Počítačové sítě

přednášky

Jan Outrata

říjen–prosinec 2010 (aktualizace září–prosinec 2013)

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

Technologie linkové vrstvy

Propojování sítí IEEE 802 [LAN]

- 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 **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.

Podvrstva LLC, norma IEEE 802.2 [LAN]

- řešena HW i SW, nezávislá na HW (fyzickém řešení sítě), rozhraní mezi podvrstvami MAC a LLC $\sim$ 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 121→125(5)

Most (Bridge) [LAN]

- **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 (síť 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 blokovaných portů
- parametry: velikost filtrační tabulky, filtrační výkon (načtené rámce/s, přenosový výkon (zopakované rámce/s)

Most (Bridge) [LAN]

Algoritmus TRA (Transport Roading Algorithm)

- naplněn, aktualizace a použití filtrační tabulky

→ pokud adresa adresáta rámce není v tabulce, pracuje jako opakovač, ale pro nevšeobecné adresy navíc uloží do tabulky adresu odesílatele rámce vs. port, kterým rámec přišel = **learning**

→ pokud v tabulce je adresa adresáta rámce a pokud je asociovaný port jiný než port asociovaný s adresou odesílatele a není blokovaný, zopakuje rámec jen na port asociovaný s adresou adresáta = **forwarding**, jinak jej nezopakuje = **filtering**

- omezení na stromovou topologii sítě s více mosty (jinak cyklický oběh rámců!)

Most (Bridge) [LAN]

Protokol a Algoritmus výběru kostry (STA, Spanning Tree Algorithm)

- výpočet **stromové topologie sítě** s potlačením smyček v libovolné topologii

→ mosty identifikovány prioritou a MAC adresou, zvolen **kořenový most** (s nejnižším id), všechny ostatní mosty si označí jako **kořenový/root port** ten port, kterým vede nejlevnější (nejkratší) cesta ke kořenovému mostu (při stejných přes souseda s nejnižším id), z mostů na stejném segmentu se vybere ten s nejlevnější cestou (a nejnižším id) a jeho port do segmentu je označen (**designated port**), ostatní porty 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 STP multicast MAC adrese

Most (Bridge) [LAN]

Protokol a Algoritmus výběru kostry (STA, Spanning Tree Algorithm)

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

Ethernet [LAN]

IEEE 802.3

- 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) Duplex
- 10Gigabitový Ethernet již nepoužívá sdílené médium (režim Full Duplex)

Ethernet [LAN]

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

→ **kolizní přístup** ke sdílenému médiu: stanice naslouchá (Carrier) a vysílá, až když nevysílá žádná jiná (tj. společné médium není používáno), když takto začne vysílat více stanic zároveň (zjistí porovnáním vysílaného a přijímaného signálu), dojde ke **kolizi**, první stanice, která ji detekuje, vyšle tzv. **signál JAM** (kvůli detekci kolize ostatními stanicemi) a všechny se na náhodný čas odmlčí (interval času odvozený od MAC adresy se v iteracích zdvojnásobuje, desítky μs, max. 16 pokusů)

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

- 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 dvou počítačů (linkovým segmentem, např. kroucenou dvojlinkou) = **bezkolizní segment**

Přepínaný Ethernet [LAN]

- místo opakovače propojuje (linkové) segmenty přímo most
- **normy IEEE 802.1d** a **802.1q**

Přepínač (Switch)

= **multiportový most**, který zpracovává příchozí rámce na svých rozhraních "paralelně", vytváří "souběžné" **virtuální linkové segmenty** (dvobodové plně duplexní spoje) propojující odesílatele s adresátem . . . **přepínání** přenosů dat

- virtualní linkový segment je bezkolizní, **kolize** nastávají pouze pro segmenty s různými odesílateli, ale stejným adresátem
- pro přepínání používá **přepínací matici**, dokáže propojit sítě obecně s různými rychlostmi (má vyrovnávací paměť, store-and-forward) a může hned po načtení záhlaví rámce načítat další rámec (cut-through)

Ethernet [LAN]

Ethernet II

Obrázek: Obrázek průvodce 116→111(5)

- předepsaný pro lokální sítě přímo připojené do Internetu
- rámec: preambule pro synchronizaci hodin uzlů přijímajících rámec s vysílajícím uzlem (fyzická vrstva, (31× 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)

Ethernet [LAN]

Ethernet IEEE 802.3

Obrázek: Obrázek průvodce 118→125(5)

- rámec stejný jako u Ethernetu II, jen místo specifikace protokolu vyšší vrstvy je délka dat (max. 1500 B, čísla protokolů jsou vyšší)
- linkové (MAC) adresy mohou mít délku 2 až 6 B
- 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)

FDDI [LAN]

- 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) přístupu ke sdílenému médiu po kruhu (podobně jako u technologie Token Ring)
- mosty pro připojení jiných technologií LAN (Ethernet/FDDI, Token Ring/FDDI)

Wi-Fi [LAN]

DODELAT

Protokol CSMA/CA (CSMA/Collision Avoidance)

= přístupová metoda ke sdíleném bezdrátovému médiu

- nelze detekovat kolize jako u CSMA/CD, používá se **pozitivní potvrzování s vyhrazením pásma na určitý čas**
- asociace = „(znovu)přihlašování“ se k přístupovému bodu (AP)

Wi-Fi [LAN]

DODELAT

Bezpečnost

- obtížná ochrana proti odposlechu na fyzické vrstvě
- **SSID (Service Set ID)**: označení AP ("jméno sítě"), AP jej nemusí vysílat
- **WEP (Wired Equivalent Privacy)**: autentizace stanic vůči AP (40bitové sdílené tajemství = **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 (EAP) oproti např. RADIUS serveru
- **WPA (Wi-Fi Protected Access)**, **WPA2**: autentizace (heslo, EAP), tvorba klíčů TKIP, silná šifra AES (WPA2)

Bluetooth [LAN]

DODELAT

VLAN sítě [LAN]

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

(C)SLIP [WAN]

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

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

Obrázek: Obrázek průvodce 67→75(5)

- pro sychronizaci 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

HDLC [WAN]

- 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, polo-duplexní přenos), typy rámců **I** (přenos dat), **U** (i řídící funkce) a **S** (řízení toku), specifikované v řídícím poli

Obrázek: Obrázek průvodce 73→77(5)

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

PPP [WAN]

Point to Point Protocol (RFC 1661)

- využití pro připojení k datové síti (Internetu) pomocí telefonní sítě, virtuálních sítích 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 78→83(5)

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

PPP [WAN]

Protokol LCP

- protokol pro navázání a ukončení spojení, dohodě 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, MPPC, rozložení do více linek – MP, BAP, BACP aj.), síťový protokol (otevření linky pomocí odpovídajícího protokolu NCP), ukončování spojení (signalizace fyzické vrstvě)

Obrázek: Obrázek průvodce 82→85(5)

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

PPP [WAN]

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 mechanizmem (EAP-MD5 – obdoba CHAP, EAP-TLS), RFC 2284

PPP [WAN]

Protokol IPCP

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

Frame Relay [WAN]

- datagramový, nespojovaný, "nespolehlivý" protokol

Obrázek: Obrázek průvodce 102→106(5)

- 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, blížící 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.

Bezpečnost protokolů linkové vrstvy

- 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 apod.
- **Access Port Control (IEEE 802.1x)**: autentizace a autorizace přístupu prvku (uzel nebo i přepínač) k síti (přepínači, serveru) pomocí autorizační autority (např. RADIUS server), **protokol EAP** na speciální skupinové adrese, na základě portů, linkových adres nebo asociace (u WLAN)