

Počítačové sítě

Jan Outrata



KATEDRA INFORMATIKY
UNIVERZITA PALACKÉHO V OLMOUCI

přednášky

Tyto slajdy byly jako výukové a studijní materiály vytvořeny za podpory grantu FRVŠ 1358/2010/F1a.

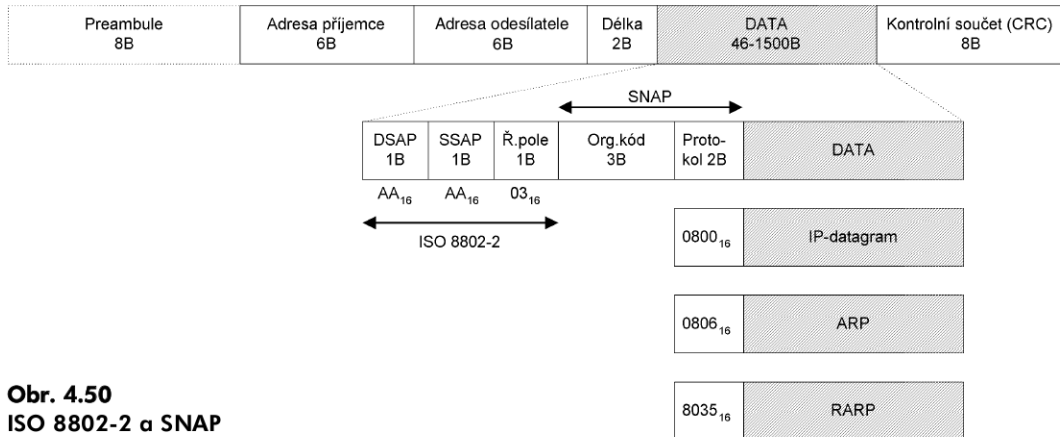
Technologie linkové vrstvy

- původně LAN = uzly propojené stejnou síťovou technologií (např. segment Ethernetu), v rámci LAN stejný linkový protokol
- dnes LAN = propojení LAN s obecně **různými technologiemi** a linkovými protokoly pomocí **mostů** nebo (většinou) **přepínačů**
- WAN = propojení (dnešních) LAN pomocí **směrovačů**
- **norma IEEE 802.1**: celková architektura sítí 802 (LAN/MAN), propojení sítí (na úrovni podvrstvy MAC), napojení na vyšší vrstvu, tvorba VLAN, bezpečnost, autorizace, atd.

■ norma IEEE 802.2

- řešena HW i SW, nezávislá na HW (fyzickém řešení sítě), rozhraní mezi podvrstvami MAC a LLC ~ rozhraní mezi HW a SW
- navazování, správa a ukončování **linkových spojení**, řízení bezpečného (s rozpoznáváním chyb) přenosu dat mezi (dvěma) uzly sítě, identifikace vyšších protokolů
- pro protokoly bez vyšších funkcí, např. NetBEUI, poskytuje **datagramovou službu** a **virtuální linkové spoje** s potvrzováním příjmu (vychází z HDLC LAPB, viz HDLC)
- rámec: specifikace cílové (**DSAP**) a zdrojové služby (**SSAP**) (pro SNAP 0xAA, pro NetBIOS 0xF0, čísla viz RFC 1700), řídící pole HDLC (číslování, znovuzasílání atd., typ rámce I, U, S, viz HDLC, u IP rámce typu U, pole = 0x3)

Obrázek: Obrázek sítě 125



Obr. 4.50
ISO 8802-2 a SNAP

- **norma IEEE 802.1d**, propojení (různých) LAN na úrovni MAC podvrstvy (**transparent MAC bridge**), např. Ethernet a WLAN, Ethernet a FDDI, možnost stanovení priorit přenosu s přiřazenou třídou (802.1p)
- transparentní vzhledem k vyšším protokolům a např. ve vícesegmentové homogenní síti Ethernet (sít se jeví jako jeden segment, např. Ethernetové segmenty s opakovači)
- = multiportový opakovač, ale rámce jsou opakovány jen na to (jiné) rozhraní (port) mostu, ke kterému je připojen adresát rámce; všesměrové (broadcast) rámce jsou opakovány na všechny ostatní porty
- **filtrační tabulka**: linková (MAC) adresa vs. port – naplněná manuálně nebo automaticky samoučením (omezená doba platnosti položek, např. 300 s)
- **stavová tabulka** portů – seznam aktivních a blokováných portů
- parametry: velikost filtrační tabulky, filtrační výkon (načtené rámce/s, přenosový výkon (zopakované rámce/s)

Algoritmus TRA (Transport Roding Algorithm)

- naplnění, aktualizace a použití filtrační tabulky
- uloží do tabulky adresu odesílatele rámce vs. port, kterým rámec přišel = **learning**
- pokud adresa adresáta rámce není v tabulce, pracuje jako opakovač (tj. zopakuje rámec na všechny svoje porty kromě toho, kterým přišel)
- pokud v tabulce adresa adresáta rámce je a pokud je asociovaný port jiný než port asociovaný s adresou odesílatele a není blokový, odešle rámec jen na port asociovaný s adresou adresáta = **forwarding**
- při blokovém portu rámec neodešle = **filtering**
- omezení na stromovou topologii sítě s více mosty (např. záložními) – jinak možný cyklický oběh rámců!

Algoritmus výběru kostry (STA, Spanning Tree Algorithm)

- výpočet **stromové topologie sítě** s potlačením smyček v libovolné topologii
- 1 mosty identifikovány prioritou a MAC adresou, zvolen **kořenový most** (s nejnižším id)
- 2 všechny ostatní mosty si označí jako **kořenový/root port** ten port, kterým vede nejlevnější (nejkratší) cesta ke kořenovému mostu (při více takových cestách ta přes souseda s nejnižším id)
- 3 z mostů na stejném segmentu se vybere ten s nejlevnější cestou (a nejnižším id) ke kořenovému mostu a jeho port do segmentu je označen (**designated port**)
- 4 ostatní porty mostu a neoznačené porty ostatních mostů jsou zablokovány (**blocked port**)
- periodicky (2 s) se opakuje, mosty si pomocí konfiguračních zpráv (BDPU rámce, SSAP a DSAP = 42 v LLC záhlaví) vyměňují info s id a cenou na speciální multicast MAC adrese

Protokol výběru kostry (STP, Spanning Tree Protocol)

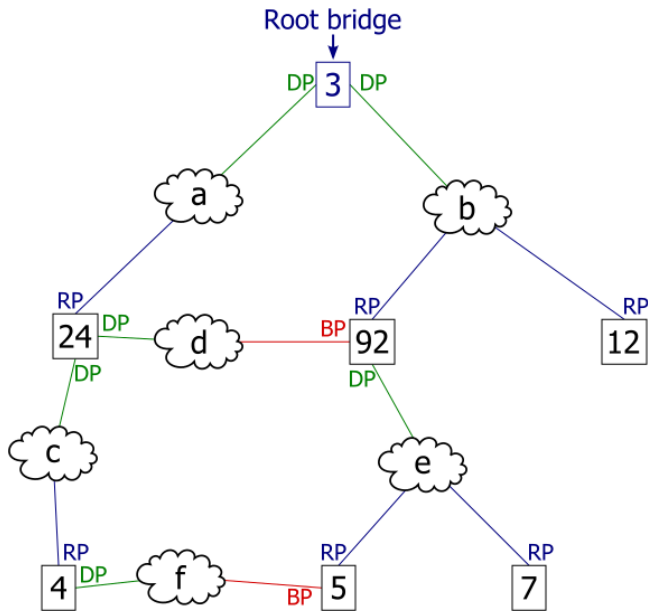
Obrázek: Obrázek Wikipedie [Spanning Tree Protocol]

BDPU rámec: typ a příznak zprávy (např. konfigurace, změna topologie), id kořenového a aktuálního mostu, id portu, který odeslal rámec, cena cesty ke kořenovému mostu, čas odeslání rámce, aj.

Protokol GARP

- dynamická registrace atributů mostu a uzlů na speciálních MAC adresách (např. skupinová adresa, VLAN identifikátor aj.)
- **protokol GMRP** pro vytváření skupin se skupinovou adresou

Most (Bridge) [LAN]



- původně s opakovači propojujícími (linkové) segmenty
- rámce se šíří segmentem po sdíleném médiu nezávisle na sobě, stanice (síťové rozhraní) **“vidí” všechny, ale přijímá jen ty adresované jí** nebo všeobecně (“normální” režim/mód)
- v tzv. **promiskuitním režimu** přijímá (a předává OS) všechny rámce
- uzly rovnocenné, jen jeden v daném čase využívá sdílené přenosové médium pro vysílání rámců = režim (Half/Full) Duplex
- 10Gigabitový Ethernet již nepoužívá sdílené médium (pouze režim Full Duplex)

Protokol CSMA/CD (Carrier Sense Multiple Access/Collision Detection)

→ **kolizní přístup** ke sdílenému médiu:

- 1 stanice na médiu naslouchá (Carrier) a vysílá, až když nevysílá žádná jiná (tj. společné médium není používáno)
- 2 když takto začne vysílat více stanic zároveň (zjistí porovnáním vysílaného a přijímaného signálu), dojde ke **kolizi** – signály se „smíchají“
- 3 první stanice, která kolizi detekuje, vyšle tzv. **signál JAM** – posilující „smíchaný“ signál, kvůli detekci kolize ostatními stanicemi)
- 4 všechny stanice se na náhodný čas odmlčí – interval času je odvozený od MAC adresy a v iteracích se zdvojnásobuje (od desítek μ s, max. 16 pokusů) = **backoff algoritmus**

= **stochastická, nedeterministická metoda** přístupu ke sdílenému médiu

- více stanic, delší vzdálenosti mezi nimi, větší provoz = více kolizí, nejlepší využití a tedy propustnost sítě kolem 20 % (limit 40 %) (u FDDI 80-90 %), teoretické max. 30 stanic na segmentu
- propojení počítače s opakovačem/mostem nebo přímo dvou počítačů nebo opakovačů/mostů (= linkový segment, např. kroucenou dvojlinkou do podporované vzdálenosti) = **bezkolizní segment**

- místo opakovače propojuje (linkové) segmenty přímo most \Rightarrow kolize pouze v rámci segmentů, oddělení tzv. **kolizních domén**
- **normy IEEE 802.1d a 802.1q**

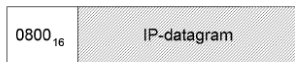
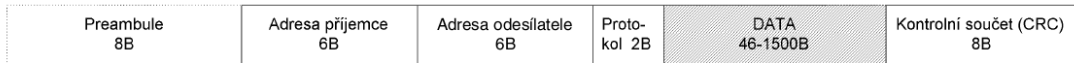
Přepínač (Switch)

- = **multiportový most**, který zpracovává příchozí rámce na svých rozhraních současně, vytváří souběžné **virtuální linkové segmenty** (dvobodové plně duplexní spoje) propojující odesílatele s adresátem = **přepínání** přenosů dat
- virtuální linkový segment je bezkolizní, **kolize** nastávají (na portu přepínače) pouze pro segmenty s různými odesílateli, ale stejným adresátem
- pro přepínání používá HW **přepínací matici**, dokáže propojit sítě s různými rychlostmi (má vyrovnávací paměť, metoda **store-and-forward**) nebo může rámec přepnout hned po načtení záhlaví (metoda **cut-through**)

Ethernet II

Obrázek: Obrázek průvodce 111

- předepsaný pro lokální sítě přímo připojené do Internetu
- rámec: preamble pro synchronizaci hodin uzlů přijímajících rámec s vysílajícím uzlem (fyzická vrstva, $(31 \times 10)11$), adresy příjemce a odesílatele, specifikace protokolu vyšší (síťové) vrstvy, data 46–1500 B a kontrolní součet v zápatí
- **linkové (MAC) adresy**: globální (druhý bit = 0, první tři bajty identifikují výrobce, v trvalé paměti síťové karty), skupinová (nejnižší bit prvního bytu = 1), všesměrová (samé 1)

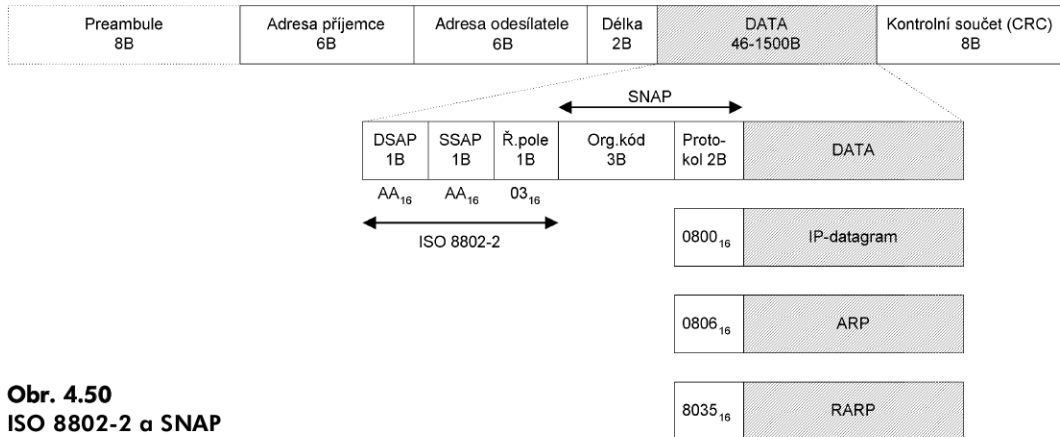


Obr. 4.47
Ethernet II

Ethernet IEEE 802.3

Obrázek: Obrázek průvodce 125

- rámec stejný jako u Ethernetu II, jen místo specifikace protokolu vyšší vrstvy je délka dat (max. 1500 B, čísla protokolů jsou vyšší)
- data nesou rámec podvrstvy **LLC** (802.2) se SNAP
- **SNAP (Sub-Network Access Protocol)** = specifikace protokolu vyšší vrstvy – kód organizace přidělující čísla a číslo protokolu (např. IP má 0x800, pro kód = 0 čísla stejná jako u Ethernet II, viz RFC 1700)



Obr. 4.50
ISO 8802-2 a SNAP

- podvrstvy LLC a MAC jako u IEEE sítí
- rámce **Token** a datový: typ, MAC adresa 2/6 B, kontrolní součet, stav (indikátor tokenu), max. 4500 B
- přístupová metoda **Token Passing**: deterministická, odevzdávání práva (tokenu) pro vysílání na sdíleném médiu po daný čas po kruhu (podobně jako u technologie Token Ring)
- mosty pro připojení jiných technologií LAN (Ethernet/FDDI, Token Ring/FDDI)

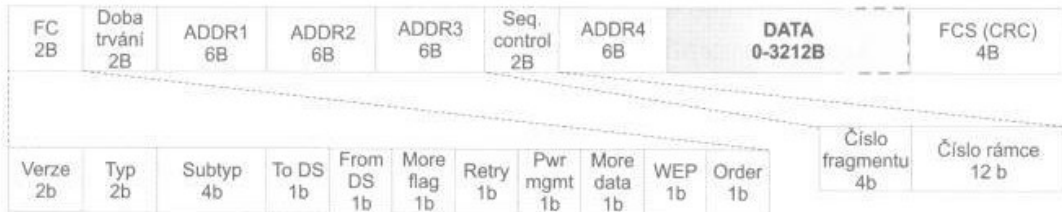
Protokol CSMA/CA (CSMA/Collision Avoidance)

- = kolizní přístupová metoda ke sdíleném bezdrátovému médiu
 - nelze detekovat kolize jako u CSMA/CD – problém „skryté“ stanice = komunikující stanice v dosahu jiné společné (AP), ale ne navzájem
 - podobně jako o CSMA/CD stanice naslouchá a když nevysílá žádná jiná, vyšle signál oznamující, že bude po určitý čas vysílat (čas určený např. AP nebo cílovou stanicí)
 - při kolizi těchto signálů od více stanic se stanice na náhodný čas odmlčí, v iteracích zdvojnásobovaný – backoff algoritmus
 - pokud nedojde ke kolizi, stanice začne vysílat datové rámce
 - příjemce potvrzuje přijetí rámců odesláním potvrzovacím rámců
 - při neobdržení potvrzovacích rámců se vysílání rámců opakuje
- = **stochastická, nedeterministická metoda** přístupu ke sdílenému médiu, jako u Ethernetu

Obrázek: Obrázek průvodce 116

Rámce

- záhlaví rádia (fyzická vrstva): např. WEP bit, přenosová rychlost, info o kanálu, parametry signálu
- obecný formát – až 4 linkové adresy, většinou 1 až 3, pole a příznaky v řídicím poli (FC): typ a subtyp rámce, rámec do/z distribučního systému (podle toho význam adres), více fragmentů, opakovaný rámec, zabezpečení WEP aj., dále doba platnosti rámce, číslo fragmentu a rámce, data až 2312 B a 4B CRC



DODELAT

Rámce

- 1 ovládací – řízení komunikace v rámci BSS (CSMA/CA), bez dat
 - 2 řídicí: v datové části řídicí (management) info, např. pro autentizaci a asociaci (probe, beacon, autentizační, asociační rámce)
 - 3 datové: v datové části záhlaví 802.2 a data
- pro zachytávání potřeba podpora v SW, jinak jen rámce Ethernetu

Adresy

- 6B MAC jako u Ethernetu
- druhy: odesílatele (SA) a příjemce (DA), vysílající (TA) a přijímající (RA) stanice, BSS ID („adresa bezdrátového média“) – typicky MAC adresa AP

Bezpečnost

- obtížná ochrana proti odposlechu na fyzické vrstvě
- **autentizace** (802.11) = prokázání identity protějščí stanici (AP), otevřená (bez) nebo na základě sdíleného hesla (pre-shared key, PSK)
- **asociace** = přiřazení stanice k AP, v rámci roamingu reasociace, potřeba **SSID (Service Set ID)** = označení AP ("jméno sítě"), AP jej nemusí vysílat (v majákových rámcích)
- **WEP (Wired Equivalent Privacy)**: autentizace 40bitovým sdíleným tajemstvím (heslo spolu s MAC adresou), symetrické šifrování přenosu (64bitový nebo 128bitový klíč, z toho 24bitů inicializační vektor měnící se s každým rámcem, proudová šifra RC4) – lze v krátkém čase zlomit = **nedostatečné**
- IEEE 802.1x: autentizace uživatele EAP oproti např. RADIUS serveru
- **WPA (Wi-Fi Protected Access)**, **WPA2**: autentizace (heslo = PSK, EAP), tvorba klíčů TKIP, silná šifra AES (WPA2)

Bluetooth [LAN]



DODELAT

VLAN (Virtual Bridged LAN)

= virtuální síť vytvořená ve fyzické (přepínané) síti

- zpočátku jen proprietární, pak **norma IEEE 802.1q**
- přiřazení uzlů do VLAN pomocí **přístupových tabulek** na přepínačích, na základě portů, MAC adres nebo protokolu vyšší vrstvy – protokol GVRP
- identifikace VLAN pomocí čísla **VLAN ID** (1 až 2048), filtrační tabulka přepínače obsahuje pro každý port přístupovou tabulku s povolenými VLANy, rozšířená filtrační pravidla, priority
- **802.1q tagging**: rozšíření záhlaví linkového rámce (např. Ethernetu) o 4 byty pro prioritu a VLAN ID

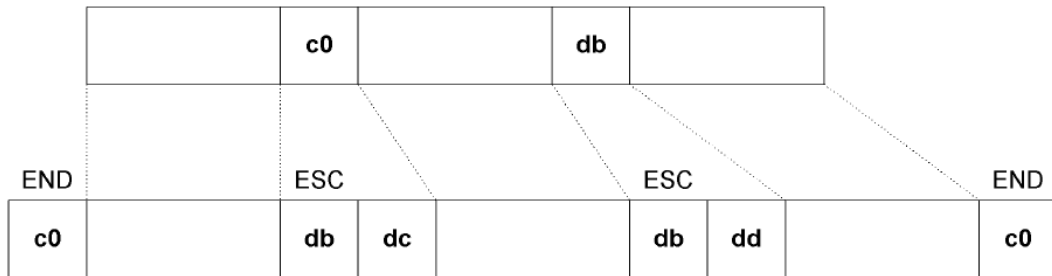
(Compressed) Serial Line IP (RFC 1055, RFC 1144)

- velice jednoduchý, vkládá síťové pakety přímo do asynchronní sériové linky

Obrázek: Obrázek průvodce 75

- pro synchronizaci značka END (0xC0) na (začátku a) konci rámce, tento znak v datech nahrazen tzv. **Esc-sekvencí** (0xDB 0xDC, 0xDB nahrazen 0xDB 0xDD)
- nezabezpečuje detekci chyb, nenese info o přenášeném síťovém protokolu – může být jen jeden, nelze dohodnout konfigurační parametry, aj.
- varianta s kompresí (CSLIP):
 - **redukce záhlaví** protokolů IP a TCP (40 bytů) na 3 až 16 bytů, nově lze použít i pro UDP a IPv6
 - pouze vynechání neměnných položek záhlaví protokolu nebo uvádění malých změn (komprimovatelný paket) v sérii paketů

IP-datagram



- více ISO norem, původně IBM SDLC, rozsáhlý protokol, využívají jej (jeho část) nebo jsou z něj odvozeny další protokoly (např. PPP, LAPB a LAPD u ISDN)
- synchronní i asynchronní přenos, detekce chyb (kontrolní součet, negativní potvrzování), řízení toku dat, možnost více síťových protokolů, stavy linky (odpojená, nastavování, přenos dat, odpojování)
- módy ABM (plně duplexní dvoubodový přenos), NRM (SDLC, poloduplexní přenos), typy rámců **I** (přenos dat), **U** (i řídicí funkce) a **S** (řízení toku), specifikované v řídicím poli

Obrázek: Obrázek průvodce 77

- značka 0x7E, **bit stuffing** (v bitovém synchronním proudu za každých 5 jedniček nula), adresa 1 byte

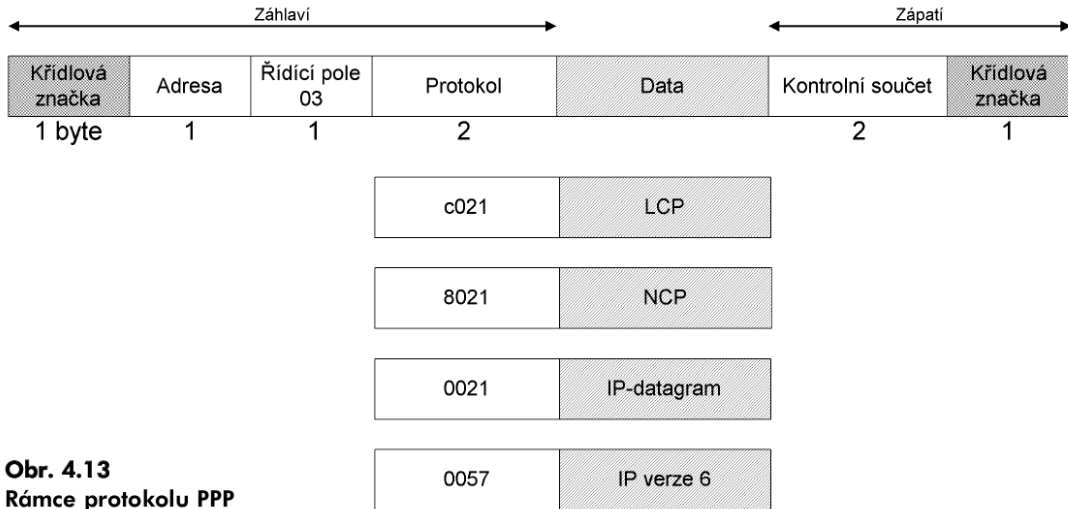


Point to Point Protocol (RFC 1661)

- využití pro připojení k datové síti (Internetu) pomocí telefonní sítě, virtuálních sítí aj.
- využívá rámce (je “zapouzřován” rámci) HDLC (u analogových telefonních linek), Ethernet (**PPPoE, PPP over Ethernet**, u ADSL), nebo i FrameRelay
- vyžaduje plně duplexní dvojbodový spoj

Obrázek: Obrázek průvodce 83

- HDLC adresa 0xFF (všesměrová), značka pro asynchronní přenos 0x7E + Esc-sekvence (0x7D 0x5E, 0x7D 0x5D, i řídicí znaky ASCII)
- **služební (pod)protokoly** pro navázání spojení, autentizaci, skupina protokolů NCP pro síťové protokoly aj. (šifrování, komprese)



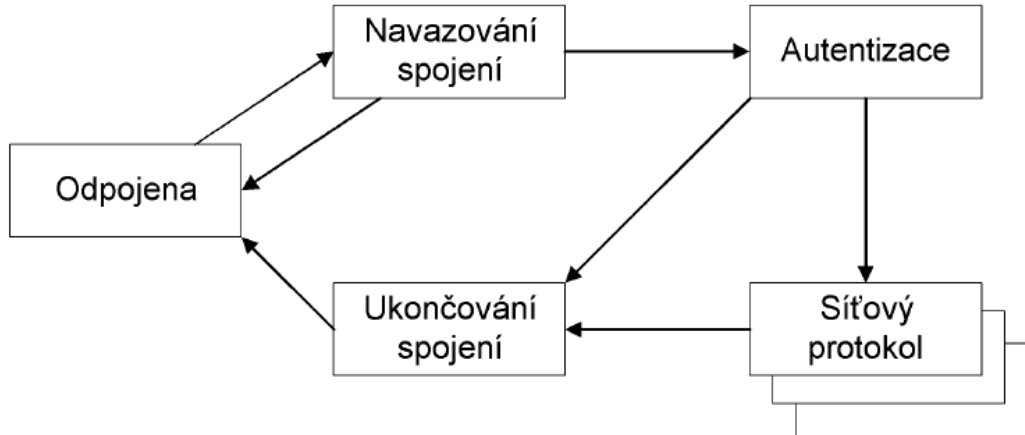
Obr. 4.13
Rámce protokolu PPP

Protokol LCP

- protokol pro navázání a ukončení spojení, dohoda na autentizaci apod.
- linka ve **fázích** odpojena, navazování spojení, autentizace (nepovinná, i oboustranně), případné zpětné volání (s případnou kontrolou klientova tel. čísla), další protokoly (šifrování – ECP, MPPE, komprimace – CCP, MPPE, rozložení do více linek – MP, BAP, BACP aj.), síťový protokol (otevření linky pomocí odpovídajícího protokolu NCP), ukončování spojení (signalizace fyzické vrstvě)

Obrázek: Obrázek průvodce 85

- rámec: kód příkazu/odpovědi (konfigurace, ukončení spojení, atd.), volby (jaká délka rámce, autentizační protokol, atd.)



Autentizace

- terminálový dialog nebo autentizační protokoly
- **PAP (Password Authentication Protocol)** – příkaz se jménem a heslem, RFC 1334
- **CHAP (Challenge Handshake AP)** – RFC 1994
 - sdílené tajemství (heslo), autentizující strana zašle náhodný řetězec (příkaz **challenge**), autentizovaná strana spočte hash (např. MD5) z tajemství a řetězce a pošle zpět (**response**), první strana stejně spočte hash a porovná
 - varianty MS CHAP 1 a 2 – uložen hash (MD4) hesla (1), navíc šifrování dat (2), RFC 2433, 2759
- **EAP** – autentizace později (v rámci vlastního datového přenosu) libovolným autentizačním protokolem nebo mechanismem (EAP-MD5 – obdoba CHAP, EAP-TLS), RFC 2284

Protokol IPCP

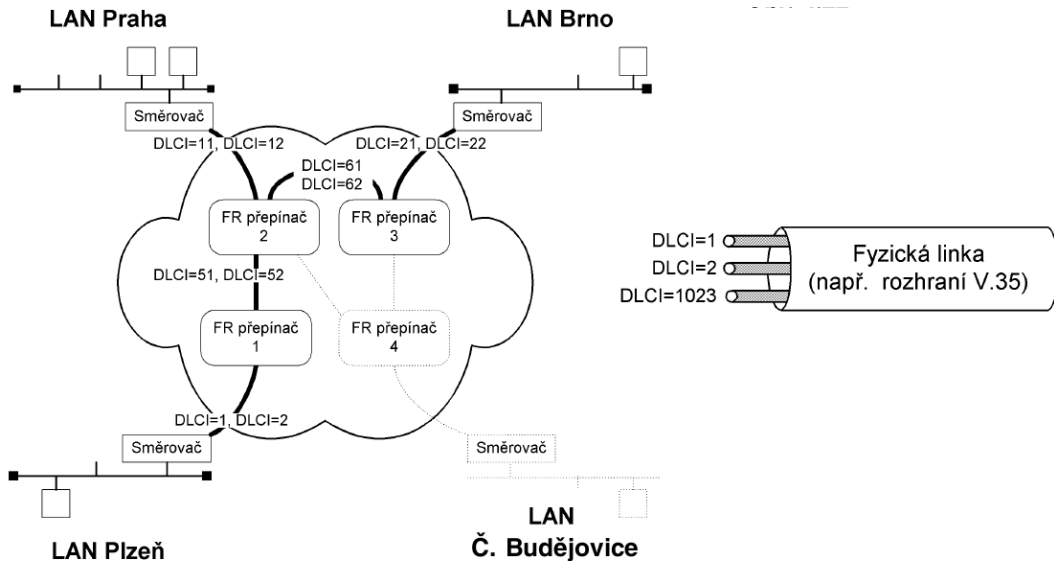
- řídicí protokol typu NCP pro otevření linky pro síťový protokol IP (v4), RFC 1332
- příkazy podobné LCP, volby pro IP adresu, adresy DNS serverů apod.

- datagramový, nespojovaný, “nespolehlivý” protokol

Obrázek: Obrázek průvodce 106

- využívá (zejména) pevné **virtuální okruhy poskytovatele** (privátní síť) – parametry množství dat, které lze síti předat za sekundu, a povolené překročení
- připojení směrovače na Frame Relay přepínač, na fyzické vrstvě rozhraní V.35, X.21, rychlosti od 56 kb/s do 100 Mb/s
- rámec: záhlaví s identifikátorem **DLCI okruhu**, bity indikující možnost zahození, blíží se zahlcení okruhu (řeší se zvýšením doby odezvy, na vyšším protoloku snížením rychlosti) aj., data a kontrolní součet
- identifikace síťového protokolu (pole NLPID rámce): **Multiprotocol over FR** (RFC 2427) – např. IP (0xCC) nebo PPP
- **Protokol LMI (Local Management Interface)**: statistiky, účtování, informace o připojení rozhraní apod.

Frame Relay [WAN]



- zápatí rámce obsahuje **kontrolní součet**, který příjemce spočítá z přijatých dat a porovná – ochrana (jen) proti rušení
- na **LAN** nebo pevných linkách (např. telefonních) se útoky **neřeší**, uživatelé jsou v pracovně-právním vztahu
- na LAN promiskuitní režim síťové karty, útoky **podvrhnutím adresy** odesilatele (např. nastavením MAC adresy), podvrhnutím položky ARP cache (ARP spoofing a.k.a. **ARP cache poisoning**, viz protokol ARP)
- na **WAN**, komutovaných linkách, např. s protokolem PPP, nebo **WLAN autentizace**, zabezpečení přenosu (**šifrování**) apod.
- **Access Port Control (IEEE 802.1x)**: autentizace a autorizace přístupu prvku (typicky počítač) k síti (přepínači, AP, serveru) pomocí autentizační autority (např. RADIUS server), na základě portů, linkových adres nebo asociace k AP (u WLAN), **protokol EAP** na speciální skupinové adrese