a přijímací obvody v síťových zařízeních.

Účelem L1 je vytvoření elektrických, optických či mikrovlnných signálů, které reprezentují jednotlivé bity každého vysílaného rámce.

Přenosová média nepřenáší rámce jako jednu entitu (jeden celek), ale jako jednotlivé bity, ze kterých je rámec tvořen.

Z tohoto důvodu je třeba jasně označit začátek a konec rámce – přidáním přesně dané posloupnosti bitů. Děje se to často na spojové vrstvě, ale u mnoha technologií i zvlášť na fyzické vrstvě.

Tři formy síťového přenosového média – a jim příslušející formy přenosu signálu:

- **měděné kabely** – elektrické signály,
- **optické kabely** – světelné pulsy,
- **bezdrátové** – mikrovlnné signály (modulace: amplitudová (AM), frekvenční (FM) a fázová (PM)).

Standardy pro L1

Standardy pro lokální sítě LAN zahrnují obvykle obě vrstvy L1 i L2.

Sady standardů pro L1 tedy zahrnují také telekomunikační organizace[68]:

68 Na rozdíl od standardů v protokolové sadě TCP/IP (pro L7 – L3) v RFC od Internet Engineering Task Force (IETF).

- The International Organization for Standardization (ISO)
- The Institute of Electrical and Electronics Engineers (IEEE)
- The American National Standards Institute (ANSI)
- The International Telecommunication Union (ITU)
- The Electronics Industry Alliance/Telecommunications Industry Association (EIA/TIA)

Čtyři oblasti, které tyto standardy zahrnují:

1. fyzikální a elektrické vlastnosti média,
2. mechanické vlastnosti média (materiál, rozměry, kontakty konektorů (*pinouts*)),
3. reprezentace bitu v signálu (kódování),
4. definice signálů pro šíření informací přes médium (přenos signálů).

HW komponenty jako jsou síťové adaptéry (NIC), rozhraní a konektory, kabely (jejich materiál i jejich provedení) jsou specifikovány ve standardech pro fyzickou vrstvu.

Základní principy a funkce L1

Tři základní funkce L1:

- **Fyzické komponenty** - elektronické HW zařízení, média a konektory, které přenášejí signály reprezentující bity,
- **Kódování dat** (*data encoding*) – metoda převodu toku bitů do předem daného kódu. Předdefinované vzory bitů umožní jednak rozlišit datové bity od bitů určených pro řízení přenosu dat (a tak zlepšit detekci výskytu chyb při přenosu na médiu) a jednak označit a určit začátek a konec rámce.
- **Vysílání přenosových signálů** (*signaling*)[69] – fyzická vrstva musí generovat elektrické, optické nebo mikrovlnné signály, které reprezentují „1“ a „0“ na médiu.

Přenos signálu médiem

Signál je digitální. Základní jednotky popisující digitální signál:

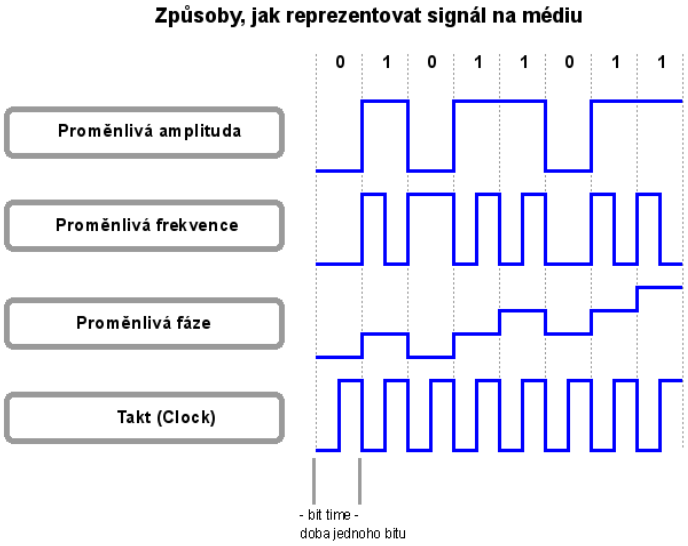
- doba trvání jednoho bitu (*bit time*),
- amplituda (= velikost přenosové veličiny).

Bity jsou na médiu reprezentovány změnou jedné nebo více následujících charakteristik signálu:

- amplituda,
- frekvence,
- fáze.

Modulace amplitudy, frekvence nebo fáze nosného signálu.

69 Termínem signalizace se ve sdělovací technice (v českém prostředí) rozumí navazování a řízení spojení na lince. Jednoslovný termín, ekvivalentní k anglickému, v češtině není.



Kódování a metody přenosu signálu

Kódování (Encoding)

Kódování je metoda převodu toku datových bitů do předem definovaného kódu. Kódy jsou skupiny (bloky) bitů použité pro vytvoření předvídatelných vzorů, které mohou být rozpoznány na jak na vysílači tak na přijímači. Použití předvídatelných vzorů pomáhá rozlišit datové bity od bitů pro řízení přenosu a zlepšuje tak detekci chyb na médiu.
Navíc k vytvoření kódů pro data mohou kódovací metody na fyzické vrstvě také poskytnout kódy pro účely řízení jako jsou identifikace začátku a konce rámce. Vysílající hostitel potom vysílá zvláštní vzor bitů nebo kód aby identifikoval začátek a konec rámce.

Vysílání přenosového signálu (Signaling)

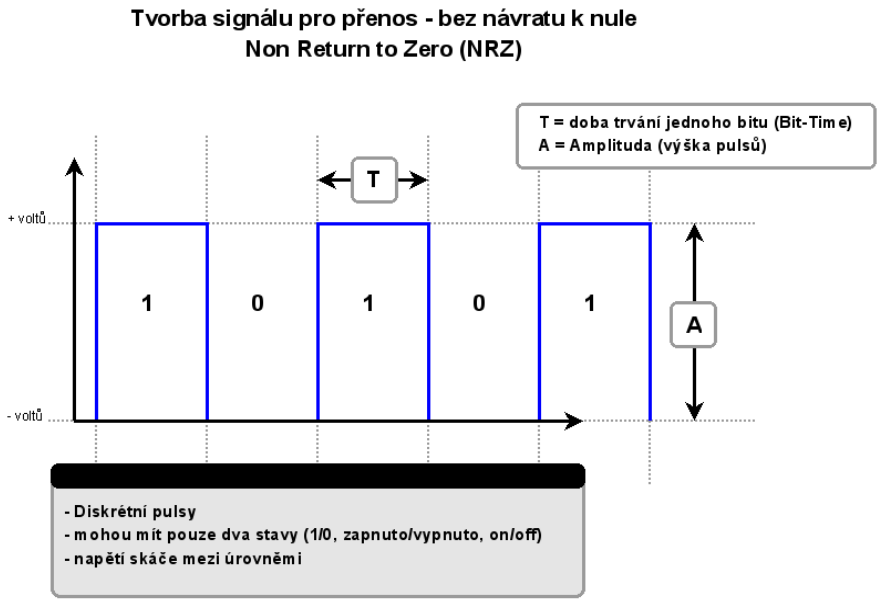
Poznámka: Signál = fyzikální nosič informace. Signaling = proces vysílání přenosového signálu na fyzické médium za účelem komunikace.
Fyzická vrstva musí generovat elektrické, optické nebo bezdrátové (= elektromagnetické) signály, které reprezentují „1“ a „0“ na médiu. Metoda reprezentace bitů se nazývá signalizační metoda. Standardy pro fyzickou vrstvu musí definovat jaký signál reprezentuje „1“ a jaký „0“. To může být tak jednoduché jako je změna úrovně (amplitudy) elektrického signálu nebo optického pulzu nebo může jít o komplexnější metodu.

Metoda kódování NRZ

NRZ (*Non Return to Zero*). Dvouúrovňové (bipolární) kódování **bez návratu k nule**: jednička je reprezentovaná vyšší hodnotou přenosové veličiny (například napětí) a nula je reprezentována nižší hodnotou (nikoliv přímo nulovou, nulovým napětím, ale obvykle hodnotou opačné polarity). Změna probíhá skokově, pulsy jsou diskrétní a mohou mít pouze jednu ze dvou amplitud. Tento přenos

signálu je vhodný **pouze pro nízké přenosové rychlosti**. V současných datových sítích se nepoužívá.

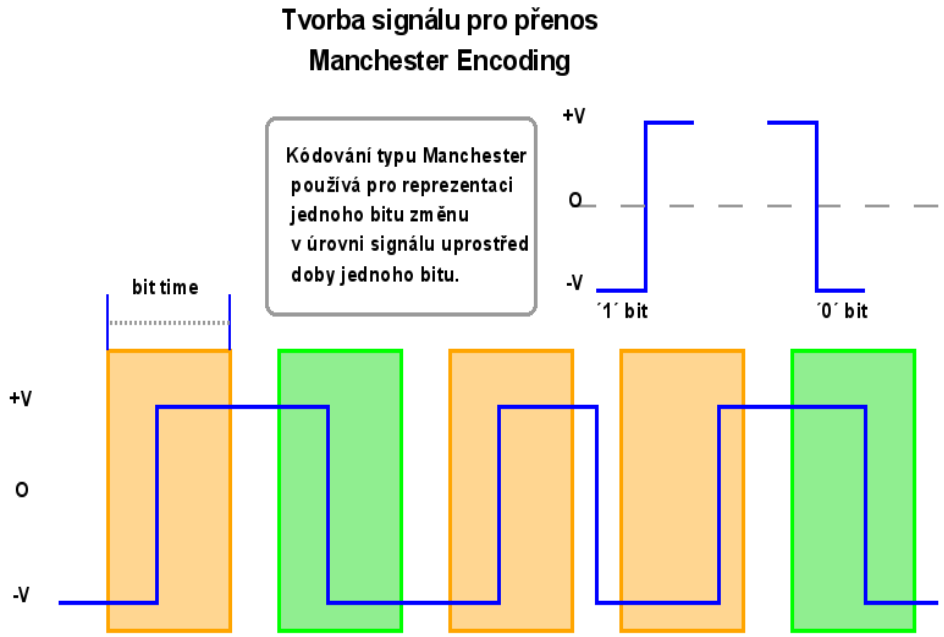
- Nevýhody: Náchylné na **elektromagnetické interference** vzniklé elektromagnetickou indukcí (ty jsou obvykle amplitudově modulované). Neobsahuje synchronizaci (u dlouhé skupiny samých nul nebo samých jedniček, už nemusí být zřejmé, kolik jich vlastně bylo).



Kódování Manchester

Diferenciální kódování typu Manchester je dvou úrovňové kódování: jednička je **reprezentována vzestupem úrovně přenosové veličiny** (náběžnou hranou) **uprostřed periody doby bitu** (hodin (*clock*)) a nula je reprezentována poklesem úrovně (doběžnou hranou). Toto kódování se používá u nejpomalejšího Ethernetu 10BASE-T (10Mbps).

- Také není příliš efektivní, ale je méně náchylné na (obvykle amplitudově modulované) rušení a interference než kódování NRZ.
- Obsahuje **synchronizační signál** (hodiny) pro synchronizaci zdrojového a cílového uzlu.



Blokové kódování (kódování seskupováním bitů)

Více úrovňové kódování. Určité skupiny bitů mají konkrétní význam. K bitům vlastního zakódovaného rámce jsou přidány navíc další bity. (Speciální znaky začátku a konce rámce.) To vše má za následek:

- snížení úrovně výskytu chyby,
- snížení spotřeby energie nutné pro přenos,
- odlišení datových bitů od bitů určených pro řízení přenosu dat,
- lepší detekce nastalých chyb,
- zvýšení přenosové rychlosti.

Náhodné signály na médiu (mimo rámce) vlivem interference nebo nebo šumu jsou jako takové určeny a nejsou propuštěny ke zpracování do druhé vrstvy.

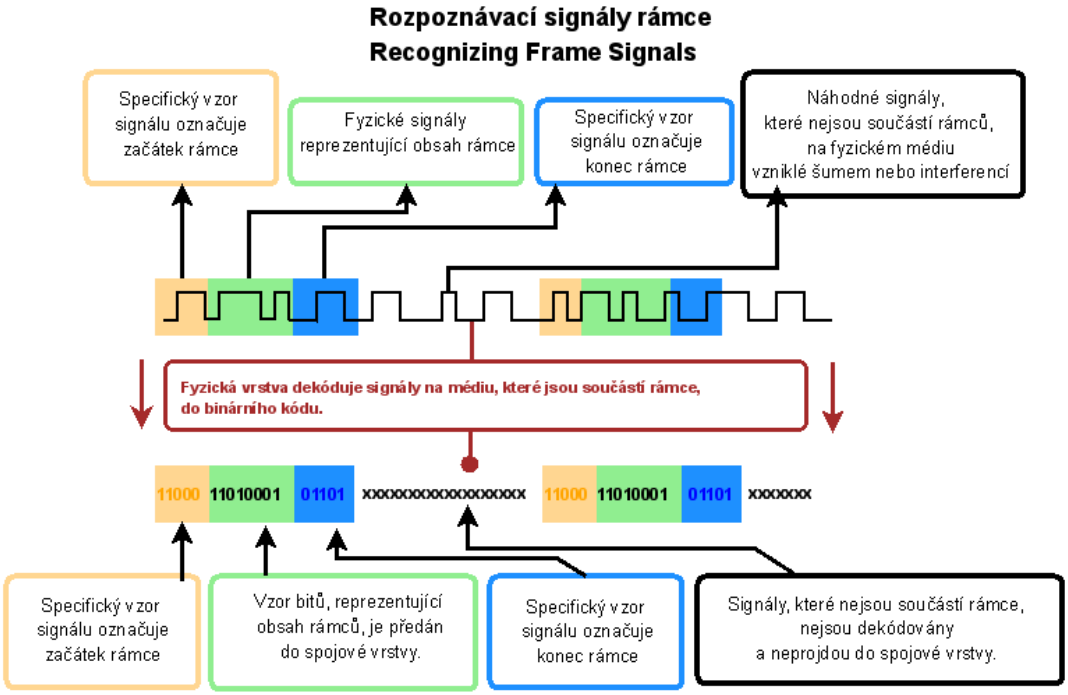
4B/5B

4B/5B - je to varianta **blokového kódování** - kdy se 4 bity dat převádějí na skupinu 5 bitů pro přenos. Každý bajt je rozdělen do dvou skupin po čtyřech bitech (*nibbles*) a každé tyto čtyři bity jsou zakódovány do pětibitové hodnoty známé jako **symbol**. V jednom symbolu mohou za sebou být nejvýše tři nuly. Například: původní 4 bitový kód 0001 je nově zakódován jako 01001. Speciální symboly určují začátek a konec rámce. Kódování zaručuje, že se v každém symbolu je nejméně jedna změna úrovně, což zaručuje synchronizaci. Původní čtyři bity mají 16 kombinací a nových 5 bitů má 32 kombinací, tzn. Že máme navíc další symboly se speciálními funkcemi (6 symbolů/kódů: konec a začátek toku dat, chyba, neobsazená linka (*idle*)) a 10 dalších kódů je neplatných. 4B/5B se používá ve FastEthernetu (100BASE-TX), HDLC a FDDI.

Příklad kódování 4B5B:

Jméno - Name	*4b*	*5b*	*Popis symbolu - Description*
0	0000	11110	hex data 0
1	0001	01001	hex data 1
2	0010	10100	hex data 2
3	0011	10101	hex data 3
4	0100	01010	hex data 4
5	0101	01011	hex data 5
6	0110	01110	hex data 6
7	0111	01111	hex data 7
8	1000	10010	hex data 8
9	1001	10011	hex data 9
A	1010	10110	hex data A
B	1011	10111	hex data B
C	1100	11010	hex data C
D	1101	11011	hex data D
E	1110	11100	hex data E
F	1111	11101	hex data F
I	-NONE-	11111	Idle
J	-NONE-	11000	SSD #1
K	-NONE-	10001	SSD #2
T	-NONE-	01101	ESD #1
R	-NONE-	00111	ESD #2
H	-NONE-	00100	Halt

SSD= Start of Stream Delimiter (100BASE-TX Ethernet)
ESD= End of Stream Delimiter (100BASE-TX Ethernet)



Přenosová kapacita

Měrné jednotky pro přenos dat (kapacita přenosu):

- ***Bandwidth* – přenosová kapacita,** (digitální) **přenosová rychlost**[70] **/** (analogová) šířka pásma: efektivní množství informací, dat, bitů přenesených z jednoho místa na druhé v jednom segmentu sítě za jednotku času (obvykle udávané v kbps = kb/s, nebo v Mbps = Mb/s) – je dané přenosovým médiem a použitou technologií.
- ***Throughput* – propustnost**: množství dat přenesených celou přenosovou cestou (udávané ve stejných jednotkách jako přenosová rychlost). Závisí na zatížení sítě, použitých jednotlivých technologiích, je určeno nejpomalejším místem cesty.
- ***Goodput* – propustnost na aplikační úrovni:** přenesené množství užitečných aplikačních dat celou přenosovou cestou za jednotku času.

Násobné jednotky (prefixy)

Dekadické prefixy:

Kilobit za sekundu (kbit/s, kb/s, nebo kbps) - 1 kb/s = 10^3 b/s = 1 000 b/s.

Megabit za sekundu (Mbit/s, Mb/s, nebo Mbps) - 1 Mb/s = 10^6 b/s = 1 000 000 b/s.

Gigabit za sekundu (Gbit/s, Gb/s, nebo Gbps) - 1 Gb/s = 10^9 b/s = 1 000 000 000 b/s.

70 Bitová rychlost – počet přenesených bitů za sekundu. Modulační (Baudová, bd) rychlost – počet změn signálu za sekundu. NRZ: 1bd = 1b . Manchester: 2bd = 1 b .

Terabit za sekundu (Tbit/s, Tb/s, nebo Tbps) – 1Tb/s = 10^{12} b/s = 1 000 000 000 000 b/s.

Existují také násobné jednotky vycházející z násobků 2 (**binární prefixy**):

Kibibit za sekundu (Kibit/s, Kib/s, nebo Kibps) - 1 Kib/s = 2^{10} b/s = 1 024 b/s.,

Mebibit za sekundu (Mibit/s, Mib/s, nebo Mibps) - 1 Mib/s =2^{20} b/s = 1 048 576 b/s.,

Gibibit za sekundu (Gibit/s, Gib/s, nebo Gibps) - 1 Gib/s = 2^{30} b/s = 1 073 741 824 b/s,

Tebibit za sekundu (Tibit/s, Tib/s, nebo Tibps) – 1Tib/s = 2^{40} b/s = 1 099 511 627 776 b/s.

Aktivní prvky sítí na první vrstvě (L1) v Ethernetu

- **Opakovač (*Repeater*)** – dvouportový digitální zesilovač – signál z jednoho portu zesílí a předá druhému portu.
- **Rozbočovač (*Hub*)** – víceportový opakovač – signál z jednoho portu zesílí a předá na všechny ostatní porty.

Standardy pro měděná média

jsou definovány pro:

- Typ použitého měděného kabelu,
- přenosovou rychlost komunikace,
- typ použitých konektorů,
- kontakty na konektorech a barevné kódy jejich připojení k médiu,
- maximální použitelná délka média.

Ethernet - fyzické charakteristiky média

	10BASE-T[71]	***100BASE-TX***	***100BASE-FX***	***1000BASE-CX***	***1000BASE-T***	***1000BASE-SX***	***1000BASE-LX***	***1000BASE-ZX***	***10GBASE-ZR***
médium	EIA/TIA kategorie 3, 4, 5 UTP 4 páry	EIA/TIA kategorie 5 UTP 2 páry	50/62,5 mikronů MMF	STP[72]	EIA/TIA kategorie 5 **nebo vyšší** UTP 4 páry	50/62,5 mikronů MMF	50/62,5 mikronů MMF **nebo** 9 mikronů SMF	9 mikronů SMF	9 mikronů SMF
maximální délka segmentu	100m	100m	2km	25m	100m	do 550m v závislosti na použitém optickém kabelu	550m (MMF) 10km (SMF)	cca 70km	do 80km
topologie (fyzická)	hvězda	hvězda	hvězda	hvězda	hvězda	hvězda	hvězda	hvězda	hvězda
konektor	ISO 8877 RJ-45	ISO 8877 RJ-45		ISO 8877 RJ-45	ISO 8877 RJ-45				

Poznámky:
SMF (Single Mode Fiber) – jednovidový optický kabel
MMF(Multi-mode Fiber) – vícevidový optický kabel

71 Struktura názvu Ethernetové technologie (např. 10BASE-T) je složena z: přenosová rychlost v Mbps, BASE = základní šířka pásma na jednom přenosovém kanálu a označení přenosového média (T = UTP, F = Fiber, ...).

72 STP zde Shielded Twisted Pair – stíněná kroucená dvoulinka.

Bezdrát (wireless) - fyzické charakteristiky média

Charakteristika/ Standard	Bluetooth 802.15	802.11 (a, b, g, n), HiperLAN 2	802.11 MMDS[73], LMDS[74]	GSM, GPRS, CDMA, 2.5 - 3G[75]
rychlost	< 1Mbps	1 – 54+ Mbps	22+ Mbps	10 – 384 Kbps
dosah	malý	střední	střední – velký	velký
použití	peer-to-peer device-to-device	podniková síť	pevný dálkový spoj	PDA, mobilní telefony

Měděná média

Nejpoužívanější přenosové médium jsou kabely používající měděné dráty pro přenos datových a řídících signálů mezi síťovými zařízeními. Kabel pro komunikaci se obvykle skládá ze sady jednotlivých měděných drátů, které vytvářejí obvody vyhrazené pro určitý signalizační účel.
Jiné typy kabelů, známé jako **koaxiální kabely** mají jeden vodič, který jde středem kabelu a kolem něho vodivé stínění oddělené izolací.
Tyto kabely mohou spojovat uzly LAN s propojovacími zařízeními (jako jsou routery a switche). Kabely mohou také propojovat zařízení WAN s poskytovatelem služby (telefonní společnost). Každý typ propojení a připojených zařízení má své požadavky na kabeláž definované standardy fyzické vrstvy.
Síťová média všeobecně používají modulární zástrčky (*jack*) a zásuvky (*plug*), které umožňují snadné zapojení a rozpojení. Jeden druh fyzického konektoru může také být použit pro více typů připojení. Například konektor RJ-45 je široce používán v LAN s jedním druhem média a některých WAN je použit s jiným typem média.

Interference vnějších (externích) signálů

Data jsou v měděných kabelech přenášena v podobě elektrických pulzů. V cílovém síťovém rozhraní musí být přijaté signály úspěšně dekódovány tak, aby byl shodné s vyslanými signály.
Hodnoty časování (tempa) a elektrického napětí těchto signálů jsou snadno ovlivnitelné interferencemi nebo elektromagnetickým „šumem“ (*noise*) z vnějšku komunikačního systému. Tyto nežádoucí signály mohou zkreslit a zkazit datové signály přenášené přes měděná média. Potenciálními zdroji šumu jsou rozhlasová a elektromagnetická zařízení jako zářivková světla, elektrické motory, atd.
Typy kabelů se stíněním (*shielding*) nebo zkroucením párů (*twisting*) jsou navrženy tak, aby mini-

73 Multichannel multipoint distribution service – pro broadband – vysokorychlostní přenos.
74 Local Multipoint Distribution Service - IEEE 802.16.1 – také broadband na pásmu 26GHz.
75 Global System for Mobile Communications (GSM) – obsahuje specifikace fyzické vrstvy, které umožňují implementovat L2 protokol General Packet Radio Service (GPRS) pro datový přenos prostřednictvím mobilních telefonních sítí.GPRS – (General Packet Radio Service) základní služba umožňující mobilnímu telefonu (či jinému přenosnému zařízení) připojení se k Internetu prostřednictvím mobilní (GSM, Global System for Mobile Communications) sítě. Je široce dostupná, ale velmi pomalá.
EDGE - „nadstavba“ GPRS – technologie umožňující rychlejší připojení k Internetu prostřednictvím mobilní (GSM) sítě. Od operátora však požaduje použití novějšího hardwaru, tudíž není dostupná všude tam, kde se lze připojit přes GPRS.
CDMA – v našem kontextu technologie mobilních sítí třetí generace (3G) pro vysokorychlostní připojení. Je realizovaná na frekvenci, kterou dříve používala starší mobilní síť a u nás ji nabízí výhradně společnost O2.
HSDPA/UMTS – v současné době nejmodernější u nás používaná technologie pro mobilní připojení k Internetu. Je nejrychlejší a zároveň nejméně dostupná.

malizovaly degradaci signálu způsobenou **elektromagnetickým (elektronickým) šumem**. (Podle frekvence rozlišujeme elektromagnetickou interferenci vlivem elektromagnetické indukce na **EMI** (*Electromagnetic Interference*) a **RFI** (*Radio Frequency Interference*) (interference na rozhlasových vlnách).)
Náchylnost měděných kabelů na elektronický šum lze také omezit pomocí:

- výběru typu kabelu nebo kategorie nejvhodnější pro ochranu datových signálů v daném síťovém prostředí,
- návrhu kabelové infrastruktury tak, aby se vyhnula známým a potenciálním zdrojům interference uvnitř infrastruktury budov,
- použití vhodných technik, jako jsou správné zacházení a zakončování kabelů.

UTP

***Unshielded twisted-pair (UTP)* – nestíněná kroucená dvoulinka.** UTP kabely se používají v Ethernetových sítích (jako nejčastěji používané médium). Skládají se ze čtyř zkroucených párů vodičů (zkroucení omezuje interferenci signálu, elektromagnetickou indukci cizího signálu), izolace jednotlivých drátů jsou označeny barevnými kódy. Z vnějšku jsou páry chráněny ohebným plastovým pláštěm. Důležité je správné zakončení kabelů (*cancelation*) (správné připojení zástrčky RJ-45 tak, aby páry byly zkrouceny až do konektoru (což zabraňuje vzniku přeslechů[76] (*crosstalks*) = interferencí mezi jednotlivými páry samotného jednoho UTP), upevnění konektoru, doražení kabelu „nadoraz“ v konektoru). Kabely UTP se vyrábějí v provedení kdy jednotlivý vodič v páru je drát (*solid*) nebo lanko (*strand*) k tomu potom odpovídá varianta konektoru RJ-45 (drát nebo lanko). POZOR: nezaměňujte je! Pro drát má jeden kontakt v RJ-45 3 hroty – prostřední hrot obemkne drát z jedné strany a dva krajní hroty z druhé strany. Pro lanko má kontakt dva hroty v jedné rovině, které proseknou lanko uprostřed. Pokud použijete pro drát variantu pro lanko, drát se ohne a může se (po čase a po mechanickém namáhání) zlomit, či dojde ke zkratu.
UTP se vyrábějí v různých kategoriích (Cat 3, Cat 5e, ...), čím vyšší kategorie kabelu, tím vyšší přenosová rychlost (*bandwitch*).

Standardy kabelů UTP

Standardy jsou společně vytvořeny Telecommunications Industry Association (TIA) a Electronics Industries Alliance (EIA). **TIA/EIA-568A** a **TIA/EIA-568B** určuje komerční standard kabelů pro instalace LAN (zapojení konkrétních kontaktů konektorů na jednotlivé barevné kódy drátů). Některé těmito standardy definované prvky:

- typy kabelu,
- délky kabelu,
- konektory,
- kabelová zakončení,
- metody testování kabelu.

76 Přeslech se měří v dB (decibel) což je obecná logaritmická jednotka pro měření podílu dvou hodnot.

Typy kabelů UTP - Přímý, překřížený a převrácený kabel

Typ kabelu	*Standard*	*Použití*
Přímý (Ethernet Straight-through)	oba konce T568A nebo oba konce T568B	Propojení síťového hostitele (PC) a zařízení typu switch nebo hub.[77]
Překřížený (Ethernet Crossover)	jeden konec T568A a druhý konec T568B (překřížené páry 2 a 3)	Propojení dvou hostitelů. Propojení dvou síťových propojovacích zařízení (switch na switch nebo router na router).[78]
Převrácený (Rollover)	Cisco (proprietární standard) Propojení kontaktů (pin) na protilehlých koncích: 1 – 8, 2 – 7, 3 -6, 4 – 5, ... , 8 - 1	Propojuje sériový port pracovní stanice s konzolovým portem směrovače. (Použití redukce.)

Standardy TIA T568A a T568B pro zapojení konektoru RJ-45

PIN	***T568A***	***T568B***	***Funkce pinu na síťové kartě 100BASE-T***
1	Bílá / Zelená	Bílá / Oranžová	TD+
2	Zelená	Oranžová	TD-
3	Bílá / Oranžová	Bílá / Zelená	RX+
4	**Modrá**	**Modrá**	nezapojené
5	**Bílá / Modrá**	**Bílá / Modrá**	nezapojené
6	Oranžová	Zelená	RX-
7	Bílá / Hnědá	Bílá / Hnědá	nezapojené
8	Hnědá	Hnědá	nezapojené

TD – *transmission* - vysílání
RX – *receiving* - příjem
\+ signál
\- zem (*ground*)

Čísla barevných párů v kabelu UTP (jsou stejné pro obě normy)

Pár	***Barevný kód***
1	modrý
2	oranžový
3	zelený
4	hnědý

77 Logicky různá zařízení. (DTE – DCE). Zařízení jsou následující: DTE = PC, Router; DCE= switch, bridge, hub, AP.
78 Logicky stejná zařízení. DTE-DTE nebo DCE-DCE.

Konektory pro UTP

RJ-45 (*Registered Jack – 45*) - zástrčka (*plug*) a k ní odpovídající zásuvka (*socket*).

Zásady správného zakončení UTP kabelu (instalace zástrčky RJ-45): Páry rozplétat pouze na nejmenší možnou délku. Vnější plášť kabelu musí být zacvaknutý v zástrčce. Nedbale provedené zakončení kabelu vede ke vzniku přeslechů (*crostalks*) na kabelu. Přeslechy mají neblahý vliv na celkový výkon přenosu dat (snižují propustnost).

Postup instalace konektoru RJ-45 na kabel UTP

Nezraňte se o ostré břity krimpovacích kleští.

1. Stahovákem odstraňte cca 4 cm vnějšího pláště (bužírky) z jednoho konce kabelu.
2. Rozpleťte páry a narovnejte jednotlivé vodiče.
3. Srovnejte vodiče dle správného pořadí barev (TIA/EIA 568A nebo 568B) – podle zvoleného typu kabelu (přímý nebo překřížený).
4. Zastřihněte správnou délku vodičů (tak, aby šly zasunout do zástrčky a bužírka kabelu byla fixována v zástrčce).
5. Zasuňte kabel do správné varianty konektoru (drát nebo lanko).
6. Zkontrolujte správné pořadí barev vodičů, jejich doražení do konce zástrčky a to, že vnější bužírka bude po zamáčknutí kleštěmi dobře fixována v zástrčce (páry jsou zkrouceny až co nejblíže je to možné ke kontaktům (pinům) konektoru).
7. Vložte konektor ve správném směru do krimpovacích kleští (*crimp tool*) a domáčknete.
8. Stejným postupem nacvakněte i druhou stranu kabelu
9. Změřte funkčnost kabelu.

Další měděná média

Koaxiální kabel

Koaxiální kabel - někdy používaná zkratka názvu je koax.

Struktura kabelu: centrální měděný vodič, plastová izolace, oplet – měděné pletené stínění, vnější plášť z PVC.

Použití: anténní přívody pro bezdrátové technologie na rozhlasových kmitočtech (RF). Také koncové přívody od konvertorů z optických datových vedení – hybridní technologie HCF. Dříve se také koaxiální kabel používat v technologiích tenkého (10BASE-2) a silného (10BASE-5) Ethernetu.

Konektory: BNC – Bayonette Neil-Concelman Connector (někdy též uváděno jako British Naval Connector) – oblíbený bajonetový konektor. Další typy šroubovacích konektorů pro rozhlasové kmitočty: Typ N, Typ F.

STP

***Shielded Twisted Pair (STP)* – stíněná kroucená dvoulinka.**

Struktura kabelu: **dva (nebo čtyři) kroucené páry** (dvoulinky), každý pár je samostatně stíněn hliníkovou fólií, všechny páry se stíněním jsou potom v jednom opletu – měděné pletené stínění, na povrchu je plastový plášť.

Použití: 10BASE-TX, 1000BASE-CX, v podobě S/FTP také 10GBASE-T.

Bezpečnost měděných přenosových médií

- Riziko elektrického napětí – průraz nebo poškození izolace silového napájecího vedení vede k poškození nízkonapěťových zařízení datových sítí nebo k úrazu personálu.
- Riziko vzniku ohně při elektrickém zkratu. Hořící plastová izolace produkuje jedovaté zplodiny.

Zásady

- Fyzické oddělení silového a datového kabelového rozvodu. Barevné značení jednotlivých druhů vedení.
- Správné připojení konektorů a jejich zapojení do zařízení.
- Pravidelné inspekce stavu a poškození kabelových rozvodů.
- Správné uzemnění jednotlivých zařízení.

Optické kabely

Optické kabely používají buď sklo nebo plastiková (umělohmotná) vlákna, aby vedly světelné impulzy ze zdroje do cíle. Bity jsou ve vlákně zakódovány jako světelné impulzy. Optické kabely mají kapacitu přenášet prvotní data velkou přenosovou rychlostí. Většina nových standardů využívá právě proto toto přenosové médium. Nejčastější použití v kabelových rozvodech páteřních sítí (*backbone*).
Pro každý směr přenosu (vysílání - Tx, nebo příjem - Rx) se používá samostatný kabel nebo samostatné vlákno. Vlákno z vysílače na jedné straně musí být zapojeno do přijímače na druhé straně a naopak.
Světlo je na straně přijímače převáděno na elektrické impulsy polovodičovými součástkami – fotodiodami. Zdroj světla je buď LED dioda (*light emitting diode*) nebo laser.

Varování: světlo laseru přenášené optickým kabelem není viditelné, ale přesto může zničit lidské oko. Nedívejte se proto nikdy do konců aktivních optických kabelů!

Průřez optickým kabelem:

- **Skleněné jádro** (*Core*) – vodič světla. Jedná se o nejdůležitější prvek vlákna určený pro vlastní přenos dat. Průměr jádra závisí na typu kabelu. Standardními rozměry jsou 9, 50 a 62.5µm (mikrometrů),
- **Skleněný obal jádra** (plášť) (*Cladding*) – zajišťuje, že světlo neuniká z jádra (zmenšuje rozptyl světla), tato část má za úkol také ochranu a zpevnění jádra. Spolu s jádrem má průměr 125µm.,
- **Primární ochrana (tlumič) jádra** (*Buffer*) – jedná se o vrstvu, která slouží k prvotní

ochraně optického vlákna od nepříznivých účinků okolního prostředí. Vrstva je nejčastěji tvořena tvrzeným akrylátovým lakem a spolu s jádrem a obalem jádra má průměr 250μm,
- **Aramidová vlákna** (*Aramid Yarn*) – pro zpevnění a ochranu skleněného jádra a pláště,
- **Vnější plášť** (*Jacket*) – vnější ochrana kabelu, obvykle z PVC.

Rozptyl světla v optickém kabelu je (kromě konstrukce a materiálu kabelu) přímo úměrný jeho délce.

Implementace optických kabelů má (ve vztahu k měděným médiím) následující výhody ale i nevýhody:

Výhody použití optiky vzhledem k mědi	*Nevýhody*
• delší použitelná vzdálenost, • větší přenosová rychlost,	• jsou (obvykle) dražší než měděná média pro stejnou vzdálenost (mají ale větší přenosovou kapacitu), • pro ukončování a dělení kabelů je třeba jiných znalostí a jiného (dražšího) vybavení než pro měděné kabely, • je třeba s nimi mnohem opatrnější manipulace než s měděnými kabely.

Módy (režimy) optických kabelů

Single-mode – SMF (jednovidový)	*Multimode – MMF (vícevidový)*
Skleněné jádro = průměr 8 - 10 mikronů Skleněný obal jádra = průměr 125 mikronů jedna přímá cesta pro světlo	Skleněné jádro = průměr 50 / 62,5 mikronů Skleněný obal jádra = průměr 125 mikronů dovoluje více cest pro světlo (odrazy od obalu jádra)
• tenké jádro • malý rozptyl (*dispersion*), minimální ztráty signálu (*signal loss*) • pro dlouhé vzdálenosti <= 100km • jako zdroj světla používá laser – vlnová délka 1300 nm (nanometr, 10^{-9} m)	• větší jádro vzhledem k jednovidovému kabelu • dovoluje větší rozptyl a z toho plynou ztráty signálu • pro dlouhé vzdálenosti, ale menší než jednovidové vlákno <= cca 2km • jako zdroj světla používá optické diody LED – vlnová délka 850 nm

Konektory pro optické kabely

ST (*Straight Type*) – přímý typ, vyvinutý firmou AT&T, běžný bajonetový konektor.
SC (*Subscriber Connector*) – pro SMF.
LC (*Lucent Connector*) – také pro SMF.

Měření na optických kabelech

OTDR - optický reflektometr (*Optical Time Domain Reflectometer*) používající metodu zpětného rozptylu.

Typy bezdrátových sítí

Bezdrátová média přenášejí elektromagnetické signály na rozhlasových a mikrovlnných frekvencích, které reprezentují bity datové komunikace. Jako síťové médium, bezdrát není omezen vodiči nebo vedením jako jsou měděné nebo optické kabely.

Bezdrátová komunikační technologie pracuje dobře v otevřeném prostoru. Přesto některé konstrukční materiály použité v budovách a konstrukcích stejně jako typ terénu omezují efektivní pokrytí (*coverage*). Navíc je bezdrátová komunikace náchylná k interferencím a může být narušena takovými běžnými zařízeními jako jsou bezdrátové telefony, některými typy fluorescenčních světel, mikrovlnnými troubami, a také jinou bezdrátovou komunikací.

A dále, protože pokrytí bezdrátovou komunikací nevyžaduje přístup k fyzickému prvku média, zařízení a uživatelé, kteří nejsou autorizováni pro přístup do datové sítě, mohou přistupovat k přenosu. Proto je síťová bezpečnost hlavní komponentou administrace bezdrátové sítě.

Standardy IEEE a telekomunikačního průmyslu pro bezdrátovou komunikaci pokrývají obě dvě vrstvy spojovou i fyzickou. Čtyři obvyklé komunikační standardy pro bezdrátová média jsou:

- **IEEE 802.11** – obvykle uváděné jako **Wi-Fi** je technologie bezdrátové LAN (**WLAN**, *Wireless LAN*), která používá soutěžní nedeterministickou přístupovou metodu Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA).
- **IEEE 802.15 - *Wireless Personal Area Network* (WPAN)** obvykle známá jako **"*Bluetooth*"** používá proces párování zařízení na vzdálenost 1 – 100 metrů.
- **IEEE 802.16 -** obvykle známá jako **WiMAX (*Worldwide Interoperability for Microwave Access*)** používá topologii point-to-multipoint pro bezdrátový vysokorychlostní přístup (wireless broadband access). Jde o **WWAN (*Wireless WAN*)**.
- ***Global System for Mobile Communications* (GSM)** – obsahuje specifikace fyzické vrstvy, které umožňují implementovat L2 protokol ***General Packet Radio Service* (GPRS)** pro datový přenos prostřednictvím mobilních telefonních sítí.

Další bezdrátové technologie jako je satelitní komunikace poskytuje datové připojení pro oblasti bez jiného dostupného připojení. Protokoly (včetně GPRS) umožňují přenos dat mezi pozemními stanicemi a satelitními linkami.
Pro všechny shora uvedené příklady, specifikace fyzické vrstvy jsou aplikovány na následující oblasti: kódování dat na rádiový signál, frekvence a výkon vysílání, příjem signálu a jeho dekódování, návrh a konstrukce antén.

WLAN

Umožňují bezdrátové připojení prostřednictvím LAN. Obecně WLAN požaduje následující síťová zařízení:

- **bezdrátový přístupový bod (AP, *Access Point*, W-AP)** – koncentruje bezdrátové signály od uživatelů a je (obvykle přes měděný Ethernetový kabel) připojen do stávající síťové infrastruktury (Ethernet LAN).
- **bezdrátová síťová karta (W-NIC)** – bezdrátová komunikace pro každého hostitele sítě.[79]

Jak se technologie rozvíjela, bylo vytvořeno množství standardů založených na Ethernet WLAN. Je třeba při koupi bezdrátového zařízení dávat pozor na kompatibilitu a interoperabilitu.

79 Karta se připojí (přidruží, associate) ke zvolenému AP v infrastrukturní síti (W-AP – W-NIC) – proces „Scanning“ : Uzel pošle „Probe“. Všechny slyšící AP pošlou „Probe Response“ . Uzel si vybere jeden a pošle „Association Request“. Příslušný AP odpoví „Association Response“.

Standardy WLAN

- **IEEE 802.11a** – pracuje na frekvenčním pásmu 5 GHz a nabízí rychlosti do 54 Mbps. Protože tento standard pracuje na vyšších frekvencích, má menší oblast pokrytí (coverage area) a méně efektivní průnik do struktury budov. Zařízení v tomto standardu nespolupracují s normami 802.11b a 802.11g popsanými dále.
- **IEEE 802.11b** - pracuje na frekvenčním pásmu 2.4 GHz a nabízí rychlosti do 11 Mbps. Zařízení implementující tento standard mají větší dosah a lépe pronikají do budov než zařízení pracující na standardu 802.11a.
- **IEEE 802.11g** - pracuje na frekvenčním pásmu 2.4 GHz a nabízí rychlosti do 54 Mbps. Zařízení implementující tento standard proto pracují na stejné rozhlasové frekvenci a dosahu jako 802.11b ale s rychlostí standardu 802.11a.
- **IEEE 802.11n** – Standard IEEE 802.11n je v současnosti ve formě návrhu (draft) – respektive verze 2009. Navrhovaný standard definuje frekvenci 2.4 GHz nebo 5 GHz. Typické očekávané přenosové rychlosti jsou 100 Mbps až 210 Mbps s dosahem vzdálenosti do 70 metrů. Jednotliví výrobci tato zařízení již vyrábějí dle své modifikace normy.

Výhody bezdrátové datové komunikace jsou evidentní, zvláště úspora nákladů za kabeláž a výhodnost mobility hostitelů. Přesto síťoví administrátoři musí navrhnout a zavést striktní bezpečnostní politiku a postupy, aby ochránili WLAN před neautorizovaným přístupem a škodami.

Bezdrátové standardy budou mnohem podrobněji probrány v kurzu *CCNA3 Exploration LAN Switching and Wireless*.

Cvičení

1. Nacvakání zástrčky RJ-45 na UTP kabel kategorie 5e pomocí „krimpovacích“ kleští, otestování testerem - LED „pípákem“ či měřícím přístrojem (např. firmy Fluke). Přímý nebo křížený kabel.
2. Konvertor (*bridge*) optického kabelu MMF na FastEthernet 100BASE-T, zapojení a otestování funkce. Nezapomeňte, že optický kabel musíte zapojit „překříženě“ - vysílač Tx na přijímač Rx a naopak (nebo zapnout automatické přehození vláken).
3. Bezdrátový přístupový bod Linksys WAP54G, nastavení i otestování provozu v režimu AP a klient.
4. PT cvičení WiFi_WRT300N.pka, WLAN_trouble.pka.

Pamatujte si, pokud spojení nefunguje, testujeme postupně od první vrstvy OSI modelu (funkční kabely, správné konektory, správné zapojení kabelů do portů, indikační kontrolky pro L1 na příslušných zařízeních) přes druhou vrstvu (odposlech rámců, indikační kontrolka příjmu signálu na zařízení) do třetí vrstvy (ping). Test funkce všech sedmi vrstev na úrovni aplikačního protokolu - například vzdáleným přihlášením se přes Telnet.

Kontrolní opakovací otázky a odpovědi (kvíz):

1) Přiřaďte k jednotlivým číslům kontaktů (*pinouts*) v propojovacím montážním kabelu (*patch cable*) dle normy 568B odpovídající barvy páru:

   a) 7 a 8: hnědá,

   b) 1 a 2: oranžová,

c) 3 a 6: zelená,

d) 4 a 5: modrá.

2) Přiřaďte k jednotlivý číslům kontaktů konektoru RJ-45 na jedné straně správná čísla kontaktů na druhé straně v případě konzolového kabelu (*rollover*) na směrovači:

a) 1 – 8

b) 2 – 7

c) 3 – 6

d) 4 – 5

e) 5 – 4

f) 6 - 3

g) 7 - 2

h) 8 – 1

3) Jaký typ propojení je mezi PC a směrovačem pomocí převráceného kabelu (rollover cable) (na jednom konci RJ-45 (v konzolovém portu směrovače) a na druhém sériový konektor DB-9 (v sériovém portu COM v PC)?

a) Konzolové připojení

4) Jaký je účel kódování (*encoding*) (= kódování signálu)?

a) Reprezentace datového bitu pomocí různých napětí, světelných vzorů nebo elektromagnetických vln které jsou umisťovány na fyzické (přenosové) médium.

5) Jaký je nejlepší popis účelu fyzické vrstvy?

a) Definuje funkční specifikace pro linku mezi koncovými systémy a elektrické, optické či elektromagnetické signály.

6) Jakým způsobem UTP předchází vzniku přeslechů (*crosstalks*)?

a) Zkroucením jednotlivých párů (zmenší se tím plocha smyčky pro elektromagnetickou indukci)

7) Uveďte tři výhody použití optického kabelu proti měděnému kabelu:

a) imunita pře elektromagnetickou interferencí,

b) delší maximální délka kabelu,

c) větší potenciál přenosové kapacity (*bandwidth*).

8) Jaký typ kabelu by mohl být použit pro přímé spojení dvou počítačů (přes Ethernet)?

a) Překřížený (*crossover*) UTP.

9) Jaký je účel skleněného ochranného obalu jádra (*cladding*) u optického kabelu?

a) Zabraňuje ztrátám světla (světelného signálu).

Kapitola 9 – Ethernet

V této kapitole se naučíme:

- Popsat evoluční vývoj Ethernetu
- Vysvětlit jednotlivá políčka Ethernetového rámce
- Popsat funkce a charakteristiky metod řízení přístupu k médiu, které jsou použity v protokolu Ethernet
- Popsat funkce Ethernetu na fyzické a spojové vrstvě
- Porovnat a zdůraznit rozdíly mezi ethernetovým rozbočovačem a přepínačem
- Vysvětlit protokol ARP (*Address Resolution Protocol*)

Ethernet - úvod

Ethernet je na světě převládající technologií pro LAN (více než 80%). Přesto, že používá různá média, přenosové rychlosti i různí jiné odlišnosti na první a druhé vrstvě OSI modelu má stále stejný formát rámce a stejné adresní schéma pro všechny varianty Ethernetu.

Postupný vývoj od sdíleného přenosového média a soutěžní přístupové metody s použitím poloviční duplexu (*half-duplex*) až k nesdílenému médiu (virtuálnímu dvoubodovému spojení) a plnému duplexu (*full-duplex*) u přepínaného Ethernetu.

Standardy IEEE[80]

IEEE 802 – skupina standardů pro LAN.[81]

Vrstva modelu OSI	***Standard***
L2 – podvrstva LLC	IEEE 802.2 – pro podvrstvu LLC obecné sítě
L2 – podvrstva MAC	IEEE 802.3 – Ethernet (1985)
L1 – fyzická vrstva	

Ethernet pracuje na L1 i L2.

Porovnání obou spodních vrstev OSI modelu

L1 – omezení	***L2 - funkce***
Nemůže komunikovat s vyššími vrstvami	Připojuje se k vyšší vrstvě (L3) prostřednictvím LLC
Nemůže identifikovat síťové zařízení	Používá adresní schéma k identifikaci konkrétního zařízení
Rozeznává pouze tok bitů (symbolů, signálu)	Používá rámce k zorganizování bitů do skupin.
Neidentifikuje zdroj přenosu, když vysílá	Používá MAC adresu k identifikaci zdroje

80 IEEE - Institute of Electrical and Electronics Engineers, Inc.

81 Na rozdíl od obecně formulovaných RFC (IETF) pro sadu TCP/IP na vrstvách L3 až L7 jsou standardy pro L1 až L2 od IEEE, ANSI, ITU zcela konkrétní. Skupina 802 v sobě zahrnuje celou řadu standardů: 802.1q, 802.2, 802.3 atd.

najednou více zařízení	přenosu

Podvrstvy spojové vrstvy

LLC

***Logical Link Control* (LLC)** – horní podvrstva *řízení logického spoje* u spojové vrstvy je odpovědná za:

- připojení k vyšším vrstvám,
- zapouzdření paketů ze síťové vrstvy do rámců,
- identifikaci protokolu síťové vrstvy.
- LLC je relativně nezávislá na fyzickém zařízení,
- LLC je realizována softwarově – ovladačem síťové karty.

<table>
<tr><td colspan="9">Podvrstva LLC</td><td></td><td rowspan="4">Ethernet</td></tr>
<tr><td colspan="9">802.3 MAC</td><td>Ethernet MAC</td></tr>
<tr><td rowspan="2">Podvrstva přenosu fyzických signálů</td><td rowspan="3">10BASE5 (500m) 50 ohmů Coax N Style</td><td rowspan="3">10BASE2 (185m) 50 ohmů Coax BNC</td><td rowspan="3">100BASE-T (100m) 100 ohmů UTP RJ-45</td><td rowspan="3">100BASE TX (100m) 100 ohmů UTP RJ-45</td><td rowspan="3">100BASE CX (25m) 150 ohmů STP mini DB9</td><td rowspan="3">1000BASE-T (100m) 100 ohmů UTP RJ-45</td><td rowspan="3">1000BASE-SX (220 - 550m) MM Fiber SC</td><td rowspan="3">1000BASE-LX (550 - 5000m) MM nebo SM Fiber SC</td><td rowspan="3">Ethernet PHY</td></tr>
<tr><td>Fyzická vrstva</td></tr>
</table>

MAC

MAC (Medium Acces Control) – spodní podvrstva *řízení přístupu na médium* je zodpovědná za:

- zapouzdření dat:
  - ohraničení rámce (synchronizace mezi vysílacím a přijímacím uzlem),
  - adresace (fyzická adresa MAC),
  - detekce chyb (CRC, FCS)
- řízení přístupu k médiu:

- řízení umístění a vyjmutí rámce na a z média,
- zotavení média po chybě.

Fyzická implementace Ethernetu (PHY)

Úspěch Ethernetu zapříčinily následující faktory:

- jednoduchost a snadná údržba,
- schopnost zahrnovat do sebe nové technologie,
- relativní spolehlivost (Ethernet je nespojovaný protokol a z tohoto pohledu (z pohledu protokolu) je „nespolehlivý“ = nepotvrzuje správné doručení dat příjemcem.)
- nízká cena instalace a aktualizace (*upgrade*).

Používaná fyzická zařízení:

- propojovací montážní panely UTP (*UTP Patch Panel*) instalované ve stavebnicových regálech / stojanech (*rack*), strukturovaná vyvázaná kabeláž,
- stohovací switche instalované ve stavebnicových regálech (*rack*)[82],
- konvertory (asymetrický bridge): například konverze UTP na optický kabel.

Historický Ethernet a jeho vývoj

- 1970: Alohanet (slovo *aloha* je havajský pozdrav) – digitální datová síť na rozhlasových frekvencích mezi havajskými ostrovy. Sdílené přenosové médium. Přístupová metoda: *aloha* – soutěžní nedeterministická metoda přístupu k médiu, předchůdce CSMA/CD (i CSMA/CA).
- 1973-75: Robert Metcalfe, Xerox_PARC, Palo Alto - Ethernet sdílené přenosové médium. "Draft Ethernet Overview" březen 1974. Přenosová rychlost 3Mbps.
- 1982: Standard Ethernet II (DIX v2.0).
- 1983: 10BASE5 - „tlustý“ Ethernet (Thicknet), koax, segment max 500m, sdílené médium, přístupová metoda: CSMA/CD, half-duplex, fyzická topologie: lineární sběrnice (*bus*), logická topologie: lineární sběrnice (*bus*),
- 1985: 10BASE2 - „tenký“ Ethernet (Thinnet), koax, segment max 185m, masové rozšíření, sdílené médium, přístupová metoda: CSMA/CD, half-duplex, fyzická topologie: lineární sběrnice (*bus*), logická topologie: lineární sběrnice (*bus*),
- 1990: 100BASE-T – FastEthernet - UTP + hub, UTP, segment max 100m, sdílené médium, přístupová metoda: CSMA/CD, half-duplex, fyzická topologie: hvězda (star), logická topologie: lineární sběrnice (*bus*),
- 1995: 100BASE-TX – přepínaný FastEthernet - UTP + switch, UTP, segment max 100m, nesdílené médium, přístupová metoda: CSMA/CD vypnuté + full-duplex (nebo half-duplex + CSMA/CD), fyzická topologie: hvězda (*star*), logická topologie: virtuální dvoubodový spoj (point to point).

82 Rozteč montážních šroubků U1 (1.75 palce = 4.45cm).

- 1998: Gigabit Ethernet,
- 2002 - současnost: 10Gigabit Ethernet - pro aplikace požadující velkou přenosovou rychlost a vysokou stabilitu (kvalitu) přenosu - VoIP, IPTV, páteřní sítě i pro WAN, MAN.

Struktura rámce 802.3 (revidovaná)

Preamble – Preambule – 7 oktetů 10101010 – úvodní synchronizace	7B	Synchro-nizace		
Start of Frame Delimiter (SDF) – oddělovač začát-ku rámce - 1 oktet 10101011 - synchronizace	1B			
Destination MAC Address – cílová MAC adresa	6B	Záhlaví	CRC 32	64 až 1518B délka rám-ce
Source MAC Address – zdrojová MAC adresa	6B			
Ether Type / Length of Data Field – typ zapouz-dřeného protokolu nebo délka datového pole. Pokud je hexadecimální hodnota rovná nebo větší než 0x0600 (nebo větší nebo rovno dekadické hodnotě 1536) jde o číslo protokolu.	2B			
Protocol Data – data protokolu – přenášená (*payload*) data + záhlaví protokolu 802.2 + eventuální dorovnání do minimální velikosti	46 - 1500B	Data		
Frame Check(sum) Sequence (FCS) – kontrolní součet CRC 32 pro detekci chyb.	4B	Zápatí		

Standard IEEE 802.3ac z roku 1998 rozšířil velikost rámce na 1522 bajtů z důvodu eventuálního vložení identifikátoru **virtuální sítě LAN** (VLAN ID) do záhlaví rámce (protokol pro VLAN Tag-ging – IEEE 802.1Q).

Pokud vypočtený kontrolní součet v cílovém uzlu neodpovídá kontrolnímu součtu vloženému do zápatí rámce ve zdrojovém uzlu, je rámce shledán poškozeným a je zahozen.

MAC adresa Ethernetu

MAC adresa Ethernetu je 48-ti bitové binární číslo, zobrazované jako 12 hexadecimálních číslic. Obvyklé způsoby zobrazení: 00-60-2F-3A-07-BC nebo 00:60:2F:3A:07:BC nebo 0060.2F3A.07BC.

Dvě pravidla pro přidělování MAC adresy výrobcem podle IEEE:

- Všechny MAC adresy přiřazené síťové kartě nebo jinému ethernetovému zařízení musí v prvních třech bajtech používat identifikátor výrobce - IEEE přiřazenou hodnotu OUI (*Or-ganizationally Unique Identifier*). Např: 00-60-2F je Cisco.[83]
- Všechny MAC adresy se stejným OUI musí mít ve zbývajících třech bajtech přiřazený

83 Pro konkrétní kód OUI nalezneme výrobce v databázi na webové stránce standards.ieee.org.

jednoznačný kód nebo sériové číslo.[84]

O MAC adrese se často hovoří jako o vypálené adrese (*burned-in address (BIA)*) protože je „vypálená“ v paměti ROM (*Read-Only Memory*) v síťové kartě. To znamená, že adresa je permanentně uložená v čipu ROM a nelze ji softwarově měnit.

Přesto, když se počítač spustí, zkopíruje MAC adresu síťové karty do operační paměti RAM. Když se rámec prozkoumává je to tato adresa v RAM, která je použita jako zdrojová adresa pro porovnávání s cílovou adresou v rámci (a tato MAC v operační paměti lze softwarově změnit).

Hexadecimální soustava a adresace

Soustava má 16 číslic: číslice 0 ... 9 a písmena A, B, C, D, E, F.
Oktet se (pokud chci říci, že je vyjádřen heaxadecimálně) zapisuje jako 0xA1 (čti „nula iks“ ...).
Převod z hexadecimální soustavy do dekadické rozvinutím definičního polynomu.
Převod z hexadecimální soustavy do binární nezávislým převedením každé číslice na čtyřbitové binární číslo.
Převod z dekadické soustavy do šestnáctkové postupným dělení základem (16).
Převod z dvojkové soustavy do šestnáctkové rozdělením zprava po čtyřech bitech a každé čtyři bity nezávisle převést na jednu šestnáctkovou číslici.

Příklady:

$(A1)_{16}$ = 0xA1 = $(10*16^1 + 1*16^0)_{10}$ = $(161)_{10}$
$(A1)_{16}$ = $(1010\ 0001)_2$
$(161)_{10}$: 161:16 = 10 a zbytek = **1**
10:16 = **0** zbytek = **10 = A** => 0x**A1** = **$(A1)_{16}$**
$(1010\ 0001)_2$ = 0xA1

Zobrazení MAC

C:\>ipconfig /all
$ /sbin/ifconfig
OUI (= první tři bajty zleva) určuje výrobce karty databáze standards.ieee.org .

Porovnání adres na L2 a L3

Stručně:

- L3 adresa umožňuje posílat (směrovat) paket do jeho cíle (v jiné síti) – mezi sítěmi.
- L2 adresa umožňuje aby byl paket (zapouzdřený do rámce) přenášen na lokálním médiu přes segment (lokální) sítě.

Unicast, broadcast a multicast v Ethernetu

Unicast

Jednosměrové (směrové) vysílání. IP adresa i MAC adresa reprezentují jeden cíl, jedno konkrétní zařízení. Standardní komunikace v síti mezi dvěma uzly.

84 MAC adresa síťové karty nastavená výrobcem je celosvětově unikátní, i když je to potřeba pouze v rámci jedné LAN.

- L2: unikátní MAC adresa cílového uzlu (například: 00-07-E9-42-AC-28, kde 00-07-E9 je OUI (unikátní identifikátor výrobce)pro Intel),
- L3: unikátní adresa cílové stanice (například: 192.168.1.200).

Broadcast

Všesměrové (nesměrové, oběžníkové) vysílání (*broadcast, b/c*)
Broadcastová IP adresa pro danou síť/podsíť:

- samé jedničky v hostitelské části adresy např: 172.16.1.255/24) => **směrovatelný (*directed*) b/c,**
- samé jedničky v celé binární adrese => **lokální, omezený (*limited*) b/c** (255.255.255.255).

Broadcastová MAC adresa obsahuje samé binární jedničky tedy hexadecimálně: FF-FF-FF-FF-FF-FF. Tento broadcast používají například protokoly ARP, DHCP a další.

- L2: v cílové MAC adrese samé jedničky FF-FF-FF-FF-FF-FF
- L3: v cílové IP buď
  - omezený (255.255.255.255)
  - nebo směrovatelný (např. 192.168.1.255) broadcast

Multicast

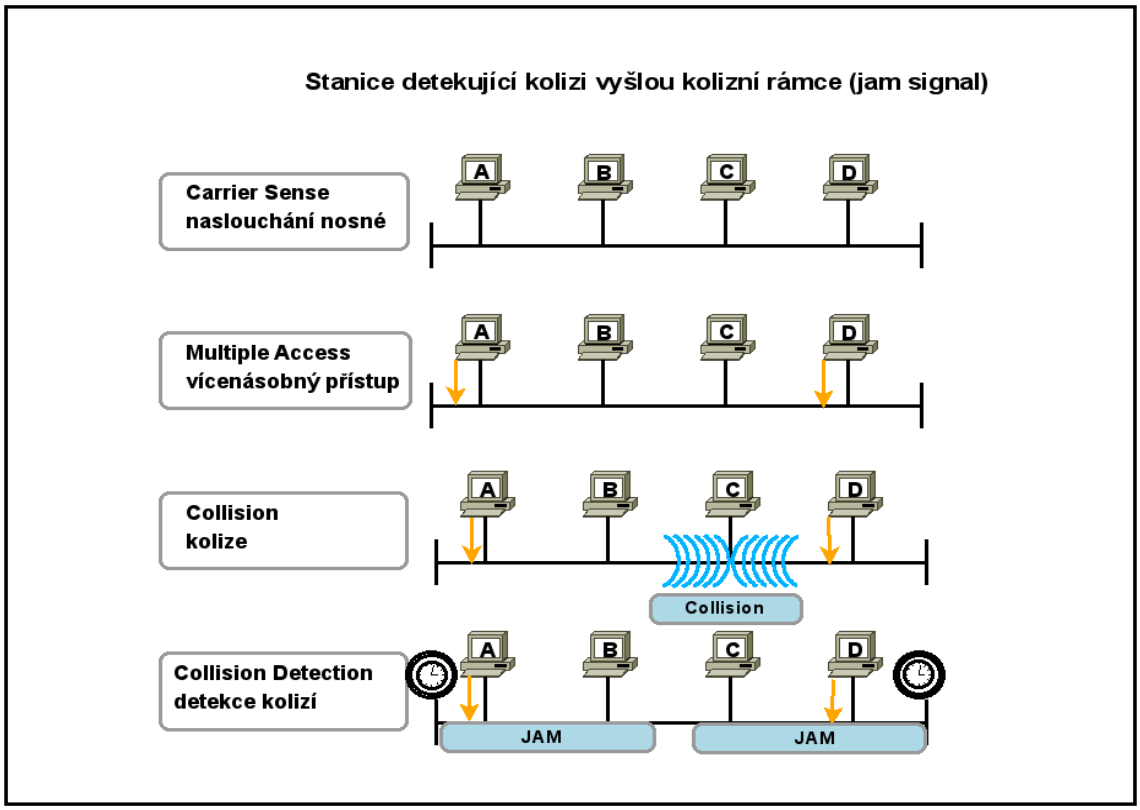
Skupinové (vícesměrové) vysílání. IP adresa v rozsahu **224.0.0.0 až 239.255.255.255**. Přidělované v definovaných skupinách. Např. 224.0.0.2 jsou všechny směrovače v podsíti. (Definice: IANA .)
MAC adresa obsahuje v prvních třech bajtech zleva hodnotu **01-00-5E** a zbytek adres je převod **posledních 23 bitů IP adresy skupiny** do hexadecimálního tvaru.

- L2: v cílové MAC adrese multicast (například: **01-00-5E-00-00-01**),
- L3: v cílové IP adrese multicast (například: **224.0.0.1**).

Přístupová metoda CSMA/CD

Carrier Sense Multiple Access / Collision Detection (CSMA/CD) – metoda naslouchání nosné, vícenásobného přístupu a detekce kolizí používaná pro přístup k médiu Ethernetem.

- **naslouchání nosné** – **před vysíláním** i **během vysílání**, pokud je signál na příjmu před vysíláním, karta počká a zkusí znovu (= **režim naslouchání před vysíláním**), pokud se na příjmu objeví signál během vysílání je to stav **kolize**.
- **vícenásobný přístup** – pro *sdílené médium*, o vysílání se může pokusit více uzlů, které vzájemně soutěží o přístup k médiu, **latence** – doba, kterou je rámec na médiu, konečná **rychlost šíření signálu**.
- **detekce kolizí** – pokud je na kartě detekována kolize (příjem signálu během vysílání) je vyslán **kolizní rámec** (*Jam signal*) = 32 bitů (4 bajty) střídavě nul a jedniček se zvýšenou amplitudou oproti normálu. **Náhodná odmlka** (algoritmus pro výpočet *backoff period* na základě hodnotu uložené v EPROM síťové karty) po výskytu kolize nebo po příjmu jam signálu se po jejím odeznění o vysílání pokusí síťová karta s nejkratší dobou náhodné prodlevy.



Rozbočovače a kolize

Kolizní doména – fyzické segmenty sítě (segmenty média) propojené zařízeními na L1 (*repeater, hub*). Čím je kolizní doména menší, tím lepší.

Důsledky velké kolizní domény:

- sdílení přenosové kapacity média jeho sdílením,
- větší potenciál ke vzniku kolizí,
- zvětšení latence v doméně.

Podmínky vedoucí ke zvětšení počtu kolizí:

- více zařízení připojených do sítě,
- častější přístup na médium,
- zvětšení délky kabelu mezi zařízeními.

Zmenšení kolizní domény:

- rozdělením na dvě pomocí můstku (bridge),
- mikrosegmentace pomocí přepínače (switch) na kolizní domény na kabelu mezi přepínačem a uzlem sítě. Na této formálně kolizní doméně (dvoubodovém spoji) je bezkolizní prostředí.

Časové hodnoty Ethernetu

Latence (*latency*) – čas, který celý rámec stráví v médiu nebo zařízení. Uvědomte si rozdíl od **zpoždění** (*delay*), což je doba, za kterou signál dorazí z jednoho místa do druhého.

Synchronizace (Pole: **Preamble** + **SDF** (*Start Frame Delimiter*)) – přenos dat je nyní (u přenosových rychlostí 100Mbps a vyšších) sice **synchronní komunikace**, ale u 10Mbps Ethernetu byl

přenos asynchronní (a synchronizace byla potřebná) nyní je tedy toto pole synchronizace ponecháno z důvodu zpětné kompatibility.

Doba jednoho bitu (*bit time*) – převrácená hodnota přenosové rychlosti (b/s) - doba, kterou trvá jeden bit při dané přenosové rychlosti:

Rychlost	***Bit Time (ns, 10^{-9}s)***
10 Mbps	100
100 Mbps	10
1 Gpbs	10
10 Gbps	0.1

Prokládací interval (Slot Time) – při přenosu polovičním duplexem – **maximální doba pro detekci kolize** = dvojnásobek doby, po kterou rámec cestuje z nejvzdálenější stanice v síťovém segmentu. Udává se v době jednoho bitu (*bit time*). Její definice slouží k tomu, aby i starší síťové karty měly dostatečný zaručený čas k detekci kolize.
Co ji omezuje:

- minimální velikost ethernetového rámce
- maximální velikost síťového segmentu

Ethernet Slot Time

Rychlost	***Slot Time***
10 Mbps	512 bitů
100 Mbps	512 bitů
1 Gpbs	4096 bitů
10 Gbps	**- (není podporováno sdílené médium)**

Mezera mezi rámci (*Interframe spacing*) – minimální mezera (prodleva) mezi rámci, slouží jako rezerva pro zpracování rámce pomalejší síťovou kartou. Pro 10Mb/s až 10Gb/s je to 96 bit time.

Rychlost	***Interframe spacing***	***Požadovaná doba (10^{-6} sec)***
10 Mbps	96 bit time	9,6 µs
100 Mbps	96 bit time	0,96 µs
1 Gpbs	96 bit time	0,096 µs
10 Gbps	96 bit time	0,0096 µs

Kolizní rámec (*Jam signal*) - 32 bitů (**4B**) střídavě jedniček a nul – 1010 10101 (vzor signálu je stejný jako u pole Preambule v rámci). Je **s větší amplitudou** než normální data. Slouží k informování všech síťových karet na sdíleném médiu, že došlo ke kolizi a data jsou jí poškozena.

Vybrané PHY charakteristiky Ethernetu

PHY = charakteristiky na fyzické vrstvě.

Terminologie technologií vzhledem k přenosové rychlosti:

- **10 Mbps**: Ethernet
- **100 Mbps**: Fast Ethernet
- **1 Gbps**: Gigabit Ethernet
- **10 Gbps**: 10 Gigabit Ethernet

Struktura názvu konkrétní technologie Ethernet (příklad 10Base-T):

10	**Base**	**-T**
Přenosová rychlost v Mb/s. 10Mb/s	Base Band = základní šířka pásma, přenos v jednom kanálu	Přenosové médium T = UTP
	~~Broad Band = více kanálů~~[85]	

Typ Ethernetu	***Bandwidth přenosová rychlost***	***Typ kabelu***	***Duplex***	***Maximální vzdálenost (m)***
10BASE5	10 Mbps	Silný („tlustý“) koax (Thicknet)	Half	500
10BASE2	10 Mbps	Tenký koax (Thinnet)	Half	185
10BASE-T	10 Mbps	Cat3/Cat5 UTP	Half	100
100BASE-TX	100 Mbps	Cat 5 UTP	Half	100
100BASE-TX	200 Mbps	Cat 5 UTP	Full	100
100BASE-FX	100 Mbps	Multimode fiber	Half	400
100BASE-FX	100 Mbps	Single-mode fiber	Half	2000
1000BASE-T	1 Gbps	Cat5e UTP	Full	100
1000BASE-TX	1 Gbps	Cat6 UTP	Full	100
1000BASE-SX	1 Gbps	Multimode fiber	Full	550
1000BASE-LX	1 Gbps	Single-mode fiber	Full	2000
10GBASE-T	10 Gbps	Cat6a/Cat7 UTP	Full	100
10GBASE-LX4	10 Gbps	Multimode fiber	Full	300
10GBASE-LX4	10 Gbps	Single-mode fiber	Full	10000

- Charakteristická impedance (Z_0) koaxiálního kabelu (obou typů) je 50 Ohm (50 Ω) a na jeho konci jsou nutné terminátory pro impedanční přizpůsobení a zabránění odrazu vlnění od

85 Od technologie broadbandu, **v tomto případě** vícekanálového přenosu (= více rámců na jednom médiu v jednu chvíli) se z důvodu obtížného udržení zpětné kompatibility upustilo.

volného konce koax.
- Impedance UTP je 100 Ohm.
- Impedance STP je 150 Ohm.

Zastaralý Ethernet

Použití rozbočovačů - hubů v Ethernetu (nepřepínaný Ethernet) má u sítě za následek:
- postrádá možnost rozšiřitelnosti (škálovatelnost),
- zvětšuje latenci (sdílená šířka pásma mezi porty) – při prodloužení segmentu pomocí hubu,
- více chyb v síti,
- více kolizí (v kolizním prostředí).

Použití switchů místo hubů (proč se ještě někde v současnosti používají huby?):

Současný přepínaný Ethernet

Použití switchů (přepínaný Ethernet) má za následek:
- vyhrazenou šířku pásma pro každý port (nesdílenou šířku pásma),
- bezkolizní prostředí,
- full-duplex.

Výhled do budoucnosti

IEEE v současnosti připravuje standardy pro přenosové rychlosti 40, 100 a 160 Gbps.

Přepínač (switch)

Ethernetový switch **výběrově přepošle** (přepne) rámec na port, ke kterému je připojen cílový uzel. Tím se vytvoří dočasné dvoubodové spojení mezi zdrojovým a cílovým uzlem. Spojení je vytvořeno pouze tak dlouhé, aby se přenesl právě jeden rámec. Během tohoto okamžiku mají oba uzly vyhrazen spoj s plnou šířku pásma (přenosovou rychlostí) a jde o **logický dvoubodový spoj**.
Technicky přesně vzato, není tento spoj vytvořen mezi dvěma uzly současně. Pokud uzel pracuje v režimu full-duplex, může vysílat kdykoliv, když má rámec k vysílání, bez ohledu na dostupnost cílového uzlu. To je důvod, proč switch ukládá rámec do **vyrovnávací paměti (*buffer*)** a přepošle ho, až když je cílový uzel volný (*idle*). Tomuto postupu se říká **střadačový** (*store and forward*).
V tomto střadačovém přepínání (když switch načte celý rámec) se ověřuje FCS. Protože ve full-duplexu je cíl volný a je bezkolizní prostředí, je možné vysílat plnou přenosovou rychlostí daného média bez nadbytečné režie správy kolizí (a také bez sdílení přenosové kapacity média).
Switch přepíná rámce na základě cílové adresy MAC v rámci a obsahu přepínací tabulky (switch table / bridge table, MAC table) umístěné v paměti typu *Content Access Memory (CAM)*. Ta obsahuje **naučené zdrojové adresy MAC** z rámce spárované s číslem portu, na kterém je připojen příslušný uzel. Switch **pracuje transparentně** (nemění obsah rámce)[86]. Protože je přepínání odvozeno ze starší technologie *transparent bridging*, nazývá se někdy přepínací tabulka také bridge tabulka. Ze stejného důvodu také mnoho činností vztahujících se k přepínači má ve svém názvu slovo bridge nebo bridging.
Bridge (můstek) je zařízení, které se používalo k propojení (přemostění) dvou fyzických segmentů sítě LAN. Switch může být k tomu použit také, stejně tak pro připojení síťového koncového za-

86 Porty switche/bridge nemají MAC ani IP adresu. Nicméně na switchi může na volitelné IP adrese běžet Web server pro administraci switche (není to ale adresa žádného konkrétního jednotlivého portu) k ní je přiřazena i její MAC adresa.

řízení do sítě.[87] Jedna oblast, kde bridge převládají jsou bezdrátové sítě. Bezdrátové můstky (*Wireless Bridge*) se používají k propojení dvou segmentů bezdrátové sítě.[88]
Tři důvody výrazného zvýšení propustnosti sítě při použití přepínače:

- Vyhrazená (nesdílená) šířka pásma na každém portu,
- Bezkolizní prostředí (na virtuální dvoubodovém spoji se kolize nemohou vyskytovat),
- Plně-duplexní provoz – zdvojnásobení přenosové kapacity proti poloviničnímu duplexu.

Činnosti přepínače

- **učení se** (*learning*) – neznámá zdrojová MAC je přidána do tabulky MAC adres – přepínací tabulky,
- **sledování stáří záznamu** (*aging*) – každý záznam má svoje stáří, po překročení maximálního stáří (implicitně 5 minut (= 300 sekund, nastavuje se v sekundách)) se záznam smaže,
- **výběrové přeposílání** (*selective forwarding*) – pokud je cílová MAC v přepínací tabulce, přepne se rámec do portu, který určuje záznam v MAC tabulce (CAM),
- **záplava** (*flooding*) – pokud cílová MAC není v přepínací tabulce MAC (CAM), je rámec (**unicast**) přepnut do všech aktivních portů (= na kterých je připojeno síťové zařízení) switche – přepínač v této chvíli pracuje jako rozbočovač,
- **filtrování** (*filtering*) – rámce lze filtrovat (zahodit), například při jejich porušení a nesouhlasu CRC přímo na přepínači (popřípadě též lze filtrovat na základě nastaveného zabezpečení na přepínači),
- **vyrovnávací paměť** (*memory buffers, store and forward*) – v případě, že by v jedné chvíli měly být na jeden port přeposlány dva rámce, přepínač jeden odloží do vyrovnávací paměti (*memory buffer*) a pošle ho až po odvysílání předchozího.

Popis činnosti přepínače (na příkladu):

1. Po zapnutí přepínače je jeho přepínací tabulka prázdná,
2. Z jednoho hostitele číslo 1 (port: Fa1, MAC: 0A) je poslán rámce do druhého hostitele číslo 2 (port: Fa6, MAC: 0C), rámec obsahuje obě dvě MAC adresy: cílovou i zdrojovou,
3. Učení se: Přepínač se naučí (zaznamená do MAC tabulky) zdrojovou adresu z rámce (0A) k portu Fa1 včetně času uložení záznamu,
4. Záplava: Cílová MAC adresa není v přepínací tabulce. Přepínač tedy zaplaví (*flooding*) všechny porty přepínač (s výjimkou portu vysílače, na který rámec přišel) jednosměrovým rámcem (*unicast*). Rámec se objeví na vstupu všech síťových karet připojených k přepínači. Kde nesouhlasí MAC adresa je rámec zahozen, na jednom cílovém uzlu MAC adresa souhlasí a rámec je přijat a zpracován.
5. Cílový hostitel zašle zdrojovému hostiteli odpověď. Cílová adresa souhlasí s MAC adresou hostitele 1.
6. Učení se: Přepínač se naučí zdrojovou adresu z rámce.(0C na portu Fa6).
7. Výběrové (selektivní) přeposílání: Cílová MAC adresa je 0A a je již uložena v MAC tabulce. Přepínač výběrově přepošle rámec pouze na port Fa1. Cílová MAC adresa souhlasí s MAC adresou hostitele 1 a ten rámec přijme.
8. Další stejný rámec už je přímo přepnut (= je vytvořen virtuální dvoubodový spoj pro tento

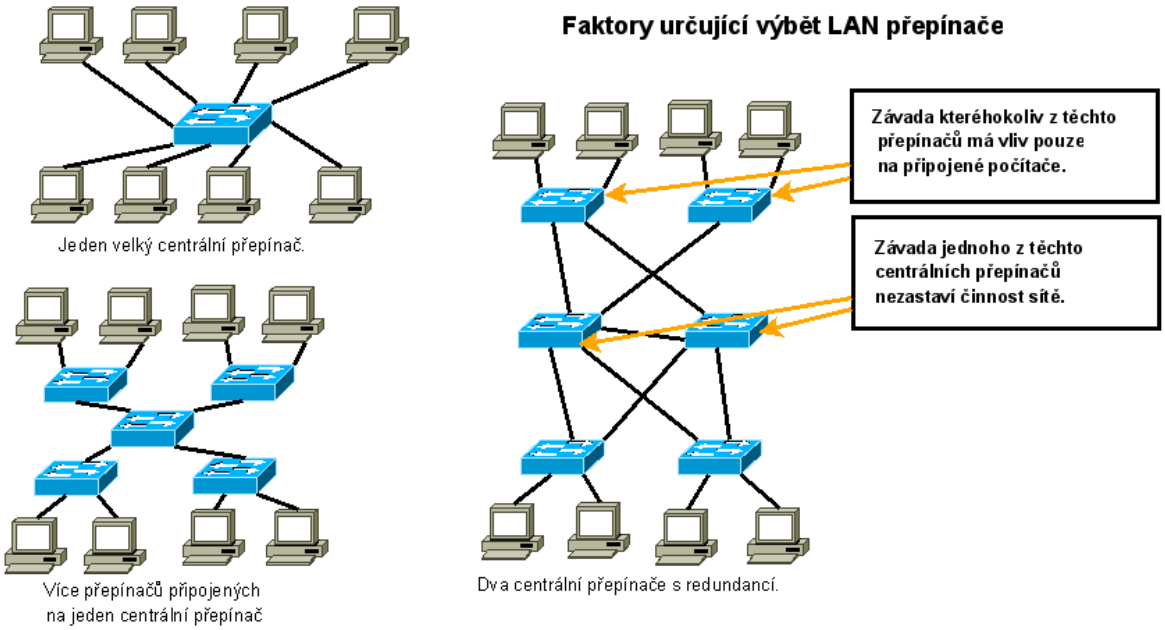
87 Bridge je dvouportové zařízení. Pokud bridge slouží k propojení dvou různých fyzických segmentů (různých médií), nazývá se konvertor. Switch je víceportový bridge. Pokud porty běží na různých přenosových rychlostech – asymetrické přepínání.

88 To je obsahem dalších kurzů (např. CCNA3).

rámec).

9. Další jiná situace, kdy jsou oba hostitelé připojeni k rozbočovači (*hub*), ten je teprve připojen k jednomu portu přepínače a oba hostitelé komunikují mezi sebou. Potom platí, že přepínač zahodí rámec, který by dle obsahu přepínací tabulky měl být přepnut na stejný port, ze kterého tento rámec přišel. Cílový PC totiž již jednou tento rámec obdržel z rozbočovače. Obecně tedy platí, že když jsou příchozí i odchozí porty v přepínací tabulce stejné, přepínač rámec zahodí.

Jedno centrální zařízení tvoří jedno kritické místo selhání (*single point of failure*). Přepínače lze proto z důvodu zajištění spolehlivé funkce sítě, při výpadcích linek i přepínačů, rozdělit na více zařízení, či je vzájemně propojovat redundantními (= nadbytečnými) spoji. Je ovšem potom nutné zablokování nadbytečných spojů, tak aby byl funkční pouze jediný spoj ve stromové struktuře do jednotlivého cílového zařízení. K tomu slouží protokol *Spanning Tree Protocol (STP)*. (STP budeme probírat ve třetím semestru tohoto kurzu.)



Cvičení:

Zapojení switche (Cisco Catalyst 2950). Zjištění obsahu přepínací tabulky.

Konzoli připojíte **rollover (převráceným) kabelem** z konzolového portu switche do **sériového portu PC**. Na PC spustíte program pro emulaci terminálu (např. Hyper Terminal) s parametry: 9600 bps, kód 8 bitů, žádná parita, 1 stop bit, řízení toku žádné.

V příkazové řádce konzole zadejte:

Switch>enable

Výpis obsahu přepínací tabulky v privilegovaném režimu:

Switch#show mac-address-table

Výpis nastaveného maximálního stáří záznamu pro zvolenou virtuální síť:

Switch#show mac-address-table aging-time

(Na Packet Traceru aging-time nelze spustit.)

Protokol ARP

Address Resolving Protocol (ARP) má v protokolové sadě TCP/IP dvě základní funkce:

- zjištění MAC adresy pro zadanou IPv4 adresu (mapování adres L3 na L2),
- správa vyrovnávací paměti namapovaných hodnot (ARP tabulky).

Zjištění MAC adresy k IP adrese uvnitř jedné LAN probíhá odesláním všesměrového (broadcastového) rámce s **ARP Request** (žádostí o zaslání IP adresy) z poptávajícího se zdrojového uzlu, uzel s konkrétní poptávanou IP adresou potom odpoví jednosměrovým (unicastovým) rámcem **ARP response** (s odpovědí) se svojí MAC adresou. Každé zařízení v LAN má pro ARP svoji vlastní vyrovnávací paměť (*ARP cache)*. Záznamy se po určité době mažou (například ve Windows po 2 minutách a zadržovací časovač lze prodloužit až na 10 minut). ARP je pro výkon sítě příkladem, že „je vždy něco za něco“ (*tradeoff*). Bez vyrovnávací paměti, musí ARP pro každý rámec neustále žádat o překlad adres, což přidává latenci a může síť zahltit (*congest*). Naopak, neomezený zadržovací časovač může způsobit chyby související se zařízeními, které již síť opustily nebo změnily svoji IP adresu.

- Cílová IP adresa **uvnitř sítě**: zjišťuje se MAC adresa přímo k této IP adrese uvnitř sítě.
- Cílová IP adresa **v jiné síti**: zjišťuje se MAC adresa **výchozí brány**.

Cvičení:

1. Odposlech ARP request a ARP response v lokální síti pomocí **WireShark**.
2. Prohlídka ARP cache pomocí příkazu v příkazové řádce: **C:\>arp –a**.

Proxy ARP

Pro propojení podsítí přes transparentní směrovač. Směrovač vrací v zastoupení (= *proxy*) odpověď *ARP response* z jedné lokální (pod)sítě do druhé.

ARP Broadcast – problémy jeho použití na sdíleném médiu

Velká režie na přenosovém médiu

Požadavek ARP (*ARP request*) je vysílán všesměrově a je tedy zpracováván na každém zařízení v lokální síti. V typické podnikové síti by tyto všesměrové rámce měly mít minimální vliv na výkonost sítě. Přesto, pokud je velký počet zařízení zapnut najednou a všechna zařízení začnou přistupovat k síťovým službám v téže chvíli, může to pro určitý okamžik znamenat snížení výkonnosti sítě. Potom, co se síťová zařízení naučí potřebné MAC adresy je vliv ARP na síť minimální.

Ohrožení bezpečnosti

V některých případech může použití ARP vést k potenciálním bezpečnostnímu riziku. *ARP spoofing*

(= navádění k nesprávné akci) neboli *ARP poisoning* (= otrávení) je technika použitá útočníkem k vnášení nesprávného přiřazení MAC adres do sítě pomocí vydávání podvodných žádostí ARP. Útočník zfalšuje MAC adresu zařízení a rámce jsou potom zasílány (unášeny, *hijack*) do nesprávného cíle. Jeden způsob, jak tomu zamezit, je nastavení statického přiřazení řádek tabulky ARP. Na některých zařízeních je také možné staticky nastavit MAC adresy, které potom omezí přístup pouze na zařízení uvedená v tomto seznamu. (Viz 3. semestr.)

Kontrolní opakovací otázky a odpovědi (kvíz):

1) Spárujte funkce políček Ethernetového rámce s jejich názvy:
   a) obsahuje zapouzdřená data z vyšší vrstvy = Záhlaví 802.2 a Data (46 – 1500 bajtů),
   b) identifikuje zamýšleného příjemce = Cílová adresa MAC (6 bajtů),
   c) určuje síťovou kartu, která je původcem rámce = Zdrojová adresa MAC (6 bajtů),
   d) hodnota rovná nebo větší než 0x0600 indikuje zapouzdřený protokol = Délka/Typ (2 bajty),
   e) použité pro synchronizaci mezi odesílajícím a přijímajícím zařízením = Preambule (7 bajtů) a Oddělovač začátku rámce – *Start of Frame Delimiter* (1 bajt),
   f) použité pro detekci chyb v rámci = Kontrolní součet rámce – *Frame Check Sequence* (4 bajty).
2) Co je primární funkcí CSMA/CD v síti Ethernet?
   a) Poskytuje metodu, kdy a jak přistupují hostitelé k přenosovému médiu.
3) K vytvoření čeho slouží standard IEEE 802.3ac?
   a) Zapouzdření virtuální sítě VLAN (*Virtual LAN*) do rámce
4) K jakému účelu slouží metoda přístupu k médiu (přístupová metoda)?
   a) Určuje, které pracovní stanice **na sdíleném přenosovém médiu** sítě LAN může vysílat data.
5) Jak jsou v Ethernetu detekovány kolize?
   a) Amplituda signálu v kolizním rámci (*jam signal*, 4 bajty) je vyšší než normálně.
6) Která podvrstva spojové vrstvy poskytuje své služby síťové vrstvě?
   a) LLC
7) Má HUB (rozbočovač) MAC adresu?
   a) Ne
8) PC A připojený k rozbočovači již odvysílal 50% 1KB rámce a této chvíli chce vysílat svůj rámec další jiný uzel PC B. Co musí PC B učinit?
   a) Počkat dokud PC A nedokončí svoje vysílání.
9) Jakou adresu používá přepínač k selektivnímu přeposílání rámců?
   a) Cílovou MAC adresu.

10) Jakou adresu používá přepínač k naplnění obsahu přepínací tabulky?
    a) Zdrojovou MAC adresu.

Kapitola 10 – Plánování sítí a kabeláž sítí

V této kapitole se naučíme:

- Určit základní síťová média pro tvorbu spojení uvnitř LAN
- Určit typy propojení pro propojovací a koncová zařízení v síti LAN
- Určit konfiguraci kontaktů v konektorech pro přímý a pro překřížený kabel UTP
- Identifikovat různé typy kabelů, standardů a fyzických portů použitých pro připojení WAN
- Definovat roli administrativních portů na síťových zařízeních v případě použití výrobků Cisco
- Návrh adresního schéma pro propojené sítě a přiřazení adresních rozsahů pro hostitelské počítače a pro rozhraní směrovače.
- Porovnat a zdůraznit důležitost promyšleného a správného návrhu sítí.

V této kapitole předpokládáme bohaté využití již získaných znalostí a zkušeností.

Volba vhodných zařízení pro LAN

Propojování dvou a více sítí:

- **směrovač** propojuje:
    - LAN – LAN,
    - LAN – WAN.

Propojování koncových zařízení v jedné LAN:

- hub – malá propustnost, malé náklady (to už dnes také neplatí),
- **switch** – všeobecně první volba.

Faktory pro výběr zařízení

Switch:

- cena - počet portů, funkce, kalkulace nákladů na jeden port (*cost per port*),
- rychlost a typy portů (rozhraní) – koupit pouze tolik, kolik jich potřebujeme v této chvíli?, různé rychlosti, použita UTP i optika zároveň?,
- rozšířitelnost,
- možnosti správy (administrace) switche,
- další potřebné funkce a služby.

Redundantní struktura sítě na L2 – není jedno místo fatální chyby => STP (*Spanning Tree Protocol*).

Router:

- Rozšířitelnost (modulární rozhraní, *expanded slots*),

- médium,
- funkce operačního systému (bezpečnost, QoS, VoIP, směrování více L3 protokolů (IPX, ...), další potřebné služby jako jsou NAT (= IP maškaráda), DHCP a další).

Propojování LAN a WAN

Čtyři oblasti v kabeláži LAN:

1. pracovní oblast (použit montážní kabel (*patch cable*) <=10m (5m), volný přímý UTP kabel od zásuvky na zdi do PC koncového uživatele) – přístupová úroveň sítě (*access level*),
2. telekomunikační místnost s distribučním switchem a propojovacím (*patch*) panelem, pevné vedení překříženým nebo přímým UTP kabelem ke switchi v pracovní místnosti – distribuční úroveň sítě (*distribution level*),
3. páteřní kabeláž/síť (*backbone*) = vertikální kabeláž, obvykle vedená optickým kabelem, připojení k ISP – (*core level*) firemní sítě,
4. distribuční kabeláž = horizontální kabeláž (max délka 90m, pevný rozvod z telekomunikační místnosti k přístupovým switchům.)

Poznámka: doporučení Cisco pro strukturu tříúrovňové hierarchické sítě LAN ve firmě. Úrovně:

- ***core*** – páteřní úroveň (*backbone*) a připojení k ISP,
- ***distribution*** – distribuční úroveň, horizontální vedení od distribučních switchů k přístupovým switchům
- ***access*** – přístupová úroveň, propojovací kabely od zásuvek na zdi do PC, přístupové switche a pevné rozvody k nim od zásuvek na zdi.

Typy médií

- UTP (Cat 5, 5e, 6 a 7)
- optické vlákno (jednovidové, vícevidové),
- bezdrát.

Každé médium má své výhody a nevýhody:

- Maximální délka (například UTP segment max 100m),
- cena,
- šířka pásma,
- snadnost instalace,
- náchylnost na EMI / RFI.

Útlum (*attenuation*) – pokles síly signálu vlivem délky média, popřípadě nehomogenit média, špatného zakončení atd.

UTP kabeláž

Konektor: RJ-45.

Normy zapojení RJ-45: T568A, T568B pro přímý (na obou koncích stejná norma) nebo překřížený (na každém konci jiná norma) UTP kabel.

Dva typy rozhraní (interface) na zařízení:

- MDI (*Media Dependend Interface*) – pro přímý UTP,
- MDIX (*Media Dependend Interface, Crossover*) – pro překřížený UTP.

Pokud je rozhraní označeno jako *MDI/MDIX* nebo *MDIX autodetection* – umí rozhraní samo automaticky přehodit páry ve 100Mb/s UTP kabelu.

Použití přímého nebo překříženého kabelu již důvěrně známe: přímý pro propojení logicky různých zařízení zařízení (DTE-DCE) a překřížený pro zapojení logicky stejných zařízení (DTE-DTE nebo DCE-DCE).

Logické typy zařízení:

- ***Data Terminal Equipment (DTE)***: PC, router (rozhraní Ethernet),
- ***Data Communications Equipment (DCE)***: hub, switch, bridge, AP).

Překřížený kabel pro 1Gbps

Uvědomte si, že překřížený UTP montážní kabel pro FastEthernet (= 100Mb/s) je zapojený jinak než překřížený montážní kabel pro Gigabit Ethernet (= 1000Mb/s). U FastEthernetu jsou přehozené pouze piny 1, 2 a 6, 3. V Gigabit Ethernetu jsou navíc ještě přehozeny piny 4, 5 a 7, 8.

Připojení WAN

Protokol:	Cisco HDLC, PPP, Frame Relay	DSL modem	Kabelový modem
Konektor:	V.35 Winchester	RJ-11	F – kabelová TV

Na sériové lince (kabelu) na straně směrovače je konektor Smart Serial a na opačné straně je 35-ti pinový konektor Winchester V.35(M) nebo konektor DB-60(M).

Vlastní zapojení

Realita:

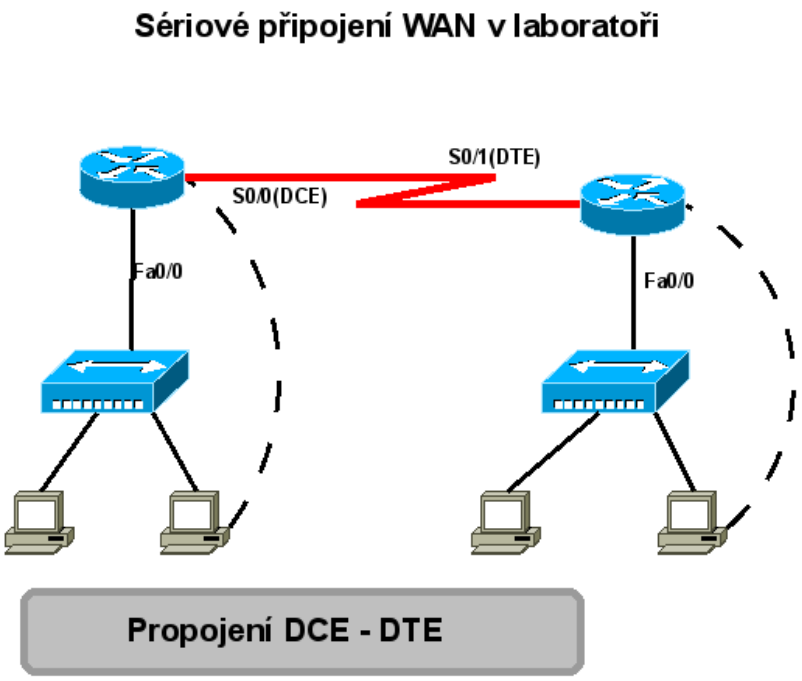
- router zákazníka (jeho sériový port je typu DTE = implicitní hodnota rozhraní)
- **<- sériový kabel[89] DTE, „samec“ (*Male*) V.35(M) a na straně směrovače Smart Serial ->**
- digitální modem (zařízení CSU/DSU (*Channel Service Unit/Data Service Unit*) je typu DCE a zajišťuje synchronizaci (nastavený takt hodin) sériové linky do směrovače)
- **< – DSL linka (*Digital Subscriber Link*) ISP** (pronajatá digitální linka, obvykle využívající existující telefonní vedení nebo kabel kabelové TV) - >

89 Pozor: WAN linka se v celé délce nerealizuje pomocí sériové linky. Sériová linka slouží pouze jako přípoj k digitálnímu modemu a digitální DSL lince. Přes sériovou linku lze přenášet data na vzdálenost 15 – 150 metrů, podle přenosové rychlosti.

- modem (zařízení CSU/DSU je typu DCE a zajišťuje synchronizaci (nastavený takt hodin) sériové linky do směrovače)
- **< - sériový kabel DTE, „samec“ (*Male*) V.35(M) a na straně směrovače Smart Serial - >**
- router zákazníka (jeho sériový port je typu DTE = implicitní hodnota rozhraní).

Laboratoř:

- router (jeho sériový port je **typu DCE a má nastavený takt hodin**, je to vynuceno zapojením sériového kabelu typu DCE s V.35(F))
- **< – sériový kabel DCE, „samice“ (*Female*) V.35(F) a na straně směrovače Smart Serial, tento kabel má překřížený Rx a Tx** - > (s tímto kabelem se setkáte pravděpodobně pouze v laboratořích Cisco Academy, nahrazuje připojení k modemu (CSU/DSU) pronajaté linky od ISP)
- **< – sériový kabel DTE, „samec“ (*Male*) V.35(M) a na straně směrovače Smart Serial, spojený s předchozím DCE kabelem - >**
- router (jeho sériový port je DTE (= implicitní hodnota rozhraní) a nemá nastavený takt hodin).



Emulace terminálu

Z konzolovému portu směrovače nebo přepínače se připojíme převráceným (*rollover)* kabelem do RS 232 (sériového portu) PC, na kterém musí běžet **program emulace terminálu** (pro Windows například **HyperTerminal**, pro Linux například **TerraTerm, GtkTerm** popřípadě pro oba systémy použitelný program **PuTTY**). Tento program MUSÍ mít nastaveny následující parametry přenosu (**pokud nebude nastaveno PŘESNĚ takto, nebude spojení fungovat!!!**):

- 9600 b/s,
- 8 bitový kód,
- 1 stop bit (-> arytmický, asynchronní přenos),
- žádná parita,
- žádné řízení toku dat.

Návrh adresního schéma (IP)

Je třeba vhodně zvolit IP adresy následujících typů zařízení:

- koncová zařízení (uživatelské PC, administrátorská PC, servery a další jako jsou síťové tiskárny , IP telefony, IP kamery atd.)
- propojovací zařízení (směrovače),
- administrativní IP rozhraní (přepínače, AP).

Výpočty podsítí: Případ 1 (*Case 1*)

Výpočty podsítí již důvěrně známe z Kapitoly 6.

Máte vytvořit čtyři (pod)sítě. Počty potřebných IP adres v jednotlivých sítích jsou:
Student LAN:

- Počítačů: 460
- Router (LAN Gateway): 1
- Switch (administrovatelný): 20
- Celkem za podsíť: 481

Instruktor LAN:

- Počítačů: 64
- Router (LAN Gateway): 1
- Switch (administrovatelný): 4
- Celkem za podsíť: 69

Administrátor LAN:

- Počítačů: 20
- Server: 10
- Router (LAN Gateway): 1
- Switch (administrovatelný): 1
- Celkem za podsíť: 32

WAN:

- WAN - Router – Router : 2
- Celkem za WAN: 2

K dispozici je **privátní rozsah (blok) ve třídě B: 172.16.0.0/16 (pro CIDR) nebo 172.16.0.0/21 pro VLSM.**

Kalkulace bez VLSM

Největší počet adres v jedné síti: 481 -> nejbližší vyšší mocnina dvou = 512 tj. 2^9 z toho plyne maska podsítě /23 tj. 255.255.254.0. Velikost bloku dat: $2^1 * 2^8$ = **0.0.2.0**. Použitá nejdelší možná maska vyhovující všem sítím. Všechny adresní bloky jsou tak stejně velké. Začněte od nulté podsítě a pokračujte v adresaci těsně za sebou (sítě 0., 1, 2, ...).

Síť	*Maska*	*Blok*	*Adresa podsítě*	*Rozsah hostitelů*	*Adresa b/c*
Student (0. podsíť)	*/23*	***0.0.2.0***	*172.16.0.0/23*	*172.16.0.1 - 172.16.1.254*	*172.16.1.255*
Instruktor (1. podsíť)	*/23*	***0.0.2.0***	*172.16.2.0/23*	*172.16.2.1 - 172.16.3.254*	*172.16.3.255*
Administrátor (2. podsíť)	*/23*	***0.0.2.0***	*172.16.4.0/23*	*172.16.4.1 - 172.16.5.254*	*172.16.5.255*
WAN (3. podsíť)	*/23*	***0.0.2.0***	*172.16.6.0/23*	*172.16.6.1 - 172.16.7.254*	*172.16.7.255*

Kolik zbude nepoužitých adres v jednotlivých podsítích a v celé síti třídy B?

Kalkulace s VLSM

Pro každou síť použita nejdelší možná maska. Každý adresní blok je tak jinak velký. Adresní bloky klaďte těsně za sebou. (**Před výpočtem si jednotlivé sítě seřaďte podle jejich velikosti sestupně od největší, k nejmenší**, předejdete tak chybě s překryvem (*overlapping*) adresních rozsahů.) (Překryv na vzdálených sítích (na rozdíl od přilehlých sítí) již směrovače nedetekují jako chybu, ale směrování potom nefunguje!)

Síť	*Maska*	*Blok*	*Adresa podsítě*	*Rozsah hostitelů*	*Adresa b/c*
Student (0. podsíť)	*/23*	***0.0.2.0***	*172.16.0.0/23*	*172.16.0.1 - 172.16.1.254*	*172.16.1.255*
Instruktor	*/25*	***0.0.0.128***	*172.16.2.0/25*	*172.16.2.1 - 172.16.2.126*	*172.16.2.127*
Administrátor	*/26*	***0.0.0.64***	*172.16.2.128/26*	*172.16.2.129 - 172.16.2.190*	*172.16.2.191*
WAN	*/30*	***0.0.0.4***	*172.16.2.192/30*	*172.16.2.193 - 172.16.2.194*	*172.16.2.195*
Nepoužité	-		-	*172.16.2.197 -172.16.3.254*	-

Kolik zbude nepoužitých adres v jednotlivých podsítích a v celé síti třídy B?

Cvičení

1. Packet Tracer: zprovoznění sériové linky mezi dvěma směrovači.
2. Zvolte síť v privátním rozsahu a masku podsítě umožňující právě dvě IP adresy.
3. Připojení konzole.
4. Nezapomeňte, že takt hodin se musí nastavit na straně DCE.
5. Ověření funkčnosti spojení (spusťte (**show ip interface brief)**, **ping** a **traceroute** na konzoli směrovače).

Kontrolní opakovací otázky a odpovědi (kvíz):

1) Máte IP síť 200.100.50.0/28. Určete, které z uvedených adres jsou nepoužitelné jako adresy hostitelů v podsítích dané plnotřídní sítě.
   a) Nepoužitelné: 200.100.50.79 (=b/c), 200.100.50.80 (=síťová adresa), 200.100.50.143 (= b/c), 200.100.50.208 (=síťová adresa)
   b) Poznámka: velikost bloku je pro masku (prefix) /28 rovná 0.0.0.16
2) Kdy se použije v síti přímý UTP kabel?
   a) Při propojení logicky různých zařízení DTE-DCE (např.: hostitelské PC-přepínač, směrovač-rozbočovač, atd.)
3) Máte propojená v řadě za sebou následující zařízení: směrovač sériovou linkou s CSU/DSU (= digitální modem) to pomocí digitální pronajaté linky (DSL) s dalším CSU/DSU a to sériovou linkou se směrovačem. Za co je, kromě přenosu dat, zodpovědné zařízení typu DCE?
   a) Takt hodin (*clocking*) na synchronní lince.
4) Směrovač, který zakončuje sériovou WAN linku, je typicky zařízení typu DTE. Za jakých okolností by mohl být nakonfigurován jako zařízení typu DCE?
   a) V laboratorních testovacích podmínkách pro na sebe těsně navazující směrovače propojené sériovou linkou (bez modemu mezi nimi).
5) Uvedené adresy rozdělte na privátní, veřejné a skupinové:
   a) privátní: 10.1.1.1, 172.16.4.4, 192.168.5.5
   b) veřejné: 172.32.10.10, 192.167.11.11
   c) skupinové: 224.0.0.9
6) Přiřaďte k prefixu (lomítkový tvar masky) poslední oktet kanonického tvaru masky podsítě:
   a) /24 = 0,
   b) /25 = 128,
   c) /26 = 192,
   d) /27 = 224,
   e) /28 = 240,
   f) /29 = 248,
   g) /30 = 252.
7) Jakým typem ethernetového UTP kabelu byste spojili přímo dva směrovače?
   a) Překříženým
8) Jaké parametry byste nastavili na emulátoru terminálu při konzolovém spojení mezi PC a směrovačem?
   a) 9600b/s, 8 bitové slovo, bez parity, stop bit 1 a žádné řízení toku dat.
9) Jaké maximální délky UTP kabelu jsou stanoveny dle standardů ANSI/TIA/EIA 568B?

(uveďte 3)

a) maximální délka mezi koncovými systémy = 100m,
b) maximální délka horizontální kabeláže = 90m,
c) maximální délka montážního propojovacího kabelu = 5m.

10) Jaký hlavní faktor byste měli určit a vzít v potaz před použitím bezdrátové technologie?
    a) Identifikovat popřípadě omezit zdroje RFI (interference na rozhlasových frekvencích).

Kapitola 11 – Konfigurace síťových zařízení

V této kapitole se naučíme:

- Definovat roli operačního systému IOS (*Internetwork Operating System*).
- Definovat účel konfiguračního souboru.
- Identifikovat několik tříd zařízení, které používají operační systém IOS.
- Určit faktory, které přispívají k tomu, jaká množina příkazů IOS je dostupná na zařízení.
- Určit režimy činnosti IOS.
- Určit základní příkazy IOS.
- Porovnat a určit rozdíly základních příkazů show.

Zařízení Cisco jako jsou switche a routery používají operační systém **Cisco Internetwork Operating System (IOS)**. Jeho hlavní funkce jsou:

- základní funkce směrování a přepínání,
- konfigurace zařízení, spolehlivý, kvalitní (*QoS*) a bezpečný přístup k síťovým zařízením,
- rozšířitelnost sítě (*scalability*) (= možnost aktualizace funkcí),
- správa zařízení.

IOS je uložen v paměti **flash** (její obsah je zachován i při vypnutí zařízení), může tam být více obrazů (*images*) – souborů s různými verzemi operačního systému. Při startu směrovače se IOS zkopíruje do paměti **RAM**. Tato funkce zvyšuje výkon zařízení.

Přístupové metody k CLI

Je několik způsobů jak přistupovat k **rozhraní příkazové řádky (CLI)**. Nejpoužívanější metody jsou:

- **konzole** (*Console*) - (konektor RJ-45, není to ale síťové připojení!!! - **přípojení přes terminál**) často se používá k přístupu k zařízení, když síťové služby nebyly nastartovány nebo selhaly. Příklady použití konzole:
  - počáteční konfigurace,
  - obnova zařízení po poruše nebo řešení problémů, pokud není možný vzdálený přístup,
  - obnova ztraceného hesla (*Password recovery procedures*) – postup lze provést výhradně s fyzickou přítomností administrátora u zařízení,
  - z tohoto důvodu (možného obejití hesla), by zařízení mělo být v uzamčené místnosti.
- **Telnet nebo SSH** - vzdálený přístup (přihlášení) přes sériové nebo ethernetové **síťové připojení**, virtuální terminál - *Virtual TeletYpe*[90] *interface (vty)*, protože Telnet je nezabezpečený protokol, je nanejvýš vhodné (= příklady nejlepší praxe, *best practice*) používat pro vzdálené přihlášení výhradně **Secure Shell (SSH)**,
- **pomocný port** (AUX port) - konektor RJ-45 **připojení k modemu pro vytáčené telefonní spojení**.

90 Teletype = dálnopis (anglicky).

Konfigurační soubory

Konfigurační soubory jsou uloženy **v různých typech pamětí směrovače**:

Typ paměti	*Konfigurační soubor / Konfigurace*	*Změny se projeví*
NVRAM **(non-volatile RAM)**	startup-config (startovací konfigurace)	Po restartu nebo reload (znovu zavedení OS)
RAM	running-config (aktuální konfigurace)	Okamžitě – běžící konfigurace

Režimy IOS

Režimy práce (mode) IOSu mají **hierarchickou úroveň**:

- **Uživatelský režim** - *User EXEC (executive) mode* – pouze prohlížení bez možnosti změn nastavení – příkazy: ping, show (pouze omezeně), enable, ...,
- **Privilegovaný režim** - *Privileged EXEC mode (enable mode)* – základní administrativní režim s možností přechodu do globálního konfiguračního režimu – všechny příkazy uživatelského režimu EXEC a debug, configure, reload, … ,
    - **Globální konfigurační režim** – *Global Configuration mode* – příkazy: hostname, enable secret, ip route, … – s možností přechodu do dalších specifických konfiguračních režimů jednotlivých oblastí:
        - **konfigurace rozhraní** – *interface*,
        - **konfigurace linky** – *line*,
        - **konfigurace konzole** – *console*
        - **konfigurace směrovacího protokolu** - *router*,
        - …

Příkazové systémové výzvy (prompt) v příkazové řádce (CLI)

Primární režimy IOS

Příkazová systémová výzva (prompt) odkazuje na **aktuální režim práce**, ve kterém se právě nacházíte.

Režim (Mode)	*Popis (Description)*	*Výzvy (Prompts)*
Uživatelský EXEC	Omezený průzkum směrovače. Vzdálený přístup.	Router>
Privilegovaný EXEC	Detailní průzkum směrovače. Trasování a testování. Manipulace se soubory. Vzdálený přístup.	Router#
Globální konfigurační (GCM)	Příkazy globální konfigurace	Router(config)#
Další konfigurační režimy	Konfigurace specifických služeb nebo rozhraní v příslušném konkrétním režimu (mode).	Router(config-*mode*)#

Znaky systémové výzvy (promptu): > - pravá lomená závorka (*right angle brackets*), # - dvojitý kříž, hašovací znak (*hash sign*).

V níže uvedeném **příkladu** vidíte i *přechody mezi jednotlivými módy*.

Uživatelský EXEC (user executive mode)	**Router>***enable*	**Switch>***enable*
Privilegovaný EXEC (privileged executive mode) (prompt # jako v UNIX)	**Router#***configure terminal*	**Switch#***configure terminal*
Globální konfigurační	**Router(config)#***interface* serial 0	**Switch(config)#**
Konfigurace rozhraní	**Router(config-if)#**ip address 192.168.1.1 255.255.255.0	
Konfigurace rozhraní	**Router(config-if)#***exit*	
Globální konfigurační	**Router(config)#***router* rip	
Konfigurace směrovacího protokolu	**Router(config-router)#***exit*	
Globální konfigurační	**Router(config)#***^Z*	
Privilegovaný EXEC	**Router#***disable*	
Uživatelský EXEC	**Router>**	

Struktura příkazu

Prompt	Command	Space	Argument/Keyword	ENTER
Výzva	Příkaz	Mezera	Argument/Klíčové slovo	ENTER
Router>	ping		192.168.1.1	
Router>	show		ip protocols	
Router#	show		running-config	

Příkazy (jednotlivá klíčová slova) není třeba vypisovat celé, ale pouze jednoznačně identifikující počet prvních písmen. Stisk klávesy ENTER vloží příkaz.

Konvence zápisu příkazů IOS

V tištěných materiálech Cisco se používá následující konvence zápisu příkazů:

Konvence	*Popis*
Tučně	Tučný text označuje příkazy a klíčová slova, které jsou vkládána přesně tak jak jsou zobrazena.
Kurzíva	Kurzíva označuje argumenty, kde uživatel dodává hodnotu.
[X]	Hranaté závorky ohraničují volitelný prvek (klíčové slovo nebo argument).
|	Svislá čára označuje výběr mezi volitelnými nebo požadovanými klíčovými slovy nebo argumenty.
[X|Y]	Hranaté závorky ohraničují klíčová slova nebo argumenty oddělené svislou čárou jako volitelný výběr.
{X|Y}	Složené závorky ohraničují klíčová slova nebo argumenty oddělené svislou čárou jako požadovaný výběr.

Nápověda

IOS má několik forem dostupné nápovědy:

- kontextová nápověda (*Context-sensitive help*),
- ověření syntaxe příkazu (*Command Syntax Check*),
- Klávesové zkratky (*Hot Keys and Shortcuts*).

Kontextová nápověda

Pro vyvolání kontextové nápovědy (*Case Sensitive Help*) použijte znak otazník „**?**“. Nápověda reaguje na konkrétní situaci.

#**?** - vrátí **všechny příkazy** použitelné v privilegovaném režimu **enable**

#sh? - vrátí všechny příkazy začínající na sh

#sh ? - vrátí všechny parametry příkazu show

Použití tabelátoru

TABELÁTOR – doplní příkaz/klíčové slovo, pokud je již zadané jednoznačně (obdoba jako v UNIX/Linux).

Tři typy chybových hlášení

- Vysvětlení příkazu,
- nejednoznačný příkaz (*Ambiguous*) (= málo zadaných písmen) – **% Ambiguos command** 'c'
- nekompletní příkaz (*Incomplete*) (= chybí parametr) - **% Incomplete command**
- nesprávný příkaz (*Incorrect*) (= chyba v příkazu s identifikací pozice chyby) – **Invalid input detected at '^' marker**

Klávesové zkratky

Skupiny klávesových zkratek (*Hot Keys and Shortcuts*):

Editace řádky v CLI

Klávesová zkratka	*Popis*
Tab	Doplní částečně vložené jméno příkazu / klíčové slovo.
Backspace	Smaže znak vlevo od kurzoru.
Ctrl-D	(Dvojhmat) Smaže znak na kurzoru.
Ctrl-K	Smaže všechny znaky od kurzoru do konce příkazové řádky.
Esc D	Smaže všechny znaky od kurzoru do konce slova.
Ctrl-U nebo Ctrl-X	Smaže všechny znaky od kurzoru do začátku příkazové řádky.
Ctrl-W	Smaže slovo vlevo od kurzoru.
Ctrl-A	Přesune kurzor na začátek příkazové řádky.
Šipka doleva nebo Ctrl-B	Přesune kurzor o jeden znak doleva.
Esc F	Přesunu kurzor o jedno slovo doprava.
Šipka doprava nebo Ctrl-F	Přesune kurzor o jeden znak doprava.
Ctrl-E	Přesune kurzor na konec (end) příkazové řádky.
Šipka nahoru nebo Ctrl-P	Znovu vyvolá příkaz ze zásobníkové paměti historie příkazů. Začíná s posledním příkazem.
Ctrl-R, Ctrl-I nebo Ctrl-L	Znovu zobrazí výzvu systému (prompt) a příkazovou řádku, po tom, co je přijatá a vypsaná zpráva konzole.

Poznámka: Tlačítko Delete (mazání znaku vpravo od kurzoru) se v terminálových programech nepoužívá (není detekováno).

Po výzvě ---More---

Klávesová zkratka	*Popis*
Klávesa Enter	Zobrazí další řádku.
Mezerník	Zobrazí další obrazovku.
Jiná alfanumerická klávesa	Vrátí do režimu EXEC.

Klávesy pro přerušení

Klávesová zkratka	*Popis*
Ctrl-C	Když je v jakémkoliv konfiguračním režimu, ukončí konfigurační režim a vrátí do privilegovaného EXEC. Když je v režimu interaktivního dialogu (setup), ukončí ho a vrátí se do příkazové řádky.
Ctrl-Z	Když je v jakémkoliv konfiguračním režimu, ukončí konfigurační

	režim a vrátí do privilegovaného EXEC.
Ctrl-Shift-6	Přerušovací sekvence (*escape sequence*) pro všechny účely. Používá se k přerušení vyhledávání v DNS (DNS lookup), traceroute, ping. (Pro uspání (*suspend*) relace Telnetu: Ctrl-Shift-6 x (Trojhmat a potom stisk klávesy x). Stisk samotného ENTER bez příkazu se zase k relaci vrací.)

Poznámka:
Ctrl-D – jsou dvojhmaty (Stiskne se CTRL a drží až do stisku klávesy příslušného písmena).
*Pro **Escape sekvence** se tlačítko Esc stiskne a pustí, potom se stiskne klávesa příslušného písmena.*

Příkazy pro prohlídku systému

Obsah jednotlivých typů pamětí a nastavení rozhraní směrovače:

Za pomlčkou je uveden parametr příkazu show, který příslušnou informaci zobrazí.

Všechny dostupné paměti (RAM, NVRAM, Flash a ROM) a jejich velikosti – **show** version

- RAM (*Random Access Memory* - po vypnutí směrovače se obsah smaže):
  - IOS zavedený v paměti – show version,
  - zavedené programy – show processes CPU, show protocols
  - aktivní běžící konfigurační soubor – show running-config,
  - tabulky a vyrovnávací paměti (buffers) – show memory, show stack, show buffers, show arp, show mac-address-table, show ip route
- NVRAM (*Non-volatile RAM* - po vypnutí směrovače obsah zůstane zachován):
  - záložní startovací konfigurační soubor – show startup-config.
- Flash (po vypnutí směrovače obsah zůstane zachován):
  - obrazy IOS – show flash
- ROM (*Read Only Memory* - po vypnutí směrovače obsah zůstane zachován):
  - omezená verze IOS.
- Rozhraní:
  - rozhraní – show interface, show ip interfaces brief

IOS Examination Commands – příkazy pro průzkum systému - různé parametry příkazu **show:**
- show arp
- show mac-address-table
- show startup-config
- show running-config
- show ip interfaces (show ip interface brief)
- show interfaces
- show version

Příklady výstupů některých příkazů viz dále.

Pokyny pro názvy, hesla a denní uvítací zprávy

Názvy zařízení (*hostname*):
- začínají písmenem,
- neobsahují mezeru,
- končí písmenem nebo číslicí,
- obsahují pouze znaky písmen, číslic a podtržítek (*dashes*),
- mají 63 znaků nebo méně.

Používejte **silná hesla**:
- více než 8 znaků dlouhá,
- kombinace malých a velkých písmen a/nebo sekvencí čísel,
- nepoužívejte stejná hesla na všech zařízeních,
- nepoužívejte běžná slova (jako heslo, administrator), protože se snadno uhádnou (nebo prolomí).

Příklady informací v denních uvítacích hlášeních MOTD (*banner motd = message of the day*):
„Použití zařízení pouze autorizovanými osobami.“
„Aktivity mohou být monitorovány.“
„Neautorizované použití může být právně stíháno.“
„Odstávka systému dnes 14.5.2010 od 14:00 do 16:00“

Přehled základních příkazů v jednotlivých režimech IOS

Uživatelský režim EXEC - User EXEC Mode

Enable	Vstup do privilegovaného režimu EXEC.

Privilegovaný režim EXEC - Privileged EXEC Mode

copy running-config startup-config	Kopíruje aktivní konfiguraci do NVRAM.
copy startup-config running-config	Kopíruje konfiguraci z NVRAM do RAM.
erase startup-configuration	Smaže konfiguraci umístěnou v NVRAM.
ping *ip_address*	Pinkne (utilita Ping) na danou adresu.
traceroute *ip_address*	Trasuje každý přeskok (*hop*), směrovač do této adresy.
show interfaces	Zobrazí statistiky pro všechna rozhraní na zařízení.
show clock	Zobrazí čas nastavený na směrovači.
show version	Zobrazí verzi aktuálně zavedeného IOS, HW a informace

	o zařízení.
show arp	Zobrazí tabulku ARP pro dané zařízení.
show startup-config	Zobrazí uloženou konfiguraci umístěnou v NVRAM.
show running-config	Zobrazí obsah aktuálně běžícího konfiguračního souboru.
show ip interface	Zobrazí statistiky pro jednotlivá rozhraní na směrovači.
configure terminal	Vstup do globálního konfiguračního režimu (terminal configuration mode).

Globální konfigurační režim - Terminal Configuration Mode

hostname *hostname*	Přiřazení jména hostitele na zařízení.
enable password *password*	**Tento příkaz nepoužívejte** – nastaví **nešifrované** heslo privilegovaného režimu enable. (Nahrazeno *enable secret*)
enable secret *password*	Nastaví **silně zašifrované** heslo privilegovaného režimu enable. (Pokud je zadáno ještě heslo **enable password**, má přednost **enable secret** a hesla nesmějí být stejná.)
service password-encryption	**Zašifruje zobrazení všech hesel ve výpisech** konfigurace (s výjimkou „enable secret“) slabou šifrou.
banner motd # *message* **#**	Nastaví přihlašovací zprávu dne (message-of-the-day banner).
line console 0	Vstup do konfiguračního režimu linky konzole.
line vty 0 4	Vstup do konfiguračního režimu linky virtuálního terminálu (vty, Telnet) pro 5 virtuálních linek (0-4). Maximální hodnotu posledního parametru zjistíte příkazem (config)#line vty 0 **?.**
interface *Interface_name*	Vstup do konfiguračního režimu síťového rozhraní (interface configuration mode).

Konfigurační režim linky - Line Configuration Mode

login	Umožní ověření hesla při přihlášení.
password *password*	Nastavení hesla pro linku.

Konfigurační režim síťového rozhraní - Interface Configuration Mode

ip address *ip_address netmask*	Nastaví IP adresu a masku podsítě na rozhraní.
description *description*	Nastaví popisku na rozhraní.
clock rate *value*	Nastaví takt hodin (clock rate) pro DCE sériové síťové rozhraní.
no shutdown	Zapne rozhraní (Set interface to up).
shutdown	Administrativně vypne síťové rozhraní.

Poznámka k nastavení přepínače (switch)

Switch se konfiguruje ve stejných režimech stejnými příkazy jako směrovač:

```
configure terminal
        hostname SW_1
        banner motd # … #
        enable secret cisco
        line console 0
                password class
                login
                exit
        line vty 0 15                   //nastavení 16 linek Telnetu (jejich počet viz line vty 0 ?)
                password class
                login
                exit
        interface fa0/1
                description Popis       //Nenastavuje se IP adresa portu switche, je zapnutý
                ^Z
copy run start                          //Uloží aktuální běžící konfiguraci jako startovací
```

1. Porty switche nemají IP adresu a jsou implicitně zapnuté.
2. Switch lze vzdáleně spravovat (administrovat) pomocí Telnet, SSH nebo webového rozhraní přes virtuální administrační port (rozhraní) ve **virtuální lokální síti VLAN** číslo 1. (VLAN 1 (Vlan1) se implicitně používá pro administrativní účely.) Tento virtuální port musí) být nastaven obdobně jako hostitel. To znamená má IP adresu, masku podsítě a switch má implicitní bránu. Virtuální rozhraní se musí zapnout.

Postup nastavení virtuálního administrativního rozhraní:

```
configure terminal
        interface vlan 1
                ip address 192.168.1.2 255.255.255.0
                no shutdown
                exit
```

ip default-gateway 192.168.1.1
exit

Stavy rozhraní/protokolu a typy možné chyby

Protože testování sítě provádíme od L1 do L7, je nejdříve nutné kontrolovat L1 (kabely a stav rozhraní na L1) a teprve po tom přejín na L2. Stavy rozhraní na L1 a L2 zjistíte pomocí příkazů:

- show ip interfaces brief
- show interface

Interface L1	***Protokol linky L2***	***Typ chyby***
UP	UP	L1 a L2 OSI modelu pracují v pořádku a případné chyby jsou výsledkem činnosti vyšších (L3 – L7) vrstev.
UP	DOWN	Chyba na L2 OSI modelu. - Chyba protokolu na L2 nebo chyba zapouzdření (např. 802.3, HDLC, PPP, autentizace CHAP, atd.). Nejsou zapnuté hodiny na straně DCE. Nepřijata zpráva typu *keepalive* (protilehlý směrovač nemá zapnuté síťové rozhraní).
DOWN	DOWN	Závada na L1 OSI modelu. - Kabely, fyzické rozhraní, další routery musí být prověřeny na přítomnost napájení a správnou instalaci a konfiguraci.
DOWN	UP	Duplikace MAC adresy v lokální síti připojené k rozhraní Ethernet, nebo chyba servisního modulu na interní rozšiřující kartě. **Na routerech lze administrativně měnit MAC adresu rozhraní, na rozdíl od běžné (starší) síťové karty.**
ADMINISTRATIVELY DOWN	DOWN	Síťové rozhraní je administrativně vypnuté (není zapnuté administrátorem).

Další informace vypsané pomocí **show interfaces** o rozhraní

- IP adresa ,
- MAC adresa ,
- maska podsítě ,
- statistické údaje o síti (výskyt různých druhů chyb),
- poslední vynulování čítače.

Cvičení

Příklad jednoduchého nastavení směrovače (v CLI)

Pro dva směrovače (Cisco 1841) Router1 a Router2 spojené přes Fa0/0 překříženým UTP kabelem.

K jednotlivým směrovačům je přes port Fa0/1 a switch (Fa0/24, Fa0/1) připojena klientská stanice. Pro jednotlivé tři sítě zleva doprava zvolte následující adresní bloky (adresy a masky): 172.16.1.0/24, 172.16.2.0/24 a 172.16.3.0/24. Brány (porty na směrovačích) budou adresované od adresy všesměrového vysílání příslušné sítě směrem dolů a adresy klientů (PC) od adresy sítě nahoru. Virtuální administrativní rozhraní přepínače budou mít adresy pod adresou implicitní brány na příslušném směrovači.

Podbarvené příkazy jsou pouze pro ověřování nastavení a funkce rozhraní. Vždy zkontrolujte názvy rozhraní (jsou závislé na typu směrovače a umístění zásuvného modulu ve slotu) a po nastavení stavy rozhraní příkazem „show interfaces brief“. **Tučně a podbarvené** jsou rozdílné hodnoty v nastavení směrovačů.

Uživatelská výzva (prompt) a příkaz	***Význam***
Router>	Po startu směrovače a stisku ENTER
Router>enable	Vstup do privilegovaného režimu
Router#show version Router#show ip interface brief	Zobrazení verze o OS, informace o HW a konfiguračním registru. Zobrazení stručných informací o všech IP rozhraních.
Router#configure terminal	Přechod do globálního konfiguračního režimu.
Router(config)#no ip domain-lookup	Zakáže prohledávání jmenného serveru pro špatně zadané názvy příkazů. (Je vhodné, protože šetří čas.) Na konci práce opět zapněte!!!
Router(config)#service password-encryption	Nastavení, že jsou všechna nešifrovaná hesla zobrazována ve výpisu konfigurace zašifrována slabou šifrou.
Router(config)#enable secret cisco	Nastavení **šifrovaného** hesla pro privilegovaný režim.
Router(config)#hostname **Router1**	Změna názvu zařízení.
Router1(config)#banner motd #Prihlaseni pouze pro autorizovane uzivatele.#	Nastavení denního uvítacího hlášení zobrazovaného před přihlášením do systému. Obvykle varování a informace týkající se odstavení systému.
Router1(config)#line console 0 Router1(config-line)#password class Router1(config-line)#login Router1(config-line)#exit	Nastavení konzole: heslo a vynucení jeho ověření při přihlášení. (Pouze jedna linka (0).)
Router1(config)#line vty 0 4 Router1(config-line)#password class Router1(config-line)#login Router1(config-line)#exit	Nastavení linek virtuálního terminálu (vty) Telnetu (maximálně možno 5 linek (0-4)), možnost vzdáleného přihlášení po síti: povinné heslo a vynucení jeho ověření při přihlášení. (Na nezaheslovaný Telnet není možno se vzdáleně přihlásit!)

Uživatelská výzva (prompt) a příkaz	*Význam*
Router1(config)#interface fa 0/1 Router1(config-if)#description ***Linka na prepinac*** Router1(config-if)#ip address ***172.16.1.254 255.255.255.0*** Router1(config-if)#no shutdown	Nastavení síťového rozhraní směrovače: IP adresa a maska, popis a zapnutí rozhraní (implicitně je vypnuté).
Router1(config)#interface fa 0/0 Router1(config-if)#description ***Linka na smerovac 2*** Router1(config-if)#ip address ***172.16.2.253 255.255.255.0*** Router1(config-if)#no shutdown Router1(config-if)#Ctrl-Z	Nastavení síťového rozhraní směrovače: IP adresa a maska, popis a zapnutí rozhraní (implicitně je vypnuté). Návrat do režimu enable. Poznámka: pokud by byla DCE strana sériového rozhraní, musí být ještě nastaven takt hodin (clock rate).
Router1#show running-config Router1#show ip interface fa 0/0 Router1#show ip interfaces brief0 Router1#ping *adresa*	Ověření obsahu běžící konfigurace. Ověření stavu rozhraní na L1 a protokolu L2. Ověření stavů všech rozhraní na L1 a L2. Ověření konektivity pro IP adresu.
Router1#configure terminal Router1(config)#ip domain-lookup Router1(config)#exit	Znovu zapnutí prohledávání jmenného serveru.
Router1#copy running-config startup-config	**Uložení běžící konfigurace z RAM do startovací konfigurace v NVRAM.**
Router1#show startup-config	Ověření obsahu startovací konfigurace
Router1#reload	Znovu zavedení OS
Router1>	po restartu … … je aplikována nová uložená (startup) konfigurace

Následující výpisy jsou vyjmuté ze simulace v Packet Traceru.

Výpis verze IOS

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-IPBASE-M), Version 12.3(14)T7, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Mon 15-May-06 14:54 by pt_team

ROM: System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)

System returned to ROM by power-on
```

```
System image file is "flash:c1841-ipbase-mz.123-14.T7.bin"


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.
Processor board ID FTX0947Z18E
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
191K bytes of NVRAM.
31360K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102

Router#
```

Zobrazované důležité informace:

- Software Version – verze IOS (uloženého v paměti flash)
- Bootstrap Version – veze zavaděče OS (loader) (uloženého v Boot ROM)
- System up-time – čas posledního restartu
- System restart info – metoda restartu (například odpojení napájení, havárie, ...)
- Software image name – jméno souboru s obrazem IOS uloženého v paměti flash
- Router Type and Processor type – číslo modelu a typ procesoru
- Memory type and allocation (Shared/Main) – hlavní RAM procesoru a sdílená paměť pro vyrovnávací paměť paketů
- Software Features – podporované protokoly a funkce
- Hardware Interfaces – dostupná rozhraní na směrovači
- Configuration Register – nastavené specifikace pro zavedení operačního systému, nastavení rychlosti konzole a související parametry

Kontrola jmen a stavů rozhraní

Před nastavováním se na výstup tohoto příkazu vždy podívejte!!! Názvy jsou závislé na typu směrovače a umístění výměnných modulů rozhraní v jednotlivých slotech.

```
Router#show ip interface brief
```

```
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        unassigned      YES manual administratively down down

FastEthernet0/1        unassigned      YES manual administratively down down

Vlan1                  unassigned      YES manual administratively down down
Router#
```

Kontrola běžící konfigurace

Po nastavení:

```
Router1#show running-config
Building configuration...

Current configuration : 601 bytes
!
version 12.3
service password-encryption
!
hostname Router1
!
!
enable secret 5 $1$.7Kl$rkt5N1W5/ZSt/M/cudiJk.
!
!
!
interface FastEthernet0/0
 description Linka na smerovac 2
 ip address 172.16.2.253 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description Linka na prepinac - sit LAN 1
 ip address 172.16.1.254 255.255.255.0
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
!
!
!
!
banner motd ^CRouter1 - Prihlaseni pouze pro autorizovane uzivatele!!!^C
line con 0
 password 7 045807071C32
 login
line vty 0 4
 password 7 1511070D1739
 login
!
```

```
!
end


Router1#
```

Kontrola stavu rozhraní (R1) před nastavením 2. směrovače

```
Router1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        172.16.2.253    YES manual up                    down

FastEthernet0/1        172.16.1.254    YES manual up                    up

Vlan1                  unassigned      YES manual administratively down down
Router1#
```

Kontrola stavu rozhraní (R2) po nastavení 2. směrovače

```
Router2#sh ip int br
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        172.16.2.254    YES manual up                    up

FastEthernet0/1        172.16.3.254    YES manual up                    up

Vlan1                  unassigned      YES manual administratively down down
Router2#
```

Stav a statistika rozhraní

Zobrazuje stav, statistiku a výskyt případných chyb.

```
Router1#show interface fa0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Lance, address is 0001.c959.b102 (bia 0001.c959.b102)
  Description: Linka na prepinac - sit LAN 1
  Internet address is 172.16.1.254/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 4 bits/sec, 0 packets/sec
  5 minute output rate 3 bits/sec, 0 packets/sec
     7 packets input, 280 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     6 packets output, 240 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

```
Router1#
```

Kontrola konektivity

```
Router2#ping 172.16.2.253

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.253, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 21/42/50 ms

Router2#
```

(všimněte si překročení maximální povolené doby odezvy (timeout) na prvním paketu, **prováděl se překlad IP adresy na MAC adresu pomocí ARP a směrovač nestačil odpovědět**)

```
Router2#traceroute 172.16.2.253
Type escape sequence to abort.
Tracing the route to 172.16.2.253

  1   172.16.2.253    28 msec   45 msec   43 msec
Router2#
```

Kontrola obsahu směrovací tabulky

#show ip route

V případě (jako zde), kdy není nastaveno směrování, vidíte na každém směrovači pouze přímo připojené sítě.
Nepřímo připojené sítě je nutné do směrovací tabulky přidat ručně (statické směrování) nebo pomocí směrovacího protokolu (dynamické směrování).

Směrovací tabulka

Obsahuje pouze přímo připojené sítě (před nastavením směrování):

```
Router1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.1.0 is directly connected, FastEthernet0/1
C       172.16.2.0 is directly connected, FastEthernet0/0
Router1#
```

Nastavení statického směrování

Router1(config)#ip route *172.16.3.0 255.255.255.0 172.16.2.254*

Nastavení
Router1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#ip route 172.16.3.0 255.255.255.0 172.16.2.254
Router1(config)#exit
Router1#

Po nastavení

```
Router1#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.1.0 is directly connected, FastEthernet0/1
C       172.16.2.0 is directly connected, FastEthernet0/0
S       172.16.3.0 [1/0] via 172.16.2.254
Router1#
```

Všimněte si:
[1/0] – administrativní vzdálenost/metrika
via 172.16.2.254 – přes další přeskok (next hop) - vstupní port dalšího směrovače pro daný směr.

Běžící konfigurace (částečný výpis) – po nastavení směrování:

```
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 172.16.3.0 255.255.255.0 172.16.2.254
!
!
```

Nastavení přepínače:

Switch>enable
Switch#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Switch1
Switch1(config)#enable secret cisco
Switch1(config)#service password-encryption
Switch1(config)#line con 0
Switch1(config-line)#password class
Switch1(config-line)#login
Switch1(config-line)#exit

Switch1(config)#line vty 0 **15**
Switch1(config-line)#passw class
Switch1(config-line)#exit
Switch1(config)#int fa0/1
Switch1(config-if)#description PC01
Switch1(config-if)#exit
Switch1(config)#interface vlan1
Switch1(config-if)#ip address 172.16.1.253 255.255.255.0
Switch1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
Switch(config-if)#exit

Switch1(config)#ip default-gateway 172.16.1.254
Switch1(config)#exit
Switch1#sh run
Switch1#copy run start

Výpis běžící konfigurace

Všimněte si použité služby „service password-encryption“ pro (slabé) šifrování hesel ve výpisu konfigurace. (Heslo pro režim enable je zašifrováno silnou šifrou příkazem „enable secret ...“.)

```
Switch1#sh run
Building configuration...

Current configuration : 1082 bytes
!
version 12.1
service password-encryption
!
hostname Switch1
!
enable secret 5 $1$HKJM$yFxzrTiO4WZrpCvUbFp9V1
!
!
!
interface FastEthernet0/1
 description PC01
 switchport mode access
!
interface FastEthernet0/2
!
...
!
interface FastEthernet0/24
!
interface Vlan1
 ip address 172.16.1.253 255.255.255.0
!
ip default-gateway 172.16.1.254
!
```

```
line con 0
 password 7 0307570A151C
 login
!
line vty 0 4
 password 7 0307570A151C
 login
line vty 5 15
 password 7 0307570A151C
 login
!
!
end


Switch1#
```

Obsah tabulky MAC adres:

```
Switch1#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.c959.b102    DYNAMIC     Fa0/24
   1    0005.5e52.a716    DYNAMIC     Fa0/1
Switch1#
```

Varianta zapojení

Předchozí zapojení změňte, v propojovací síti mezi směrovači použijte sériovou linku. Adresy propojovací sítě zvolte v rozsahu adresního bloku 172.16.2.0/30. Nezapomeňte na straně DCE nastavit takt hodin a zrušit nastavení původní FastEthernetové propojovací linky.

Postup testování nastavené konfigurace

Obecně se testuje postupně od L1 do L7 a na další vrstvu se přejde až po ověření předchozí nižší vrstvy.

Testování protokolové sady TCP/IP

ping

návratové hodnoty ping na směrovačích:

! **OK**

. **překročení maximální povolené doby odezvy (*timeout*)**

U **nedosažitelný cíl (*destination unreachable*)**

Ověření správné instalace protokolové sady TCP/IP (protokolu IP) na klientu je:

ping localhost = #**ping 127.0.0.1**

Pokud ping na localhost funguje, je IP protokol v pořádku.

Ping na localhost neprodukuje žádný signál na přenosovém médiu.

Test stavu rozhraní směrovače

#show ip interface brief

Test konektivity směrovače

#ping 192.168.254.1

#traceroute 192.168.254.1

Test stavu rozhraní přepínače

#show ip interface brief

Test konektivity přepínače

#ping …, na síťovou kartu počítače v lokální síti

#traceroute …, na bránový směrovač

Testování lokální sítě

Otestování dostupnosti brány, bránového směrovače, směrovače dalšího přeskoku,

test směrovací tabulky bránového směrovače,

Test vzdálené sítě

Ping, traceroute

Správná „nejlepší“ cesta a krátká doba odezvy.

Monitorování a dokumentace sítě

Stav vaší sítě je nanejvýš vhodné průběžně monitorovat a porovnávat s průběžně pořizovanou dokumentací.

Důležitost vytváření dokumentace nelze dostatečně zdůraznit. Ověření konektivity (dostupnosti spojení), latence a řešení identifikovaných problémů administrátorovi pomáhá udržovat síť funkční a v maximální míře efektivní. (Směrnice pro dokumentaci na korporátní úrovni jsou samozřejmě detailnější než návod v tomto kurzu.) Pro naše účely postačí dokumentovat kompletní výstupy následujících příkazů:

- ping
- traceroute/tracert

Zjišťování uzlů v lokální síti

Ping 255.255.255.255 ($ping -b 255.255.255.255)

C:\>Arp -a (zobrazí uzly lokální sítě ve vyrovnávací paměti ARP klienta sítě)

#show mac-address-table zobrazí přepínací tabulku na přepínači

Cvičení

Odposlech komunikace na klientu lokální sítě pomocí analyzátoru síťových protokolů WireShark.

Analýza obsahu PDU na jednotlivých vrstvách pro různé typy komunikací: Telnet, , ping, tracert.

Kontrolní opakovací otázky a odpovědi (kvíz):

1) Spárujte popis příkazu a příslušný příkaz:
   a) vstup do privilegovaného režimu = enable
   b) kopie běžící konfigurace na TFTP server = copy run tftp
   c) přihlášení na vzdálený server Telnet, pouze vložením jeho lokality (IP adresou) = 192.168.23.5
   d) vložení jména souboru s konfigurací = router-config (=> není to žádné klíčové slovo IOSu)
2) Jaká sekvence příkazů umožní vzdálený přístup přes pět virtuálních linek Telnet s heslem „cisco“:
   a) Router(config)#line vty 0 4

      Router(config-line)#password cisco

      Router(config-line)#login
3) Který příkaz zapne rozhraní směrovače?
   a) Router(config-if)#no shutdown
4) Jaký je účel příkazu „enable secret“?
   a) Umožní administrátorovi nastavit silně zašifrované heslo, které bude ve výpisech konfigurace zobrazované zašifrované
5) Který příkaz vypíše statistiky všech rozhraní nastavených na směrovači?
   a) show interfaces
6) Který příkaz vypíše seznam všech příkazů, které umožňují vypisovat stavy na směrovači?
   a) Router#show ?
7) Administrátor konfiguruje nový směrovač se jménem SANJOSE. Potřebuje nastavit heslo CISCO pro konzolové připojení tohoto směrovače. Jakými příkazy?
   a) SANJOSE(config)#line con 0

      SANJOSE(config-line)#password CISCO

SANJOSE(config-line)#login

8) Administrátor musí nastavit na sériovém rozhraní IP adresu a masku, nastavení by mělo zároveň obsahovat i popis (*description*) vzdáleného připojení. Jakými příkazy?
   a) Chicago(config)#interface serial0/0/0

      Chicago(config-if)#ip address 192.168.204.9 255.255.255.252

      Chicago(config-if)#description San Jose T1

9) Co znamená na směrovači výpis „**.**“ (tečky) po příkazu ping?
   a) Vypršela povolená doba odezvy (doba čekání na odpověď echo reply)

10) Která utilita (příkaz) zobrazí cestu paketu pro dosažení cíle?
   a) traceroute

Přílohy

Rychlé zopakování prvního semestru (Cram Sheet)

Model ISO OSI

Vrstva OSI ***OSI Layer***	***Důležité funkce / Important Functions***
Aplikační ***Application***	Poskytuje rozhraní mezi komunikačním softwarem hostitele a jakoukoliv potřebnou externí aplikací. Vyhodnocuje jaké jsou potřebné a dostupné systémové zdroje pro komunikaci mezi dvěma zařízeními. Synchronizuje aplikace klient/server. Mezi aplikacemi poskytuje řízení chyb a integritu dat. Poskytuje hostiteli zpracování nezávislé na systému.
Prezentační ***Presentation***	Prezentuje data aplikační vrstvě. Funguje jako překladač formátu dat. Ovládá strukturování dat a vyjednávání syntaxe transferu dat do sedmé vrstvy. Zpracování zahrnuje šifrování a dešifrování, komprimaci a dekomprimaci dat.
Relační ***Session***	Zabývá se řízením dialogu mezi zařízeními. Určuje začátek, prostředek a konec relace (*session*) či konverzace, která se odehrává mezi (mezilehlými) aplikacemi.
Transportní ***Transport***	Řídí spojení mezi koncovými systémy (*end-to-end connections*) a doručení dat mezi dvěma klienty. Segmentuje a opětovně skládá data. Poskytuje transparentní přenos dat při skrytí detailů přenášených dat z vyšších vrstev, zapouzdřených do segmentu.
Síťová ***Network***	Určuje nejlepší cestu (*best path*) pro doručení paketu napříč sítí. Určuje logickou adresaci, která identifikuje cíl paketu či datagramu. Používá datové pakety (IP, IPX) a pakety s aktualizací tras (směrovacích protokolů RIP, EIGRP, atd.). Používá směrované protokoly IP, IPX a AppleTalk DDP. Zařízení: router a L3 switch.
Spojová ***Data Link***	Zajišťuje přenos dat ze síťové vrstvy do fyzické vrstvy. Dohlíží na fyzickou či hardwarovou adresaci. Zapouzdřuje pakety do rámce. Oznamuje výskyt chyb. Zařízení: bridge, L2 switch, network interface card.
Fyzická ***Physical***	Přenáší bity v podobě signálu mezi uzly (*node*). Asistuje při aktivaci, správě a deaktivaci fyzické konektivity mezi zařízeními. Zařízení: hub, repeater.

Standardně nejsou v OSI modelu obsaženy konkrétní protokoly, v následující tabulce jsou uvedeny protokoly spárované s OSI z protokolové sady TCP/IP a příklady protokolů pro L6 a L5.

Vrstva *Layer*	*Jméno* *Name*	*Protokoly* *Protocols*	*Adresace* *Addressing*	*Zařízení* *Devices*	*Zapoudření* *PDU*
7	Application	FTP, Telnet, TFTP, SMTP, POP3, SNMP, DNS, NTP, HTTP, HTTPS, DHCP			Data
6	Presentation	ASCII, .jpg, .doc			Data
5	Session	RPC, SQL/Telnet (pouze pro přihlášení)			Data
4	Transport	TCP - spojově orientovaný, spolehlivost dosažena pomocí dopředného potvrzování a opětovnému posílání (PAR) UDP - nespojově orientovaný, nespolehlivý, pro zajištění spolehlivosti použity protokoly vyšších vrstev	Procesy, aplikace (well known ports) (čísla portů)		Segment
3	Network	IP, ICMP, (OSPF) směrování a výběr nejlepší cesty	Logická adresace (IP adresy)	Router	Packet
2	Data Link	Ethernet, Frame Relay, PPP, HDLC	Fyzická (HW) adresace (MAC adresy)	NIC, Bridge, Switch	Frame
1	Physical	Bity přenášené na médiu v podobě signálu		Hub, Repeater, Connector	Bits

TCP a UDP

Zapamatujte si následující **dobře známá čísla portů** (*well known ports*) vybraných aplikačních protokolů:

TCP		*UDP*	
FTP	20,21	DNS	53
SSH	22	DHCP	67, 68
Telnet	23	TFTP	69
SMTP	25	NTP	123
DNS	53	SNMP	161
HHP	80		
POP	110		
NNTP	119		
HTTPS	443		

TCP

TCP používá **pozitivní potvrzení a opětovné poslání** (*Positive Acknowledgment and Retransmission (PAR)*):

- Zdrojové zařízení spustí časovač pro každý segment. Pokud nepřijde potvrzení před vypršením tohoto časovače, je segment poslán znovu.
- Zdrojové zařízení eviduje všechny odeslané segmenty a očekává pro každý z nich potvrzení.
- Cílové zařízení potvrzuje přijetí segmentu odesláním potvrzení (ACK) s pořadovým číslem (SEQ) očekávaným v následujícím segmentu.

Identifikujte jednotlivá pole záhlaví TCP:

Source Port	Destination Port
Sequence Number (SEQ)	
Acknowledgment Number (ACK)	
Misc. Flags	Window Size
Checksum	Urgent
Options	

Identifikujte jednotlivá pole záhlaví UDP:

Source Port	Destination Port
Length	Checksum

Technologie LAN

- **Ethernet:** Fyzická adresace = MAC adresa
  - 12 hexadecimálních číslic,
  - prvních 6 číslic je identifikátor (OUI) výrobce síťové karty
- Přímý kabel UTP (*straight-through*): PC k přepínači/rozbočovači (switch/hub)
- Překřížený kabel UTP (*cross-over*): hub-hub, switch-switch, router – router, PC-router (přímo tedy nikoliv přes switch nebo hub).
- Kolizní doména = jeden segment fyzické sítě.
- Switch, bridge a router segmentují kolizní doménu (segment fyzické sítě). Hub a repeater naopak fyzickou síť (kolizní doménu) rozšiřují.
- Switch zvětšuje počet kolizních domén (segmentace do mikrosegmentů, kde je ale bezkolizní prostředí) ale nerozděluje doménu všesměrového vysílání. Router, L3 switch a virtuální sítě VLAN rozdělují (segmentují) doménu všesměrového vysílání.

Přepínání (Switching)

- Přepínač (*switch*) je víceportový (*multiport*) můstek (*bridge*). Přepínače přeposílají rámce s použitím hardwarových integrovaných obvodů pro specifické použití (*ASIC, Application Specific Integrated Circuit*), což je činí rychlejšími než jsou můstky (*bridge*). Vyhrazena přenosová kapacita na port.
- Můstky a přepínače se učí MAC adresy přečtením zdrojové MAC adresy každého rámce.
- Přepínače pracují v jednom ze tří následujících režimů:
  - *Store-and-Forward* - střadačový: Je načten celý rámec a spočten kontrolní součet FCS (detekce chyb).
  - *Cut-Through*: je přečtena pouze cílová MAC adresa a rámec je přeposílán.
  - *Fragment-Free*: je načteno prvních 64 bajtů a rámec je přeposílán. Proprietární metoda Cisco.

- *Half-duplex* – poloviční duplex: sdílí kolizní doménu a nižší propustnost (*throughput*).
- *Full-duplex* – plný duplex: dvoubodové spojení (*point-to-point*) a vyšší propustnost.
- Pro vzdálenou administraci přepínače potřebujete IP adresu, masku podsítě a výchozí bránu. Přepínač musí být dosažitelný na portu ve své administrativní VLAN. (Budeme to probírat ve třetím semestru kurzu CCNA Exloration.)

Základní cíle zabezpečení dat

Cíl zabezpečení	***Popis***	***Příklady narušení tohoto zabezpečení***	***Kroky ke zmírnění nebezpečí***
Confidentiality **Důvěrnost**	Zajistí neveřejnost dat a to, aby nemohla být odposlouchávána (*eavesdropping*).	Zachytávání paketů.	Šifrování, aby se skryl obsah přenášených dat.
Integrity **Integrita**	Zajistí, aby data nemohla být změněna.	Útoky vlastních zaměstnanců. (*Man-in-the-middle (MiTM) attacks*)	Výpočty a uložení kontrolních součtů (*hashing*) identifikující data (*fingerprint*), aby se ověřilo, že data nebyla změněna oproti jejich původní podobě.
Availability **Dostupnost**	Zajistí, aby byly vaše data, klienti a služby dostupné pro jejich zamýšlený účel.	Útoky typu odepření služby (*Denial of service (DoS) attacks*)	Použití limitů rychlostí a objemů datových přenosů, aby se zarazily extrémní datové toky a instalace posledních dostupných záplat (*patch*) OS.

Opakování – Poziční číselné soustavy a data v počítači

Uložení informací v počítači

Informace je zpráva o nějaké nové skutečnosti z reálného světa, to jak člověk chápe data. (Význam, který člověk přisuzuje datům. (ČSN 369001/1-1987))

Data jsou formou uložení jednotlivých částí informace v počítači.

Počítač je stroj na zpracování informací.

Jednotky dat (informace) v počítači

1 bit (bit) (1 b) (zkratka „**b**inary dig**it“** česky **binární číslice**; jinak slovo bit znamená anglicky kousek) má 2 stavy (2^1): {0, 1}; nebo také {False; True} nebo-li {Nepravda, Pravda}[91]

1 byte (česky někdy též **bajt) (1 B)** česky **slabika** je osmibitové binární číslo, má 256 stavů (2^8): {00, 01, … EF, FF} (zápis jednoho bajtu je dvouciferným hexadecimálním číslem, 1 hexadecimální číslice například 8_{16} je binárně zapsaná jako 1000_2). Byte je nejmenší přímo adresovatelné místo v paměti počítače.

1 word česky **slovo** je obvykle šestnáctibitové binární číslo, má 65 536 stavů ($2^{16} = 16^4$): {0000, … FFFF} (zápis je čtyřciferným hexadecimálním číslem). Moderní počítače používají délku slova 16, 32 nebo 64 bitů ("quadruple word").

Prefixy pro binární násobky používající symboly SI

1 KB = 2^{10} B =1024 B	na rozdíl od **k** ve fyzice	= 10^3 = 1 000
1 MB = 2^{20} B = 2^{10} KB = 1 048 576 B	na rozdíl od **M** ve fyzice	= 10^6 = 1 000 000.
1 GB = 2^{30} B = 2^{10} MB = ...	na rozdíl od **G** ve fyzice	= 10^9 = 1 000 000 000.

Prefixy pro binární násobky podle IEC

Podle *Internernational Electrotechnical Comission (IEC).*

Mocnina	Jméno	Symbol	Původ jména (z EN)	Odvození a jméno SI prefixu
2^{10}	kibi	Ki	kilobinary: $(2^{10})^1$	kilo: $(10^3)^1$
2^{20}	mebi	Mi	megabinary: $(2^{10})^2$	mega: $(10^3)^2$
2^{30}	gibi	Gi	gigabinary: $(2^{10})^3$	giga: $(10^3)^3$
2^{40}	tebi	Ti	terabinary: $(2^{10})^4$	tera: $(10^3)^4$

91 Slovo bit navrhl J. W. Tukey. Zařízení se dvěma stabilními stavy, jako je relé nebo klopný obvod, může uchovat jeden bit informace. N takových zařízení může uchovat N bitů. [The Bell System Technical Journal, Vol. 27, p. 379, (July 1948).] V počítačové terminologii se udává, že jeden bit je jednotkou informace. Jeden bit je přitom vyčíslen jako pravděpodobnost jevu že nastane nějaká skutečnost. Pokud máme nějakou skutečnost s pravděpodobností 50% máme jeden bit

Mocnina	Jméno	Symbol	Původ jména (z EN)	Odvození a jméno SI prefixu
2^{50}	pebi	Pi	petabinary: $(2^{10})^5$	peta: $(10^3)^5$
2^{60}	exbi	Ei	exabinary: $(2^{10})^6$	exa: $(10^3)^6$

Příklady a srovnání hodnot binárních prefixů s SI prefixy

jeden **kibibit**	1 Kibit = 2^{10} bit = **1024 bit**
jeden **kilobit**	1 kbit = 10^3 bit = **1000 bit**
jeden **mebibyte**	1 MiB = 2^{20} B = **1 048 576 B**
jeden **megabyte**	1 MB = 10^6 B = **1 000 000 B**
jeden **gibibyte**	1 GiB = 2^{30} B = **1 073 741 824 B**
jeden **gigabyte**	1 GB = 10^9 B = **1 000 000 000 B**

Poziční číselné soustavy

Zápis celého kladného N-ciferného čísla v poziční číselné soustavě o základu Z pomocí rozvoje (polynomu):

$$(a_{N-1}a_{N-2}\ldots a_1a_0)_Z = a_{N-1}\cdot Z^{N-1} + a_{N-2}\cdot Z^{N-2}\ldots + a_1\cdot Z^1 + a_0\cdot Z^0 = \sum_{i=0}^{N-1} a_i\cdot Z^i$$

kde je:

a_{N-1} číslice (koeficient polynomu) (= celé kladné číslo) na N-1 řádu (pozici s váhou Z^{N-1})

Z základ číselné soustavy (= celé kladné číslo větší než 0) a zároveň počet číslic v dané číselné soustavě

Z–1 nejvyšší číslice v číselné soustavě o základu Z

Pamatujte, že v každé číselné soustavě platí, při přičtení jedničky k nejvyšší číslici v dané číselné soustavě dojde k přenosu 1 do vyššího řádu: $((Z-1)+1)_{10} = (10)_Z$

N počet číslic v čísle

Z^{N-1} váha číslice v čísle na N-1 pozici zprava (začíná se od nulté pozice)

Z^N celkový počet možných stavů (kombinací) v čísle o počtu N míst při základu Z.

Σ (velké řecké sigma) čtěte „suma“ značí operátor „součet řady“

Všichni znáte čísla v desítkové (Z = 10) soustavě, dále se budeme zabývat čísly v soustavě dvojkové (Z = 2) a šestnáctkové (Z = 16). Pro práci v lepším kontextu se nejprve ještě podíváme na desítkovou soustavu.

Desítková (dekadická) soustava

Základ Z = 10. (Zkratka (dolní index) 10 nebo D nebo také žádný – je nejobvyklejší.)

Počet stavů jedné dekadické číslice = počet různých číslic = $10^1 = 10$: {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}

Řád	*Dekadicky*
10^0 =	1
10^1 =	10
10^2 =	100
10^3 =	1 000
10^4 =	10 000
10^5 =	100 000
10^6 =	1 000 000

Příklad

Pamatujte na přenos do vyššího řádu: $(9+1)_{10}=(10)_{10}$

Počet stavů (možných kombinací) dvoumístného desítkového čísla je $10^2 = 100$ (0 .. 99).

$(101)_{10} = (1.\ 10^2 + 0.\ 10^1 + 1)_{10} = (101)_{10}$

Dvojková (binární) soustava

Základ Z = 2. (Zkratka (dolní index) 2 nebo B.)

Počet stavů jedné dekadické číslice = počet různých číslic = $2^1 = 2$: {0, 1}

Řád	*Dekadicky*	*Binárně*
2^0 =	1	1
2^1 =	2	10
2^2 =	4	100
2^3 =	8	1 000
2^4 =	16	10 000
2^5 =	32	100 000
2^6 =	64	1 000 000
2^7 =	128	10 000 000
2^8 =	256	100 000 000
2^9 =	512	1 000 000 000
2^{10}=	1 024	10 000 000 000
2^{11}=	2 048	100 000 000 000
2^{12}=	4 096	1 000 000 000 000
2^{13}=	8 192	10 000 000 000 000
2^{14}=	16 384	100 000 000 000 000

Řád	*Dekadicky*	*Binárně*
2^{15}=	32 768	1 000 000 000 000 000
2^{16}=	65 536	10 000 000 000 000 000

Příklad

$(2)_{10} = (10)_2$

$(101)_2 = (1. 4 + 0. 2 + 1. 1) = (5)_{10}$

$(5)_{10} = (1. 100 + 0. 10 + 1. 1)_2 = (101)_2$

Algebraické operace ve dvojkové soustavě

Sčítání ve dvojkové soustavě

Pravidla:

0 + 1 = 1

0 + 0 = 0

1 + 1 = 10 = 0 a zároveň „přetečení“ tj. přenos 1 do vyššího řádu.

Všimněte si, že poslední pravidlo platí pro libovolnou číselnou soustavu: pokud přičtu jedničku k nejvyšší číslici v dané číselné soustavě je výsledek 0 a přenos 1 do vyššího řádu. (Například v desítkové soustavě: $(9+1=10)_{10}$ v šestnáctkové: $(F + 1 = 10)_{16}$.)

Příklad

$(01100111)_2 + (11101110)_2 = (101010101)_2$

Odečítání ve dvojkové soustavě

Pravidla:

0 – 0 = 0

1 – 0 = 1

0 – 1 = 1 a zároveň přenos 1 do vyššího řádu **menšitele**

1 – 1 = 0

Odečítání je přičtení záporného čísla. Záporné číslo vytvoříte z kladného inverzí všech bitů (0<->1) a přičtením 1 na nultém řádu. Nejvyšší řád čísla tvoří tzv. Znaménkový bit. Z toho je patrné, že předem musíte znát s kolika místnou reprezentací binárních čísel pracujete.

Příklad

$(0000\ 1101)_2 – (0000\ 1100)_2 = (0000\ 1101)_2 + (1111\ 0011)_2 + (1)_2 = (0000\ 0001)_2$

Přenos jedničky do osmého řádu (přenosového bitu (*auxiliary bit*)) již neuvažujeme (je to mimo rozsah zpracovávaného formátu čísla).

Uvědomte si, že pokud od nuly odečtete jedničku v libovolné číselné soustavě, je výsledkem vždy nejvyšší číslice v příslušné číselné soustavě a přenos mínus jedničky do vyššího řádu.

Například v číselné soustavě o základu 256, což je mimo jiné také takzvaný kanonický zápis IPv4 adres, dostaneme:

$$\left(\begin{array}{r} 0.\ 0.\ 2.\ 0 \\ -\ 0.\ 0.\ 0.\ 1 \\ \hline 0.\ 0.\ 1.255 \end{array}\right)_{256}$$

Šestnáctková (hexadecimální) soustava

Základ Z = 16. (Zkratka (dolní index)16 nebo H.)

Počet stavů jedné hexadecimální číslice = počet různých číslic = 16^1 = 16: {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F}

Desítkové tvary šestnáctkových číslic

10	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

Poznámka: u číslic A – F se nerozlišuje, zda jde o malá nebo velká písmena.

Řád	*Dekadicky*	*Binárně*	*Hexadecimálně*
16^0 =	1	2^0	1
16^1 =	16	2^4	10
16^2 =	256	2^8	100
16^3 =	4 096	2^{12}	1 000
16^4 =	65 536	2^{16}	10 000
16^5 =	1 048 576	2^{20}	100 000
16^6 =	16 777 216	2^{24}	1 000 000

POZOR: Všimněte si, že při posuvu (zvětšení) řádu čísla o jeden v šestnáctkové soustavě se ve dvojkové soustavě posune (zvětší) řád čísla o čtyři. Příklad:$(10)_{16} = (0001\ 0000)_2$

Příklad

$(16)_{10} = (10)_{16}$

$(26)_{10} = (10 + A)_{16} = (1A)_{16} = (1A)_H$

$(1A)_{16} = (1.\ 16 + 10\ .\ 1)_{10} = (26)_{10}$

Poznámka

V ICT (počítačové) branži se 1 B (1 bajt) (což je dvojciferné šestnáctkové číslo) obvykle zapisuje s prefixem

0x.. (nula a malé písmeno x) (Například $1A_{16}$ = 0x1A).

Převod čísla ze soustavy o základu Z do desítkové soustavy

Použitá metoda: Přímou aplikací (výpočtem) polynomu (rozvoje) definující číslo v číselné soustavě o základu Z. Jednotlivé číslice z čísla o základu Z si vždy rovnou převádíte do desítkové soustavy a násobíte příslušnou váhou řádu (pozice) číslice v čísle = mocninou základu Z.

Příklad

$(1\ 1\ 0\ 1\ 0)_2 = (1.\ 2^4 + 1.\ 2^3 + 0.\ 2^2 + 1.\ 2^1 + 0.\ 2^0)_{10} = 16 + 8 + 2 = (26)_{10}$

4 3 2 1 0 16 8 4 2 1

řád ↑

Převod čísla z desítkové soustavy do soustavy o základu Z

Použitá metoda: Hledáním zbytku po celočíselném dělení čísla v desítkové soustavě základem číselné soustavy Z, do které převádíme.

Příklad

$(26)_{10} = (X)_{16}$ 26 : 16 = 1 (zbytek po dělení = $10_{10} = A_{16}$)

1 : 16 = **0** (zbytek po dělení = $1_{10} = 1_{16}$) = $1A_{16}$

Konec výpočtu vždy až do výsledku dělení = 0.

POZOR: **první zbytek po dělení** nejvyššího řádu převáděného desítkového čísla tvoří první číslici zprava (tj. **nejnižší řád čísla) výsledku** v nové číselné soustavě.

$(26)_{10} = (1A)_{16}$

Proveďte si vždy také zpětnou kontrolu!!!: $1A_H = (1.\ 16 + 10\ .\ 1)_{10} = 26_{10}$

Převeďte: (255)10 = (XX)16. (255:16)=15 (Zbytek pro dělení = $15_{10} = F_{16}$)

(15:16)= 0 (Zbytek po dělení = $15_{10} = F_{16}$) => **FF_{16}**

Modifikace postupu pro základ 2 (odečítací metoda)

Pro převod malých čísel (obvykle <=255) z desítkové soustavy do dvojkové lze ještě použít následující postup (je to vlastně modifikace výše uvedeného):

Hodnoty mocnin dvojky (základu) na jednotlivých pozicích binárního čísla slouží jako pomůcka pro zápis výsledku v dále uvedené tabulce:

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Od zadaného desítkového čísla postupně odečítáte od nejvyšší jednotlivé mocniny dvou a do tabulky zapisujete v příslušném sloupci jednotku, pokud jste tak učinili a nulu, pokud ne.

Je to zřejmé z následujícího příkladu pro číslo 207.

Postupné odečítání mocnin dvou od desítkového čísla je uvedené dále:

128	207
	-128
64	79
	-64
8	15
	-8
4	7
	-4
2	3
	-2
	1

1. Začněte od nejvyššího čísla vlevo v tabulce (tj. 128). Určete, zda je jím desítkové číslo dělitelné, pokud ano, zapište 1 do 3. řádky v tabulce pod číslo 128 a spočtěte zbytek (= odečtěte 128), tj 79.
2. Když je zbytek dělitelný další hodnotou 64, zapište 1 do třetí řádky v tabulce pod 64 a odečtěte 64.
3. Když zbytek není dělitelný 32 nebo 16, zapište 0 do třetí řádky tabulky pod 32 a 16.
4. Pokračujte, dokud není zbytek roven nule.
5. Pokud je třeba použijte čtvrtou řádku tabulky pro kontrolu práce.

7	6	5	4	3	2	1	0
128	64	32	16	8	4	2	1
1	1	0	0	1	1	1	1
128	64			8	4	2	1

Součet čtvrté řádky v tabulce je 207, což jsme chtěli dokázat.

Vzájemné převody šestnáctkové a dvojkové soustavy

Převod ze šestnáctkové do dvojkové soustavy

Každou šestnáctkovou číslici (ze šestnáctkového čísla) z hlavy převedete na desítkové číslo a to obvyklým postupem (převod 2_{10} -> 0010_2) na čtyřmístné dvojkové číslo (anglicky nibble). Nezapomeňte v případě potřeby vždy doplnit nevýznamné nuly zleva (do čtyř pozic). Takto vypočtená čtyřmístná dvojková čísla zapisujete zleva doprava. (Například: číslici D si „z hlavy“ (postupným celočíselným dělením dvojkou nebo odečítáním mocnin dvojky) převedete na na desítkové číslo 13, to si rozložíte na součet 8 + 4 +1 a zapíšete jako 1101.)

Tabulka převodu hexadecimálních číslic na čtyřbitová binární čísla (binární čtyřčíslí[92])

16	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
10	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111

Příklad

$(25)_{16} = (0010\ 0101)_2$

$(1D65)_{16} = (0001\ 1101\ 0110\ 0101)_2$

Pamatujte

$(F + 1)_{16} = (10)_{16}$

Převod z dvojkové do šestnáctkové soustavy

Dvojkové číslo zprava (od nejnižšího řádu) rozdělíte po čtyřech řádech. Každé toto čtyřmístné binární číslo zleva doprava převedete z hlavy na desítkové číslo a to pak také z hlavy na šestnáctkovou číslici. Tyto šestnáctkové číslice opět zapíšete zleva doprava.

Příklad

$(0001\ 0000)_2 = (10)_{16}$

Souhrnné příklady

Vyzkoušejte si několik následujících převodů:

Desítková	*Šestnáctková*	*Dvojková*
150	96	1001 0110
99	63	0110 0011
10	A	1010
15	F	1111

92 Binárnímu čtyřčíslí se anglicky říká nibble.

Desítková	*Šestnáctková*	*Dvojková*
25	19	0001 1001
200	C8	1100 1000
~~500~~	~~1F4~~	~~0001 1111 0100~~
~~450~~	~~1C2~~	~~0001 1100 0010~~
~~2000~~	~~7D0~~	~~0111 1101 0000~~
~~3333~~	~~D05~~	~~1101 0000 0101~~
~~5432~~	~~1538~~	~~0001 0101 0011 1000~~
~~4256~~	~~10A0~~	~~0001 0000 1010 0000~~
~~10251~~	~~280B~~	~~0010 1000 0000 1011~~
~~9153~~	~~23C1~~	~~...~~
~~524288~~	~~80000~~	~~...~~
~~1048576~~	~~100000~~	~~...~~

Poznámka: pro naše účely postačuje umět „z hlavy“ převádět celá čísla v rozsahu jeden bajt.

Logické binární operátory

Binární logický operátor vrací logickou hodnotu nepravda/pravda (0, 1) v závislosti na hodnotě dvou vstupních logických operandů.

Logický součin (**AND**, anglicky “a zároveň“) je pravdivý pouze a jen tehdy, pokud jsou oba vstupní operandy pravdivé.

Logický součet (**OR**, anglicky „nebo“) je nepravdivý pouze a jen tehdy, pokud jsou oba vstpní operandy nepravdivé.

Pravdivostní tabulka

A	*B*	*A AND B*	*A OR B*
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	1

Logický operátor AND používáme při práci se síťovou maskou.

Příklad:

168 AND 192 = 128.

Vycházíme z toho, že se jedná o binární čísla a logický součin AND se provádí pro každé dvě číslice stejných řádů v obou číslech.

1010 1000 AND 1100 0000 = 1000 0000.

Adresace v počítačové síti

IP adresa

32-bitové celé binární číslo, zapisované obvykle (z důvodu pro člověka jednoduššího čtení) v *kanonickém* neboli *tečkovém desítkovém formátu* (= dekadickém formátu odděleném tečkami). Číslo je děleno po jednotlivých *oktetech* (= 8 bitech) do čtyř bajtů, které jsou vyjádřeny dekadicky.

IP adresa identifikuje síťové rozhraní počítače vůči protokolu IP, který odesílá a přijímá pakety IP.

Příklad kanonického zápisu IP adresy

00001000 00000100 00000010 00000001 → **8.4.2.1**

MAC adresa

48-bitové celé binární číslo. 48 bitů = 6 bajtů. Obvykle se vypisuje po jednotlivých oktetech v hexadecimálním tvaru odděleném po každých dvou bajtech (čtyřech hexadecimálních číslicích) tečkami.

Ethernetová MAC adresa. Fyzická adresa síťové karty. (*MAC = Media Access Control = nižší ze dvou podvrstev spojové vrstvy)*

Příklad zápisu MAC adresy

11111111 11111111 11111111 11111111 11111111 11111111 → **FFFF.FFFF.FFFF**

→ **FF-FF-FF-FF-FF-FF**

→ **FF:FF:FF:FF:FF:FF**

Převody mezi soustavami (0 - 127)

Binární	Dekadická	Hexa-decimální	Znak ANSI
00000000	0	0	□
00000001	1	1	
00000010	2	2	
00000011	3	3	
00000100	4	4	
00000101	5	5	
00000110	6	6	
00000111	7	7	
00001000	8	8	
00001001	9	9	
00001010	10	A	
00001011	11	B	
00001100	12	C	
00001101	13	D	
00001110	14	E	
00001111	15	F	
00010000	16	10	
00010001	17	11	
00010010	18	12	
00010011	19	13	
00010100	20	14	
00010101	21	15	
00010110	22	16	
00010111	23	17	
00011000	24	18	
00011001	25	19	
00011010	26	1A	
00011011	27	1B	
00011100	28	1C	
00011101	29	1D	
00011110	30	1E	
00011111	31	1F	
00100000	32	20	
00100001	33	21	!
00100010	34	22	"
00100011	35	23	#
00100100	36	24	$
00100101	37	25	%
00100110	38	26	&
00100111	39	27	'
00101000	40	28	(
00101001	41	29	)
00101010	42	2A	*
00101011	43	2B	+
00101100	44	2C	,
00101101	45	2D	-
00101110	46	2E	.
00101111	47	2F	/
00110000	48	30	0
00110001	49	31	1
00110010	50	32	2
00110011	51	33	3
00110100	52	34	4
00110101	53	35	5
00110110	54	36	6
00110111	55	37	7
00111000	56	38	8
00111001	57	39	9
00111010	58	3A	:
00111011	59	3B	;
00111100	60	3C	<
00111101	61	3D	=
00111110	62	3E	>
00111111	63	3F	?

Binární	Dekadická	Hexa-decimální	Znak ANSI
01000000	64	40	@
01000001	65	41	A
01000010	66	42	B
01000011	67	43	C
01000100	68	44	D
01000101	69	45	E
01000110	70	46	F
01000111	71	47	G
01001000	72	48	H
01001001	73	49	I
01001010	74	4A	J
01001011	75	4B	K
01001100	76	4C	L
01001101	77	4D	M
01001110	78	4E	N
01001111	79	4F	O
01010000	80	50	P
01010001	81	51	Q
01010010	82	52	R
01010011	83	53	S
01010100	84	54	T
01010101	85	55	U
01010110	86	56	V
01010111	87	57	W
01011000	88	58	X
01011001	89	59	Y
01011010	90	5A	Z
01011011	91	5B	[
01011100	92	5C	\
01011101	93	5D	]
01011110	94	5E	^
01011111	95	5F	_
01100000	96	60	`
01100001	97	61	a
01100010	98	62	b
01100011	99	63	c
01100100	100	64	d
01100101	101	65	e
01100110	102	66	f
01100111	103	67	g
01101000	104	68	h
01101001	105	69	i
01101010	106	6A	j
01101011	107	6B	k
01101100	108	6C	l
01101101	109	6D	m
01101110	110	6E	n
01101111	111	6F	o
01110000	112	70	p
01110001	113	71	q
01110010	114	72	r
01110011	115	73	s
01110100	116	74	t
01110101	117	75	u
01110110	118	76	v
01110111	119	77	w
01111000	120	78	x
01111001	121	79	y
01111010	122	7A	z
01111011	123	7B	{
01111100	124	7C	|
01111101	125	7D	}
01111110	126	7E	~
01111111	127	7F	□

Převody mezi soustavami (128 - 255)

Binární	Dekadická	Hexa-decimální	Znak ANSI
10000000	128	80	€
10000001	129	81	
10000010	130	82	‚
10000011	131	83	
10000100	132	84	„
10000101	133	85	…
10000110	134	86	†
10000111	135	87	‡
10001000	136	88	
10001001	137	89	‰
10001010	138	8A	Š
10001011	139	8B	‹
10001100	140	8C	Ś
10001101	141	8D	Ť
10001110	142	8E	Ž
10001111	143	8F	Ź
10010000	144	90	
10010001	145	91	‘
10010010	146	92	’
10010011	147	93	“
10010100	148	94	”
10010101	149	95	•
10010110	150	96	–
10010111	151	97	—
10011000	152	98	
10011001	153	99	™
10011010	154	9A	š
10011011	155	9B	›
10011100	156	9C	ś
10011101	157	9D	ť
10011110	158	9E	ž
10011111	159	9F	ź
10100000	160	A0	
10100001	161	A1	ˇ
10100010	162	A2	˘
10100011	163	A3	Ł
10100100	164	A4	¤
10100101	165	A5	Ą
10100110	166	A6	¦
10100111	167	A7	§
10101000	168	A8	¨
10101001	169	A9	©
10101010	170	AA	Ş
10101011	171	AB	«
10101100	172	AC	¬
10101101	173	AD	-
10101110	174	AE	®
10101111	175	AF	Ż
10110000	176	B0	°
10110001	177	B1	±
10110010	178	B2	˛
10110011	179	B3	ł
10110100	180	B4	´
10110101	181	B5	µ
10110110	182	B6	¶
10110111	183	B7	·
10111000	184	B8	¸
10111001	185	B9	ą
10111010	186	BA	ş
10111011	187	BB	»
10111100	188	BC	Ľ
10111101	189	BD	˝
10111110	190	BE	ľ
10111111	191	BF	ż

Binární	Dekadická	Hexa-decimální	Znak (1250)
11000000	192	C0	Ŕ
11000001	193	C1	Á
11000010	194	C2	Â
11000011	195	C3	Ă
11000100	196	C4	Ä
11000101	197	C5	Ĺ
11000110	198	C6	Ć
11000111	199	C7	Ç
11001000	200	C8	Č
11001001	201	C9	É
11001010	202	CA	Ę
11001011	203	CB	Ë
11001100	204	CC	Ě
11001101	205	CD	Í
11001110	206	CE	Î
11001111	207	CF	Ď
11010000	208	D0	Đ
11010001	209	D1	Ń
11010010	210	D2	Ň
11010011	211	D3	Ó
11010100	212	D4	Ô
11010101	213	D5	Ő
11010110	214	D6	Ö
11010111	215	D7	×
11011000	216	D8	Ř
11011001	217	D9	Ů
11011010	218	DA	Ú
11011011	219	DB	Ű
11011100	220	DC	Ü
11011101	221	DD	Ý
11011110	222	DE	Ţ
11011111	223	DF	ß
11100000	224	E0	ŕ
11100001	225	E1	á
11100010	226	E2	â
11100011	227	E3	ă
11100100	228	E4	ä
11100101	229	E5	ĺ
11100110	230	E6	ć
11100111	231	E7	ç
11101000	232	E8	č
11101001	233	E9	é
11101010	234	EA	ę
11101011	235	EB	ë
11101100	236	EC	ě
11101101	237	ED	í
11101110	238	EE	î
11101111	239	EF	ď
11110000	240	F0	đ
11110001	241	F1	ń
11110010	242	F2	ň
11110011	243	F3	ó
11110100	244	F4	ô
11110101	245	F5	ő
11110110	246	F6	ö
11110111	247	F7	÷
11111000	248	F8	ř
11111001	249	F9	ů
11111010	250	FA	ú
11111011	251	FB	ű
11111100	252	FC	ü
11111101	253	FD	ý
11111110	254	FE	ţ
11111111	255	FF	˙

Použitá literatura

- Kolektiv: Online kurikulum CCNA Exploration – Network Fundamentals verze 4.0 (aktuální verze je pro registrované uživatele dostupná na portálu cisco.netacad.net)
- Kolektiv: Course Booklet CCNA Exploration – Network Fundamentals verze 4.0, Cisco Press 2009
- Prezentace PowerPoint k jednotlivým kapitolám kurikula (pro registrované instruktory jsou dostupné na portálu cisco.netacad.net)
- DYE, Mark A. a kol.: CCNA Exploration Companion Guide – Network Fundamentals, Cisco Press 2008
- RUFI, Antoon W. a kol.: CCNA Exploration Labs and Study Guide – Network Fundamentals, Cisco Press 2008
- SCOTT, Empson: CCNA Portable Command Guide, Cisco Press 2007 (v roce 2009 vyšel český překlad „CCNA Kompletní přehled příkazů“ v nakladatelství Computer Press)
- Kolektiv: jednotlivá RFC ke zmiňovaným protokolům http://www.ietf.org/rfc.html
- CIOARA, Jeremy a kol.: CCNA Exam Prep (Second Edition), Pearson Education 2008
- VALENTINE, Michael a kol.: CCNA Exam Cram (Third Edition), Que Publishing 2008
- CIOARA, Jeremy: CCNA Practice Questions (Exam 640-802) (Third Edition), Que Publishing 2008
- ODOM, Wendell: CCNA Video Mentor (Second Edition), Cisco Press 2008
- McQUERRY, Steve: Authorized Self-Study Guide Preparation Library (Seventh Edition), Cisco Press 2008
- LAMMLE Todd: CCNA: Cisco Certified Network Associate, Study Guide (Sixth Edition), Wiley Publishing 2007 (v roce 2010 vyšel český překlad CCNA „Výukový průvodce přípravou na zkoušku 640-802“ v nakladatelství Computer Press)

Doporučená motivační četba – bezpečnost datových sítí

- STOLL, Cliff: The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, Simon & Schuster, Inc. 1989 (v roce 1997 vyšel český překlad „Kukaččí vejce“ v nakladatelství Mladá fronta)

Studijní materiál

CCNA Exploration – Základy sítí

(Semestr 1)

Kolektiv autorů (řešitelé projektu):

Koncepce a text: Ing. Miroslav Páv

Vektorová grafika: Mgr. Jan Syřínek

Konzultace angličtiny: Mgr. Jana Hošková

Vydala: VOŠ a SPŠE Plzeň, Koterovská 85, 326 00 Plzeň v roce 2011

Tisk: Typos, tiskařské závody, s.r.o., Podnikatelská 1160/14, 320 56 Plzeň

Vydání: 1. (*elektronická verze: 3.04, export do formátu PDF: 10.10.2011*)

218 stran

Tato publikace je spolufinancována Evropským sociálním fondem a státním rozpočtem České republiky v rámci projektu „Výuka počítačových sítí v mezinárodním programu Síťová akademie Cisco na střední průmyslové škole elektrotechnické“.

Registrační číslo projektu: CZ.1.07/1.1.12/01.0004.