Počítačové sítě 2

Jan Outrata

KATEDRA INFORMATIKY
UNIVERZITA PALACKÉHO V OLOMOUCI

přednášky

Obsah

Anotace

Předmět navazuje na předmět Počítačové sítě 1, rozšiřuje zde nabyté znalosti a seznamuje studenty s pokročilejšími tématy fungování počítačových sítí a Internetu.
Obsah předmětu zahrnuje další vybrané síťové technologie, novější protokoly a pokročilejší záležitosti fungování počítačových sítí (Internetu) jako např. bezdrátové sítě (Wi-Fi, mobilní), protokoly IPv6 a HTTPv2, směrovací protokoly nebo technologie DNSSec. Na cvičeních se studenti prakticky seznámí s dalšími síťovými zařízeními, analyzováním provozu a konfigurací sítě v operačních systémech Microsoft Windows a GNU/Linux a prací s dalšími aplikačními službami.

Literatura

- [KR] Kurose J. F., Ross K. W.: *Computer Networking: A Top-Down Approach*, 7th Edition. Pearson, 2017.
- Kurose J. F., Ross K. W.: *Počítačové sítě*. Computer Press, 2014.
- [TFW] Tanenbaum A. S., Feamster N., Wetherall D.: *Computer Networks*, 6th edition. Pearson, 2021.
- Forouzan B.: *TCP/IP Protocol Suite*. McGraw-Hill Science/Engineering/Math, 2009.
- [PS] Satrapa P.: *IPv6 - čtvrté vydání*. Edice CZ.NIC, 2019.
- Peterson L. L., Davie B. S.: *Computer Networks: A Systems Approach*, 6th edition. Morgan Kaufmann, 2022.

Bezdrátové sítě (Wireless networks)

Úvod

- za posledních 30 let **mobilní sítě** – telefon + SMS (1G, 2G), připojení k Internetu (3G), aplikace (4G/LTE), „smart“ (5G) $\sim$ počítač

Úvod

- za posledních 30 let **mobilní sítě** – telefon + SMS (1G, 2G), připojení k Internetu (3G), aplikace (4G/LTE), „smart“ (5G) $\sim$ počítač
- za posledních 20 let **bezdrátová LAN (Wi-Fi)** – (původně) vnitřní i vnější použití: počítače, spotřební elektronika, domácí spotřebiče / připojení k Internetu, hotspot

Úvod

- za posledních 30 let **mobilní sítě** – telefon + SMS (1G, 2G), připojení k Internetu (3G), aplikace (4G/LTE), „smart“ (5G) $\sim$ počítač
- za posledních 20 let **bezdrátová LAN (Wi-Fi)** – (původně) vnitřní i vnější použití: počítače, spotřební elektronika, domácí spotřebiče / připojení k Internetu, hotspot
  - \+ **bezdrátová PAN (Bluetooth)** – bezdrátové propojení (mobilních) zařízení „všeho druhu“ (počítače, spotřební elektronika, periferie)

Úvod

- za posledních 30 let **mobilní sítě** – telefon + SMS (1G, 2G), připojení k Internetu (3G), aplikace (4G/LTE), „smart“ (5G) $\sim$ počítač
- za posledních 20 let **bezdrátová LAN (Wi-Fi)** – (původně) vnitřní i vnější použití: počítače, spotřební elektronika, domácí spotřebiče / připojení k Internetu, hotspot
  + **bezdrátová PAN (Bluetooth)** – bezdrátové propojení (mobilních) zařízení „všeho druhu“ (počítače, spotřební elektronika, periferie)
  + **„bezkontaktní“ sítě/technologie (RFID/NFC)** – prezence, identifikace (platby) aj., „čipy“

Úvod

- za posledních 30 let **mobilní sítě** – telefon + SMS (1G, 2G), připojení k Internetu (3G), aplikace (4G/LTE), „smart“ (5G) $\sim$ počítač
- za posledních 20 let **bezdrátová LAN (Wi-Fi)** – (původně) vnitřní i vnější použití: počítače, spotřební elektronika, domácí spotřebiče / připojení k Internetu, hotspot
  + **bezdrátová PAN (Bluetooth)** – bezdrátové propojení (mobilních) zařízení „všeho druhu“ (počítače, spotřební elektronika, periferie)
  + **„bezkontaktní“ sítě/technologie (RFID/NFC)** – prezence, identifikace (platby) aj., „čipy“
  + **senzorové sítě** – vestavěná zařízení (senzory) pro sběr dat o okolí

Úvod

- za posledních 30 let **mobilní sítě** – telefon + SMS (1G, 2G), připojení k Internetu (3G), aplikace (4G/LTE), „smart“ (5G) $\sim$ počítač
- za posledních 20 let **bezdrátová LAN (Wi-Fi)** – (původně) vnitřní i vnější použití: počítače, spotřební elektronika, domácí spotřebiče / připojení k Internetu, hotspot
  + **bezdrátová PAN (Bluetooth)** – bezdrátové propojení (mobilních) zařízení „všeho druhu“ (počítače, spotřební elektronika, periferie)
  + **„bezkontaktní“ sítě/technologie (RFID/NFC)** – prezence, identifikace (platby) aj., „čipy“
  + **senzorové sítě** – vestavěná zařízení (senzory) pro sběr dat o okolí
  ?

Úvod

- za posledních 30 let **mobilní sítě** – telefon + SMS (1G, 2G), připojení k Internetu (3G), aplikace (4G/LTE), „smart“ (5G) $\sim$ počítač
- za posledních 20 let **bezdrátová LAN (Wi-Fi)** – (původně) vnitřní i vnější použití: počítače, spotřební elektronika, domácí spotřebiče / připojení k Internetu, hotspot
  + **bezdrátová PAN (Bluetooth)** – bezdrátové propojení (mobilních) zařízení „všeho druhu“ (počítače, spotřební elektronika, periferie)
  + **„bezkontaktní“ sítě/technologie (RFID/NFC)** – prezence, identifikace (platby) aj., „čipy“
  + **senzorové sítě** – vestavěná zařízení (senzory) pro sběr dat o okolí
  ?
- osobní přenosná a vniřní domácí zařízení, venkovní infrastruktura, auta („mobilní kancelář“), „věci“ (IoT)...s bezdrátovým připojením k Internetu (Wi-Fi, mobilní)

Úvod

- za posledních 30 let **mobilní sítě** – telefon + SMS (1G, 2G), připojení k Internetu (3G), aplikace (4G/LTE), „smart“ (5G) $\sim$ počítač
- za posledních 20 let **bezdrátová LAN (Wi-Fi)** – (původně) vnitřní i vnější použití: počítače, spotřební elektronika, domácí spotřebiče / připojení k Internetu, hotspot
  - \+ **bezdrátová PAN (Bluetooth)** – bezdrátové propojení (mobilních) zařízení „všeho druhu“ (počítače, spotřební elektronika, periferie)
  - \+ **„bezkontaktní“ sítě/technologie (RFID/NFC)** – prezence, identifikace (platby) aj., „čipy“
  - \+ **senzorové sítě** – vestavěná zařízení (senzory) pro sběr dat o okolí
  - ?
- osobní přenosná a vniřní domácí zařízení, venkovní infrastruktura, auta („mobilní kancelář“), „věci“ (IoT)...s bezdrátovým připojením k Internetu (Wi-Fi, mobilní)
- jiné problémy než drátové sítě, *bezdrátovost vs. mobilita*

Architektura

- uzly = **stanice** bezdrátově připojené k **base station** a/nebo mezi sebou
- **base station**
  - řízení komunikace připojených = **asociovaných** stanic, typicky komunikace stanic pouze s base station
  - přepínač + most: volitelně připojený do ostatní (typicky drátové) sítě = **infrastruktury** a zprostředkovávající ji stanicím – **infrastrukturní režim**
  - např. access point (AP, Wi-Fi), BTS (mobilní sítě)
- **ad hoc režim**: komunikace stanic přímo mezi sebou (včetně point-to-point), typicky bez base station

\+ problémy komunikace (přímá/nepřímá), s mobilitou stanic aj.

Příklady

- **Wi-Fi (IEEE 802.11)**, WiMAX (802.16) – (W)LAN/MAN, jednotky Mb/s až Gb/s, desítky m až jednotky km
- **mobilní** – WAN, jednotky kb/s až stovky Mb/s, stovky m až desítky km
- **Bluetooth (IEEE 802.15.1)** – PAN, stovky kb/s až jednotky Mb/s, jednotky až desítky m
- satelitní – WAN, až stovky Mb/s, stovky až tisíce km

Fyzická vrstva

- přenosové médium elektromagnetické záření (**rádio, mikrovlny**) – výhody i nevýhody
- přenos dat pomocí šíření signálu na dané (nosné) frekvenci, problémy:
  - path fading (loss) = klesající úroveň signálu se vzdáleností a průchody materiály
  - interference signálů a šumu na stejném frekvenčním pásmu
  - multipath propagation = více cest s modifikovaným signálem k příjemci, kvůli odrazům a interferencím
  - horší s vyšší frekvencí a nižší úrovní signálu $\Rightarrow$ více chyb
  - řešení: použití více frekvencí (spread, multiplex) a vysílačů/přijímačů (antén), různé metody modulace bitů do signálu, opakování přenosu, opravné kódy dat aj.

Fyzická vrstva

- přenosové médium elektromagnetické záření (**rádio, mikrovlny**) – výhody i nevýhody
- přenos dat pomocí šíření signálu na dané (nosné) frekvenci, problémy:
  - path fading (loss) = klesající úroveň signálu se vzdáleností a průchody materiály
  - interference signálů a šumu na stejném frekvenčním pásmu
  - multipath propagation = více cest s modifikovaným signálem k příjemci, kvůli odrazům a interferencím
  - horší s vyšší frekvencí a nižší úrovní signálu $\Rightarrow$ více chyb
  - řešení: použití více frekvencí (spread, multiplex) a vysílačů/přijímačů (antén), různé metody modulace bitů do signálu, opakování přenosu, opravné kódy dat aj.

- **signal-to-noise ratio (SNR, S/N)** = poměr úrovně přijímaného (kombinovaného degradovaného) signálu a šumu prostředí, v dB ($= 10 \log_{10} poměr$), úroveň signálu (typicky) v dBm = SNR k 1 mW (šumu)

Obrázek z knihy
zdroj: TFW 2-8

- **signal-to-noise ratio (SNR, S/N)** = poměr úrovně přijímaného (kombinovaného degradovaného) signálu a šumu prostředí, v dB ($= 10 \log_{10} poměr$), úroveň signálu (typicky) v dBm = SNR k 1 mW (šumu)

Obrázek z knihy
zdroj: KR 7.3

- **signal-to-noise ratio (SNR, S/N)** = poměr úrovně přijímaného (kombinovaného degradovaného) signálu a šumu prostředí, v dB ($= 10 \log_{10} poměr$), úroveň signálu (typicky) v dBm = SNR k 1 mW (šumu)

Fyzická vrstva

- **šíření signálu** ve **frekvenčním pásmu (band)** – pásmo jako okruh (circuit):
  - frequency hopping spread spectrum (FHSS): pseudo-náhodné přeskakování v čase mezi více (nosnými) frekvencemi
  - direct sequence spread spectrum (DSSS): současné využívání více (nosných) frekvencí
- **modulace** bitů dat do (analogového) signálu: změna aplitudy (ASK), frekvence (FSK), fáze (PSK) frekvence nebo kombinace (A+P)
- **multiplex** více přenosů (paralelních částí nebo různých stanic) do frekvenčního pásma:
  - frekvenční (FDM): rozdělení (division) na nepřekrývající se (pod)pásma dané šířky pro přenos
  - ortogonální frekvenční (OFDM(A)): mnoho nosných frekvencí (subcarriers) pro přenosy s překrývajícími se (pod)pásmy
  - časový (TDM): disjunktní rozdělení času na (časové) rámce s konstantním počtem slotů pevné délky s daným slotem každého rámce pro přenos
  - kódový (CDM(A)): kódování přenosů v celém pásmu (chipping/XOR bitů vhodným kódem pro přenos a předpoklad součtu, vyšší chipping rate, např. 11x)

Fyzická vrstva

Obrázek z knihy
zdroj: TFW 2-16

Fyzická vrstva

Obrázek z knihy
zdroj: TFW 2-17

Fyzická vrstva

Obrázek z knihy
zdroj: KR 1.14

Fyzická vrstva

Obrázek z knihy
zdroj: TFW 2-20

Fyzická vrstva

Obrázek z knihy
zdroj: KR 7.6

Linková vrstva

- frekvenční (pod)pásmo = broadcast sdílené médium – potřeba **protokol vícenásobného přístupu (vysílání)**

+ řešení **problémů skryté** (hidden) – A i C „vidí“ B, ale ne sebe, **a vystavené stanice** (exposed terminal) – B „vidí“ A a C „vidí“ D, ale i sebe navzájem
+ **zabezpečení přenosu** – šíření signálu „kdekoliv“, příjem „kýmkoliv“, propojení s infrastrukturou → autentizace stanic (vůči base station nebo navzájem) a šifrování přenosu
+ **mobilita stanic** → „předávání“ (handoff) stanic mezi base station nebo sebou

Linková vrstva

Obrázek z knihy
zdroj: TFW 4-11
Obrázek z knihy
zdroj: TFW 4-26

Wi-Fi (IEEE 802.11, Wireless Fidelity)

- IEEE, 1997, Wi-Fi Alliance – certifikace zařízení

= bezdrátová LAN/MAN, (původně) vnitřní i vnější použití: počítače, spotřební elektronika, domácí spotřebiče (desítky až stovky m) / připojení k Internetu, hotspot (až jednotky km), jednotky Mb/s až Gb/s

- několik standardů (rozšíření): až po ax zpětná kompatibilita
  - (legacy)/b/g = Wi-Fi 0/1/3: 1997/1999/2003, 2,4 GHz, až 2/11/54 Mb/s (běžně cca polovina), FHSS/DSSS/OFDM
  - a/ac = 2/5: 1999/2013, 5 GHz, až 54 Mb/s/6,9 Gb/s, OFDM
  - n/ax = 4/6: 2008/2019, 2,4 a 5 GHz, až 0,6/9,6 Gb/s, OFDM
  - ax = 6E: 2020, 6 GHz, až 9,6 Gb/s, OFDMA
  - ad/ay = WiGig: 2012/2021, 60 GHz, až 7/40 Gb/s, OFDM
- bezlicenční pásma (ISM) 2,4–2,4895 GHz, 5,03–5,99 GHz, 57,24–70,20 Ghz (V band)
- licencované pásmo 5,945–7,125 GHz
- infrastrukturní i ad hoc režim

Wi-Fi

Fyzická vrstva

- antény: všesměrové, (sektorové) směrové, různé polarizace signálu, vestavěné i venkovní (VF koax kabel a konektor SMA nebo N)
- MIMO: více vysílacích i přijímacích antén pro vícecestnou komunikaci (dvou účastníků na 1 kanálu, n/ac+ax+ad, 4/8), MU: více účastníků (ac+ax+ay)

Wi-Fi

Fyzická vrstva

- antény: všesměrové, (sektorové) směrové, různé polarizace signálu, vestavěné i venkovní (VF koax kabel a konektor SMA nebo N)
- MIMO: více vysílacích i přijímacích antén pro vícecestnou komunikaci (dvou účastníků na 1 kanálu, n/ac+ax+ad, 4/8), MU: více účastníků (ac+ax+ay)

Architektura (infrastrukturní)

- **basic service set (BSS)** = asociované stanice + případně base station (**access point, AP**), identifikovaná (B)SSID (adresa AP $\neq$ „jméno sítě“!), frekvenční kanál
- **asociace stanice** (k AP): nutná, komunikace jen asociované
  - AP periodicky vysílá majákové (beacon) rámce s (volitelně) „jménem sítě“ a adresou AP (a info k zabezpečení, rychlostem/modulacím aj.)
  - stanice skenuje kanály, pasivně nebo aktivně (vyšle probe request rámec a od AP response), a vybere AP (nestandardizované, typicky s nejvyšším SNR) – association request k AP (nutné „jméno sítě“!) a od něj response
  - volitelně nutná autentizace stanice (jinak otevřená), pak až datové rámce, např. DHCP

Wi-Fi: linková vrstva

CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance)

- CSMA = **náhodný vícenásobný přístup** (multiple access) **k** broadcast sdílenému **médiu** (frekvenčnímu kanálu/pásmu)
  - **čekání na klid** (carrier sense) a vysílání
  - /CD (např. Ethernet) = při detekci kolize (collision detection) náhodná pauza a znovu vysílání – kolize na straně vysílajícího ⇒ nejvýše jedno současné vysílání

Wi-Fi: linková vrstva

CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance)

- CSMA = **náhodný vícenásobný přístup** (multiple access) **k** broadcast sdílenému **médiu** (frekvenčnímu kanálu/pásmu)
  - **čekání na klid** (carrier sense) a vysílání
  - /CD (např. Ethernet) = při detekci kolize (collision detection) náhodná pauza a znovu vysílání – kolize na straně vysílajícího ⇒ nejvýše jedno současné vysílání
- /CA = **předcházení kolizím** (collision avoidance): náročné/nemožné současně přijímat a vysílat → poloduplexní přenos + problém skryté/vystavené stanice ⇒ kolize na straně příjemce!, možno více současných vysílání
- **pozitivní potvrzování** (ACK, příjemcem) a případné znovuzaslání rámce

1. při klidu chvíle čekání (DIFS), jinak náhodná pauza – odpočítávaná při klidu!
2. vyslání celého rámce, příjemce po chvíli od přijetí (SIFS) potvrdí, pokud do určité doby ne, znovu 1. (= iterace), po několika pokusech chyba

Wi-Fi: linková vrstva

Obrázek z knihy
zdroj: KR 7.10

- /CA = **předcházení kolizím** (collision avoidance): náročné/nemožné současně přijímat a vysílat → poloduplexní přenos + problém skryté/vystavené stanice ⇒ kolize na straně příjemce!, možno více současných vysílání
- **pozitivní potvrzování** (ACK, příjemcem) a případné znovuzaslání rámce

1. při klidu chvíle čekání (DIFS), jinak náhodná pauza – odpočítávaná při klidu!
2. vyslání celého rámce, příjemce po chvíli od přijetí (SIFS) potvrdí, pokud do určité doby ne, znovu 1. (= iterace), po několika pokusech chyba

Wi-Fi: linková vrstva

Obrázek z knihy
zdroj: TFW 4-25

- /CA = **předcházení kolizím** (collision avoidance): náročné/nemožné současně přijímat a vysílat → poloduplexní přenos + problém skryté/vystavené stanice ⇒ kolize na straně příjemce!, možno více současných vysílání
- **pozitivní potvrzování** (ACK, příjemcem) a případné znovuzaslání rámce

1. při klidu chvíle čekání (DIFS), jinak náhodná pauza – odpočítávaná při klidu!
2. vyslání celého rámce, příjemce po chvíli od přijetí (SIFS) potvrdí, pokud do určité doby ne, znovu 1. (= iterace), po několika pokusech chyba

Wi-Fi: linková vrstva

Rezervace média

- volitelná pro delší vysílání stanice (ne AP)

1. **žádost** (RTS) AP s časem pro přenos dat a potvrzení (CSMA/CA 1.)
2. AP vyšle všem po chvíli (SIFS) **rezervaci média** (CTS) na čas pro stanici (CSMA/CA 1.)
3. vyslání dat a potvrzení (CSMA/CA 2., po SIFS), ostatní po čas nezkouší vysílat

Wi-Fi: linková vrstva

Obrázek z knihy
zdroj: TFW 4-27

Wi-Fi: linková vrstva

Obrázek z knihy
zdroj: KR 7.12

Wi-Fi: linkový rámec

- data až 2312 B (obvykle do 1500, LLC), CRC32 rámce
- před ním záhlaví fyzické vrstvy (rádia) – modulace (rychlost), frekvenční kanál aj.

Záhlaví

- až 4 **MAC adresy**: 1. přijímající stanice (R), 2. vysílající stanice (T)
  - 3. příjemce (D)/odesílatel (S) v infrastruktuře (nebo v ad hoc režimu): AP = (netransparentní) most = R/T, S/D = T/R, jinak AP (BSSID)
  - 4. $S \neq T$ = AP s D (3.) „u“ jiného k AP bezdrátově připojeného AP (nebo v ad hoc režimu): oba AP mosty = T + R – tzv. **(bezdrátový) distribuční systém ((W)DS)**
- čas „obsazení“ a rezervace média, pořadové číslo rámce (a ID fragmentu)
- řídící pole: verze (00), typ a subtyp pro rozlišení **control** (ACK, RTS, CTS, bez dat), **management** (beacon, probe, association, autentizační) a **datových** rámců, od a do DS pro význam adres (3., 4.), indikace více fragmentů, opakování rámce, power management („spaní“), dalšího rámce, šifrování (dat) rámce

Wi-Fi: linkový rámec

Obrázek z knihy
zdroj: KR 7.13

Wi-Fi: mobilita v LAN

- ve **stejné IP síti** (zachování IP adresy aj.)
- mezi více **BSS se stejným „jménem sítě“** = **extended service set (ESS)** – AP v distribučním systému
- stanice při slábnoucím signálu od AP aktivně skenuje a reasociuje se k silnějšímu (handoff)
- infrastruktura? – např. na přepínači samoučení: rámec od stanice přes nový AP nebo (broadcast) od AP po asociaci se zdrojovou MAC stanice (hack!) nebo (WDS) protokol mezi AP

Wi-Fi: další

Adaptace rychlosti (rate adaptation)

= změna modulace dat do signálu dle SNR

- nestandardizované, např. při dvou rámcích bez potvrzení následující rámce nižší rychlostí, při 10 potvrzených nebo vypršení času od posledního snížení vyšší

Správa energie (power management)

- nestandardizované, minimalizace doby funkce stanice (ne AP), jinak „spí“

1. stanice nastaví power management bit v rámci k AP a spí dokud AP nepošle beacon rámec (má nastavený „budík“ těsně před)
2. AP rámce pro stanici ukládá do bufferu a v beacon rámci pošle seznam stanic, pro které má rámce
3. stanice v seznamu si rámce vyžádá, jinak případně opět spí

- APSD (n): ukládání rámců AP pro stanici a zaslání i po obdržení rámce od stanice, rozvrhování vysílání stanic AP (ax) aj.

Další:

- fragmenty = kratší rámce: nestandardizovaná délka, vysílány za sebou s potvrzením
- prioritizace provozu (QoS, různé IFS, TXOP, 802.11e), omezení vyzářeného výkonu (regionální) aj.

Wi-Fi: zabezpečení

- původní specifikace **WEP** (Wired Equivalent Privacy, 1999) – „průšvih“, dočasné **WPA** (Wi-Fi Protected Access, 2002), pak **WPA2** (802.11i, 2004), **WPA3** (2018)

Autentizace – stanice vůči AP!

- **sdílené heslo (Personal)** – WEP: před asociací, až 4 40/104 b, šifrování a dešifrování náhodné výzvy!, WPA(2/3): generování pre-shared key (PSK) ($\sim$ MK = PMK) z hesla 8 až 63 B a SSID
- **autentizační protokol (Enterprise)** – WPA(2/3), 802.11i: EAP (EAPoL/802.1X, volitelně šifrované, autentizace uživatele), může místo AP řešit **autentizační server** (RADIUS, DIAMETER, šifrované, AP relay pouze s ním), volitelná „předběžná“ k jinému AP (pro handoff, WPA2/3)
  1. dohoda na metodě
  2. (vzájemná) autentizace a vygenerování sdíleného master key (MK)
  3. vytvoření pairwise MK (PMK) z MK a předání AP ze serveru (**distribuce klíče**)

Wi-Fi: zabezpečení

Obrázek z knihy
zdroj: KR 8.32

Wi-Fi: zabezpečení

Šifrování – rámců (dat a CRC) mezi stanicí a AP

- proudová symetrická **šifra RC4** – WEP: klíč sdílené heslo + 24b IV za záhlavím, WPA = TKIP/WEP-fix: 128b klíče vytvářené z IV, pořadového čísla rámce, klíče relace (PTK) vytvořeného z PMK aj. + 64b kód integrity rámce (MIC) za šifrovanými daty
- bloková symetrická **šifra AES (Rijndael)** – WPA2/3 = CCMP: klíče jako u WPA, ale jen z PTK, kód integrity jako u WPA

Wi-Fi: zabezpečení

Šifrování – rámců (dat a CRC) mezi stanicí a AP

- proudová symetrická **šifra RC4** – WEP: klíč sdílené heslo + 24b IV za záhlavím, WPA = TKIP/WEP-fix: 128b klíče vytvářené z IV, pořadového čísla rámce, klíče relace (PTK) vytvořeného z PMK aj. + 64b kód integrity rámce (MIC) za šifrovanými daty
- bloková symetrická **šifra AES (Rijndael)** – WPA2/3 = CCMP: klíče jako u WPA, ale jen z PTK, kód integrity jako u WPA

WPS (Wi-Fi Protected Setup)

- generování a distribuce „jména sítě“ a nastavení zabezpečení (nejvyšší metoda, sdílené heslo) z AP na stanice – PIN od AP stanici (nebo i opačně)

Wi-Fi: zabezpečení

Obrázek z knihy
zdroj: KR 8.30

WPS (Wi-Fi Protected Setup)

- generování a distribuce „jména sítě“ a nastavení zabezpečení (nejvyšší metoda, sdílené heslo) z AP na stanice – PIN od AP stanici (nebo i opačně)

Bluetooth (IEEE 802.15.1)

- Ericsson, 1994, + IBM, Intel, Nokia, Toshiba, 1998

= bezdrátové propojení (PAN) různorodých (mobilních) nízkoenergetických zařízení s malým dosahem (jednotky až desítky m) menší rychlostí (stovky kb/s až jednotky Mb/s): „počítačových“ (vč. mobilu) i „ne-počítačových“, např. periferie počítačů, komunikační aj. spotřební elektronika – „náhrada kabelů“

- verze: 1 (1999), 2 (2004, rychlejší přenosy), 3 (2009, kombinace s Wi-Fi), 4 (2010, nízkoenergetický provoz), 5 (2016, 2x rychlosti, větší dosah, IoT zařízení, lepší zabezpečení), 5.1 (2019)
- 2,4 GHz (pásmo ISM), TDM s FHSS (adaptivní s vyloučením využívaných pásem), 1 Mb/s basic rate, 2/3 Mb/s enhanced rate (od verze 2)

Bluetooth: architektura

- **piconet**: propojená zařízení, až 8 aktivních (komunikujících), ostatních až 255 zaparkovaných (uspaných, nekomunikujících)
  - jedno **master**: řídí komunikaci v piconetu, např. počítač, mobil
  - ostatní **slave**: komunikace jen s master
  - **scatternet**: více propojených piconetů (přes slave v jednom a master v druhém – most), zařízení může být ve více piconetech
- **párování zařízení**: před propojením (vytvořením spoje), PIN nebo heslo od jednoho (i jen potvrzení zobrazeného)
- **profily**: různá použití (aplikace) a protokoly, 20+
  - základní (generic): zjištění služeb, správa spojů (links), výměna dat, emulace sériové linky aj.
  - HID (vstupní periferie), A/V (streaming, headset, hands-free, intercom), přenos souborů (speciálně obrázků), remote control, dial-up (připojení k telefonní síti přes modem), PAN (ad-hoc, připojení k jiné síti, např. Wi-Fi přes AP) aj.
- **vlastní protokolová architektura**: vrstvy radio $\sim$ fyzická, link control (baseband) $\sim$ MAC, link manager (správa spojů a energie, párování, šifrování) a L2CAP (rámce, jejich potvrzování a znovuzasílání, multiplexing pro profily, QoS) $\sim$ LLC, profily využívající L2CAP nebo napříč vrstvami
  - host controller interface: rozhraní mezi Bluetooth čipem a zařízením, mezi link manager a L2CAP

Bluetooth: architektura

Obrázek z knihy
zdroj: TFW 4-31

Bluetooth: linková vrstva

- **spoje (links)**: synchronní spojované (SCO) pro real-time přenosy (A/V, až tři 64kb/s) a asynchronní nespojované (ACL) pro paketové přenosy (souborů, PAN aj., jen jeden)
- CSMA s rezervací média a pozitivním potvrzováním (a znovuzasláním) rámců, bez předcházení kolizím (TDM, sloty)
  - při klidu žádost (RTS) příjemci s časem pro přenos dat a potvrzení
  - příjemce vyšle všem rezervaci (CTS) na čas
  - vyslání dat a potvrzení, ostatní po čas nezkouší vysílat
- linkový rámec: více typů, data až 2744/8184 b basic/enhanced rate, volitelně šifrovaná (klíč vytvořený při spojování)
  - před nimi synchronizace a přístupový kód = ID master zařízení, záhlaví 3x opakovaně:
  - adresa (0 = broadcast), typ (SCO, ACL aj., délka, jaký samoopravný kód), bity flow (slave má plný buffer), ACK a seq (znovuzaslání), CRC-8
  - různé formáty dat dle spoje a rate – i jen např. 13% využití kapacity

Bluetooth: linková vrstva

Obrázek z knihy
zdroj: TFW 4-32

Zigbee (IEEE 802.15.4)

= bezdrátové propojení (PAN) ještě méně-energetických zařízení než Bluetooth, s podobným dosahem (jednotky až desítky m), ale menší rychlostí (desítky až stovky kb/s), např. (domácí) senzory, ovladače spotřebičů apod.

- více režimů (architektur) sítě, zařízení plně funkční ($\sim$ master u Bluetooth, může jich být víc) a redukovaně funkční ($\sim$ slave)
- CSMA/CA ($\sim$ Wi-Fi) i TDM sloty, potvrzování (a znovuzasílání) rámců, střídání aktivních (vysílání) a neaktivních period (spaní) aj.

Network Address Translation (NAT)

Úvod

- pro (tzv. koncovou, přímou) komunikaci v IP síti, např. Internetu, potřebuje zařízení **IP adresu** – unikátní v celé síti
  - IPv4: omezený počet přidělených adres pro místní síť (LAN/MAN) od poskytovatele připojení k Internetu (ISP), vyčerpaný omezený celkový adresní prostor
  - částečné řešení: dynamické adresy jen pro aktuálně připojená odpojovaná zařízení – např. v mobilních sítích, v LAN DHCP
  - (trvalé?) řešení: IPv6 – „neomezený“ adresní prostor, ale pomalý přechod z IPv4
  - „trvalé“ „řešení“?!: **Network Address Translation (NAT)**

Úvod

- pro (tzv. koncovou, přímou) komunikaci v IP síti, např. Internetu, potřebuje zařízení **IP adresu** – unikátní v celé síti
  - IPv4: omezený počet přidělených adres pro místní síť (LAN/MAN) od poskytovatele připojení k Internetu (ISP), vyčerpaný omezený celkový adresní prostor
  - částečné řešení: dynamické adresy jen pro aktuálně připojená odpojovaná zařízení – např. v mobilních sítích, v LAN DHCP
  - (trvalé?) řešení: IPv6 – „neomezený“ adresní prostor, ale pomalý přechod z IPv4
  - „trvalé“ „řešení“?!: **Network Address Translation (NAT)**

= **překlad IP adres** = přepisování v IP paketech libovolných adres v LAN na přidělené adresy v síti ISP a opačně – **basic (one-to-one) NAT**, mnoho RFC

- původně pro odstranění potřeby změny adres při změně (sítě) ISP
- téměř výhradně pro IPv4 (ale pro IPv6 experimentální Network Prefix Translation, NPTv6)

Úvod

- pro (tzv. koncovou, přímou) komunikaci v IP síti, např. Internetu, potřebuje zařízení **IP adresu** – unikátní v celé síti
  - IPv4: omezený počet přidělených adres pro místní síť (LAN/MAN) od poskytovatele připojení k Internetu (ISP), vyčerpaný omezený celkový adresní prostor
  - částečné řešení: dynamické adresy jen pro aktuálně připojená odpojovaná zařízení – např. v mobilních sítích, v LAN DHCP
  - (trvalé?) řešení: IPv6 – „neomezený“ adresní prostor, ale pomalý přechod z IPv4
  - „trvalé“ „řešení“?!: **Network Address Translation (NAT)**

= **překlad IP adres** = přepisování v IP paketech libovolných adres v LAN na přidělené adresy v síti ISP a opačně – **basic (one-to-one) NAT**, mnoho RFC

- původně pro odstranění potřeby změny adres při změně (sítě) ISP
- téměř výhradně pro IPv4 (ale pro IPv6 experimentální Network Prefix Translation, NPTv6)

- pro LAN vyhrazené **rozsahy IPv4 adres pro privátní sítě** (RFC 1918): 10./8, 172.16./12, 192.168./16 – pakety s nimi se nesměrují, „platné“ pouze v LAN, tzv. **privátní**

Úvod

- pro (tzv. koncovou, přímou) komunikaci v IP síti, např. Internetu, potřebuje zařízení **IP adresu** – unikátní v celé síti
  - IPv4: omezený počet přidělených adres pro místní síť (LAN/MAN) od poskytovatele připojení k Internetu (ISP), vyčerpaný omezený celkový adresní prostor
  - částečné řešení: dynamické adresy jen pro aktuálně připojená odpojovaná zařízení – např. v mobilních sítích, v LAN DHCP
  - (trvalé?) řešení: IPv6 – „neomezený“ adresní prostor, ale pomalý přechod z IPv4
  - „trvalé“ „řešení“?!: **Network Address Translation (NAT)**

= **překlad IP adres** = přepisování v IP paketech libovolných adres v LAN na přidělené adresy v síti ISP a opačně – **basic (one-to-one) NAT**, mnoho RFC

- původně pro odstranění potřeby změny adres při změně (sítě) ISP
- téměř výhradně pro IPv4 (ale pro IPv6 experimentální Network Prefix Translation, NPTv6)

- pro LAN vyhrazené **rozsahy IPv4 adres pro privátní sítě** (RFC 1918): 10./8, 172.16./12, 192.168./16 – pakety s nimi se nesměrují, „platné“ pouze v LAN, tzv. **privátní**
- **carrier-grade/large-scale NAT (CGN/LSN)**: privátní adresy i v síti ISP, NAT mezi LAN a ní i mezi ní a sítí jeho ISP2, vyhrazený rozsah pro ISP (RFC 6598): 100.64./10

Překlad adres

- obvykle provádí (hraniční, přístupový) směrovač mezi LAN a sítí ISP – pro ni LAN $\sim$ koncový uzel v ní, „skrytí“ LAN za adresu (příp. více)
- adresa v LAN se při překladu neukládá např. do (záhlaví) paketu
- přidělených, tzv. **veřejných**, adres v síti ISP pro LAN je typicky méně než (privátních, současně „komunikujících“) v LAN

Překlad adres

- obvykle provádí (hraniční, přístupový) směrovač mezi LAN a sítí ISP – pro ni LAN ∼ koncový uzel v ní, „skrytí“ LAN za adresu (příp. více)
- adresa v LAN se při překladu neukládá např. do (záhlaví) paketu
- přidělených, tzv. **veřejných**, adres v síti ISP pro LAN je typicky méně než (privátních, současně „komunikujících“) v LAN

→ přepis **adresy a portu** – TCP/UDP (NAPT, PAT), z TCP spojení nebo výměny UDP datagramů (adresa socketu), **one-to-many NAT**

1. při přeposlání (úvodního) paketu jedním směrem uložení překládané adresy a porty v LAN a v síti ISP do **NAT translation table**
2. využití záznamu u dalších paketů v rámci spojení/výměny (pro stejný překlad) a u paketů opačným směrem (pro opačný překlad)!

Překlad adres

Obrázek z knihy
zdroj: KR 4.25

Source NAT (SNAT)

= překlad (privátní) zdrojové adresy a portu u paketů z LAN do sítě ISP a (veřejné) cílové u paketů zpět

- dynamický: dynamicky náhodná nová adresa (z více) a port v síti ISP (port volný)
- **maškaráda** („NAT“) = jediná (veřejná) adresa v síti ISP
- ne plně standardizované metody překladu ⇒ různé (nedokumentované) implementace se specifickým chováním:
  - **full/address+port restricted-cone (in/dependent filtering)**: pakety zpět jen ze (zdrojové) adresy a portu jakýchkoliv / takových, na které (cílové) šel úvodní paket (jen adresu nebo obojí)
  - **symetrický (dependent mapping)**: pro různé cílové adresy a porty různý překlad, jen u restricted cone
  - ponechat při překladu stejný (zdrojový) port?, kdy a jak (dynamicky) změnit překlad? aj.

Destination NAT (DNAT)

= překlad (veřejné) cílové adresy a portu u paketů ze sítě ISP do LAN a (privátní) zdrojové u paketů zpět

- **přesměrování portu (port forwarding)** = stejný (cílový) port
- pro pakety z LAN (na veřejnou adresu) potřeba i SNAT! = **NAT loopback/reflection/hairpinning**
- rozložení zátěže (load distribution): dynamicky vybraná nová adresa v LAN z více

Problémy/kontroverze

- narušení **koncové (end-to-end) komunikace** – přenos dat jedním směrem není možný dokud není zahájený druhým, do té doby neznámé (veřejné) adresy
  - problém pro některé služby, např. A/V telefonie, P2P sítě, navíc pokud protokol používá přepisovanou (privátní) IP adresu a/nebo TCP/UDP port → náročný **protocol tracking** a překlad „v datech“
  - → veřejná proxy/relay (např. SOCKS), DNAT (port triggering), metody **NAT traversal** (NAT-T, RFC 5389): (TCP/UDP/ICMP) hole punching, STUN, TURN, ICE, UPnP IGDP, NAT-PMP, PCP, predikce adresy a portu v síti ISP (u symetrického SNAT) aj.

Problémy/kontroverze

- narušení **koncové (end-to-end) komunikace** – přenos dat jedním směrem není možný dokud není zahájený druhým, do té doby neznámé (veřejné) adresy
  - problém pro některé služby, např. A/V telefonie, P2P sítě, navíc pokud protokol používá přepisovanou (privátní) IP adresu a/nebo TCP/UDP port → náročný **protocol tracking** a překlad „v datech“
  - → veřejná proxy/relay (např. SOCKS), DNAT (port triggering), metody **NAT traversal** (NAT-T, RFC 5389): (TCP/UDP/ICMP) hole punching, STUN, TURN, ICE, UPnP IGDP, NAT-PMP, PCP, predikce adresy a portu v síti ISP (u symetrického SNAT) aj.
- narušení **unikátnosti identifikace zařízení** připojeného k Internetu (IP adresou) – „sdílejí“ adresu v síti ISP, v různých LAN mohou mít stejné, rozšíření na adresu a port

Problémy/kontroverze

- narušení **koncové (end-to-end) komunikace** – přenos dat jedním směrem není možný dokud není zahájený druhým, do té doby neznámé (veřejné) adresy
  - problém pro některé služby, např. A/V telefonie, P2P sítě, navíc pokud protokol používá přepisovanou (privátní) IP adresu a/nebo TCP/UDP port → náročný **protocol tracking** a překlad „v datech“
  - → veřejná proxy/relay (např. SOCKS), DNAT (port triggering), metody **NAT traversal** (NAT-T, RFC 5389): (TCP/UDP/ICMP) hole punching, STUN, TURN, ICE, UPnP IGDP, NAT-PMP, PCP, predikce adresy a portu v síti ISP (u symetrického SNAT) aj.
- narušení **unikátnosti identifikace zařízení** připojeného k Internetu (IP adresou) – „sdílejí“ adresu v síti ISP, v různých LAN mohou mít stejné, rozšíření na adresu a port
- proměna Internetu z **nespojované (IP) sítě** na „jakousi“ spojovanou – udržování překladů (tj. stavů) pro TCP spojení nebo výměny UDP datagramů, jejich závislost na existenci překladů

Problémy/kontroverze

- narušení **koncové (end-to-end) komunikace** – přenos dat jedním směrem není možný dokud není zahájený druhým, do té doby neznámé (veřejné) adresy
  - problém pro některé služby, např. A/V telefonie, P2P sítě, navíc pokud protokol používá přepisovanou (privátní) IP adresu a/nebo TCP/UDP port → náročný **protocol tracking** a překlad „v datech“
  - → veřejná proxy/relay (např. SOCKS), DNAT (port triggering), metody **NAT traversal** (NAT-T, RFC 5389): (TCP/UDP/ICMP) hole punching, STUN, TURN, ICE, UPnP IGDP, NAT-PMP, PCP, predikce adresy a portu v síti ISP (u symetrického SNAT) aj.
- narušení **unikátnosti identifikace zařízení** připojeného k Internetu (IP adresou) – „sdílejí“ adresu v síti ISP, v různých LAN mohou mít stejné, rozšíření na adresu a port
- proměna Internetu z **nespojované (IP) sítě** na „jakousi“ spojovanou – udržování překladů (tj. stavů) pro TCP spojení nebo výměny UDP datagramů, jejich závislost na existenci překladů
- narušení **nezávislosti na vyšší vrstvě** (datech) – využití TCP/UDP portů pro přeposílání IP paketů, pro ICMP pakety využito místo portu ID (echo) nebo (část) záhlaví IP paketu v datech (jiné zprávy)

Problémy/kontroverze

- omezení počtu aktivních TCP spojení / UDP výměn mezi LAN a sítí ISP – $\approx$ 60 tis. (volných TCP/UDP portů) $\times$ přidělených adres v síti ISP

Problémy/kontroverze

- omezení počtu aktivních TCP spojení / UDP výměn mezi LAN a sítí ISP – $\approx$ 60 tis. (volných TCP/UDP portů) $\times$ přidělených adres v síti ISP
- pro pakety mezi LAN a sítí ISP manipulace s tabulkou překladů, přepočítání kontrolních součtů v IP a TCP/UDP záhlaví aj. – nutné výpočetní zdroje (výkon, paměť)
- ...

Problémy/kontroverze

- omezení počtu aktivních TCP spojení / UDP výměn mezi LAN a sítí ISP – $\approx$ 60 tis. (volných TCP/UDP portů) $\times$ přidělených adres v síti ISP
- pro pakety mezi LAN a sítí ISP manipulace s tabulkou překladů, přepočítání kontrolních součtů v IP a TCP/UDP záhlaví aj. – nutné výpočetní zdroje (výkon, paměť)
- ...

! u SNAT **„bezpečnost“ LAN, „skrytí“** před (ne-bezpečným) Internetem – typicky součást firewallu, ale pak port forwarding/triggering (DNAT), NAT traversal (zejm. UPnP) atd.!

Internet Protocol verze 6 (IPv6)

Úvod

- 90. léta **rozmach Internetu** (komercionalizace) + mobilní sítě a WiFi + IoT – změna rozsahu a způsobu využívání $\Rightarrow$ potřeba mnoha (unikátních) IP adres

Úvod

- 90. léta **rozmach Internetu** (komercionalizace) + mobilní sítě a WiFi + IoT – změna rozsahu a způsobu využívání $\Rightarrow$ potřeba mnoha (unikátních) IP adres

$\rightsquigarrow$ **vyčerpávání adresního prostoru IPv4** – nedostatečný [PS-1.1]

Úvod

- 90. léta **rozmach Internetu** (komercionalizace) + mobilní sítě a WiFi + IoT – změna rozsahu a způsobu využívání $\Rightarrow$ potřeba mnoha (unikátních) IP adres

$\rightsquigarrow$ **vyčerpávání adresního prostoru IPv4** – nedostatečný [PS-1.1]

$\rightarrow$ setření (CIDR, NAT), ale na (nejvyšší) úrovni IANA-RIR **vyčerpaný** 2/2011, na úrovni RIR-LIR 11/2019 [PS-1.2] $\rightsquigarrow$ černý trh s (globálními, veřejnými) IPv4 adresami

Úvod

- 90. léta **rozmach Internetu** (komercionalizace) + mobilní sítě a WiFi + IoT – změna rozsahu a způsobu využívání ⇒ potřeba mnoha (unikátních) IP adres

⇝ **vyčerpávání adresního prostoru IPv4** – nedostatečný [PS-1.1]

→ setření (CIDR, NAT), ale na (nejvyšší) úrovni IANA-RIR **vyčerpaný** 2/2011, na úrovni RIR-LIR 11/2019 [PS-1.2] ⇝ černý trh s (globálními, veřejnými) IPv4 adresami

= **následovník IPv4**, IPng: otevřený vývoj IETF od 1991, základ **RFC** 1883 (1995), **2460** (1998), 8200 (2017), neustálý vývoj, mnoho dalších RFC

- příležitost řešení více nedostatků IPv4 – např. nejednotné adresní schéma pro Internet a LAN (NAT)
- jediné dlouhodobé řešení problémů Internetu

Úvod

- 90. léta **rozmach Internetu** (komercionalizace) + mobilní sítě a WiFi + IoT – změna rozsahu a způsobu využívání ⇒ potřeba mnoha (unikátních) IP adres

⇝ **vyčerpávání adresního prostoru IPv4** – nedostatečný [PS-1.1]

→ setření (CIDR, NAT), ale na (nejvyšší) úrovni IANA-RIR **vyčerpaný** 2/2011, na úrovni RIR-LIR 11/2019 [PS-1.2] ⇝ černý trh s (globálními, veřejnými) IPv4 adresami

= **následovník IPv4**, IPng: otevřený vývoj IETF od 1991, základ **RFC** 1883 (1995), **2460** (1998), 8200 (2017), neustálý vývoj, mnoho dalších RFC

- příležitost řešení více nedostatků IPv4 – např. nejednotné adresní schéma pro Internet a LAN (NAT)
- jediné dlouhodobé řešení problémů Internetu

- nejen **větší adresní prostor** (delší adresy), **nový pohled** na síťový paket, adresy a protokol:
  - zjednodušení záhlaví paketu, volitelná další záhlaví
  - **automatická konfigurace zařízení** a objevování sousedů – lokální adresy, SLAAC, ND
  - podpora QoS, real-time přenosů – tok/flow paketů
  - **zabezpečení** (autentizace a šifrování) – IPsec
  - **mobilita** – s využitím tzv. domácích agentů („zastupující“ směrovač v domácí síti)

Úvod

- 90. léta **rozmach Internetu** (komercionalizace) + mobilní sítě a WiFi + IoT – změna rozsahu a způsobu využívání ⇒ potřeba mnoha (unikátních) IP adres

⇝ **vyčerpávání adresního prostoru IPv4** – nedostatečný [PS-1.1]

→ setření (CIDR, NAT), ale na (nejvyšší) úrovni IANA-RIR **vyčerpaný** 2/2011, na úrovni RIR-LIR 11/2019 [PS-1.2] ⇝ černý trh s (globálními, veřejnými) IPv4 adresami

= **následovník IPv4**, IPng: otevřený vývoj IETF od 1991, základ **RFC** 1883 (1995), **2460** (1998), 8200 (2017), neustálý vývoj, mnoho dalších RFC

- příležitost řešení více nedostatků IPv4 – např. nejednotné adresní schéma pro Internet a LAN (NAT)
- jediné dlouhodobé řešení problémů Internetu

- nejen **větší adresní prostor** (delší adresy), **nový pohled** na síťový paket, adresy a protokol:
  - zjednodušení záhlaví paketu, volitelná další záhlaví
  - **automatická konfigurace zařízení** a objevování sousedů – lokální adresy, SLAAC, ND
  - podpora QoS, real-time přenosů – tok/flow paketů
  - **zabezpečení** (autentizace a šifrování) – IPsec
  - **mobilita** – s využitím tzv. domácích agentů („zastupující“ směrovač v domácí síti)

! při zachování podstaty IP (end-to-end komunikace, nespojovost, hop-by-hop doručování) a kompatibility s dalšími protokoly (TCP/UDP, ICMP, IGMP → MLD, OSPF, BGP, DNS aj.)

Síťový paket

- před daty až 64 kB záhlaví 40 B:
- verze 4 b – hodnota 6
- traffic class 8 b $\sim$ TOS z IPv4 – priorita doručení/QoS (pro aplikaci nebo v rámci toku, v praxi differentiated services) a signalizace zahlcení (ECN, 2 b)
- **flow label** 20 b – ID **toku/flow paketů** = označení „souvisejících“ paketů mezi odesílatelem a příjemcem pro stejné zacházení $\sim$ **pseudospojení**, využití např. pro:
  - směrování – rozhodnutí jen u prvního paketu toku, rozkládání zátěže do více cest apod.
  - rezervaci přenosové kapacity (QoS, real-time, protokol RSVP) – např. pro streamovaný A/V přenos
  - prioritní uživatel aj.
- **délka dat** 16 b (v B) $\neq$ délka paketu z IPv4 – včetně volitelných záhlaví
- **další záhlaví** 8 b = číslo protokolu z IPv4 v datech (např. TCP 6, UDP 17, ICMP 58) nebo typ následujícího volitelného záhlaví
- hop limit 8 b $\sim$ TTL z IPv4 – snižování směrovačem o 1
- **adresy odesílatele a příjemce** 128 b – „aby už nikdy nedošly“

Síťový paket

Obrázek z knihy
zdroj: KR 4.16

Obrázek z knihy
zdroj: KR 4.26

Síťový paket

Z IPv4 záhlaví zrušeny:

- délka záhlaví – pevná (20 B)
- ID paketu, bity a offset pro **fragmentaci** paketu – směrovači náročná, pouze odesílatelem – volitelné záhlaví, udržování infa o minimální MTU k příjemcům
- kontrolní součet záhlaví – jsou na transportní a linkové (CRC) vrstvě

Síťový paket

Z IPv4 záhlaví zrušeny:

- délka záhlaví – pevná (20 B)
- ID paketu, bity a offset pro **fragmentaci** paketu – směrovači náročná, pouze odesílatelem – volitelné záhlaví, udržování infa o minimální MTU k příjemcům
- kontrolní součet záhlaví – jsou na transportní a linkové (CRC) vrstvě

Volitelná záhlaví (rozšíření $\sim$ volby z IPv4):

- posloupnost více, řetěz: v každém první položka typ následujícího 8 b [PS-2.3], druhá délka 8 b (v 8B, mimo 8 B), další proměnlivé [PS-2.4] – typy v pořadí:
- volby pro všechny (hop-by-hop) 0 – pro směrovače na cestě, položky typ 8 b, délka 8 b (mimo 2 B), hodnota [PS-2.5], např. výplně 1 (jen typ) a více B, upozornění směrovače, rychlý start (přenosová rychlost např. u 1. segmentu TCP), jumbogram (64 kB $<$ velikost paketu $<$ 4 GB) aj.
- volby pro cíl (destination) 60 – i za ESP (pro příjemce), např. výplně, PDM (měření zpoždění), domácí adresa aj.

Síťový paket

Volitelná záhlaví (rozšíření $\sim$ volby z IPv4):

- směrování 43 – typ 0 $\sim$ explicitní směrování z IPv4 2007 zrušen, typ 2 pro mobilitu (domácí adresa po doručení)
- fragmentace 44 $\sim$ z IPv4 – délka 8 B, jen bit více fragmentů, ID 32 b [PS-2.7], všechna záhlaví (i transportní) v prvním, ve všech záhlaví před fragmentačním [PS-2.9]
- **autentizace AH** 51 – odesílatele, i integrita paketu
- **šifrování ESP** 50 – dat, odesílatelem nebo směrovačem, poslední záhlaví, + AH = **IPsec**
- další volitelné, např. mobilita 135 aj.
- problém firewally – neznají záhlaví, paket zahodí

Adresy

- RFC 4291
- pro síťové rozhraní více (povinně), všichni v LAN stejná (pod)síť
- typy: unicast (individuální), multicast (skupinové, paket doručen všem členům skupiny) – broadcast speciální skupiny, např. všichni v LAN
  - **anycast (výběrové)** = skupinové, paket doručen jednomu „nejbližšímu“ (v počtu směrovačů na cestě) členu skupiny, např. routery v síti, (kořenové) DNS servery nebo webové servery – duplikace služby (rozložení zátěže, zrychlení, zálohy), i pro IPv4
- notace např. 2001:0718:1401:0050:0000:0000:0000:000d, zkrácený (kanonický) zápis 2001:718:1401:50::d, v URL v [] (RFC 3986)
- **síťový prefix** $\sim$ adresa sítě/maska z IPv4 – maska = počet bitů 1 (CIDR) = délka prefixu, např. 2001:718:1401:50::/64
- ::/128 (0) nedefinovaná (nepřidělená), ::1/128 **lokální smyčka (loopback)**

Adresy

Unicast (individuální)

- až 64 b síť (síťový prefix), 64 b ID (síťového) rozhraní [PS-3.1]
- **globální** zatím 2000::/3 (RFC 3587) – jednoznačné v rámci celého Internetu, dalších 45 b globální (směrovací) prefix sítě [PS-3.22]:
  - RIR: 32 b (má /12, přiděluje /29 až /32)
  - LIR: 16/24/32 b (přiděluje /48, /56 nebo /64)
  - pak ID podsítě zákazníků LIR: 16/8/0 b
  - pro dokumentace 2001:db8::/32 – u IPv4 tři /24
- **link local** fe80::/10 – jednoznačné v rámci LAN (propojení na linkové vrstvě), nesměrují se, dalších 54 b nulových
- **unique local (ULA)** fc00::/7 (fd00::/8 lokální přidělení, RFC 4193) – jednoznačné v rámci organizace (intranetu), nesměrují se, dalších 40 b náhodné globální ID, 16 b ID podsítě
  - dříve site local fec0::/10 – jednoznačné v rámci „místní“ sítě, 54 b ID podsítě, problém více „míst“ jedné organizace
  - obdoba vyhrazených rozsahů adres pro privátní sítě z IPv4 – link a unique local jejich rozšíření
  - NAT netřeba (dostatek globálních adres), ale existuje NPTv6 (RFC 6296, bezstavový obousměrný překlad síťových prefixů)

Adresy

ID rozhraní (unicast)

- pevně 64 b, vlastní (přidělené) – jako u IPv4, nebo generované:
- původně **modifikované IEEE EUI-64** = MAC adresa rozhraní dle IEEE 802.x s 0xfffe „uprostřed“ a druhý bit prvního byte 1 (lokalita), např. pro 00:02:b3:bf:30:ea je 202:b3ff:febf:30ea – problém globálního ID = MAC a ne-bezpečnosti (zneužití)

→ **kryptografické** (CGA, RFC 3972) – na základě veřejného klíče „vlastníka“ rozhraní, problém komplikovanosti určení

→ **náhodné krátkodobé** (Privacy Extensions, RFC 4941) pro odchozí komunikaci – náhodné, problém dočasnosti, návrh polovina stálá

→ **náhodné stálé** (RFC 7217) = posledních 64 b RID = hash síťového prefixu, (jiného) ID rozhraní a LAN, čítače a tajného klíče

Adresy

Multicast (skupinové)

- ff00::/8 – trvalé a dočasné, první 4 b druhého byte **dosah skupiny** [PS-3.15] $\sim$ jednoznačnost adresy v zóně, např. 1 rozhraní, 2 linka (LAN), 5 místo, 8 organizace, E globální, ostatní např. ISP, A CESNET2, 112 b ID skupiny
- ID skupiny: definované IANA (trvalé) a vlastní (dočasné) – typy: obsahující globální unicast prefix sítě, od jediného odesílatele (SSM), obsahující ID rozhraní aj., 32 b ID
- speciální např. ff0x::1 **broadcast** rozhraní/LAN, ff0x::2 všechny směrovače, ff02::1:ff00:0/104 **vyzývaný uzel (solicited node)** (poslední 3 B ID rozhraní, pro objevování sousedů), pro další typy uzlů a služeb (definované IANA, RFC 2375)

Adresy

Multicast (skupinové)

- ff00::/8 – trvalé a dočasné, první 4 b druhého byte **dosah skupiny** [PS-3.15] ∼ jednoznačnost adresy v zóně, např. 1 rozhraní, 2 linka (LAN), 5 místo, 8 organizace, E globální, ostatní např. ISP, A CESNET2, 112 b ID skupiny
- ID skupiny: definované IANA (trvalé) a vlastní (dočasné) – typy: obsahující globální unicast prefix sítě, od jediného odesílatele (SSM), obsahující ID rozhraní aj., 32 b ID
- speciální např. ff0x::1 **broadcast** rozhraní/LAN, ff0x::2 všechny směrovače, ff02::1:ff00:0/104 **vyzývaný uzel (solicited node)** (poslední 3 B ID rozhraní, pro objevování sousedů), pro další typy uzlů a služeb (definované IANA, RFC 2375)

Anycast (výběrové)

- ze stejné části adresního prostoru jako globální unicast (individuální)
- směrování v rámci nejdelšího společného síťového prefixu (udržování skupin na směrovačích) ⇒ téměř výhradně v rámci sítě/AS, globálně výjimečně
- problém různých „nejbližších“ příjemců (dynamičnost směrování) → zjištění unicast adresy nebo nestavová komunikace, např. DNS
- (pod)síť (∼ „obecná“ adresa): pevné ID rozhraní, např. 0 směrovače pro každý prefix

Nedokončené – přehledově

Objevování sousedů (Neighbor Discovery)

- **zjišťování a aktualizace linkové adresy** (MAC) rozhraní uzlu v LAN pro IPv6 adresu a opačně $\sim$ ARP a RARP u IPv4
- ověřování dosažitelnosti sousedů a detekce duplicitních adres v LAN

$\rightarrow$ žádost o a oznámení o linkové adrese – zprávy **neighbor solicitation (NS)** a **neighbor advertisement (NA)**

- používání link local adres, NS na (multicast) adresu vyzývaného uzlu
- součást **ICMPv6** (RFC 4443): formát paketu a zprávy jako u ICMPv4, nové zprávy

Autokonfigurace rozhraní

Bezstavová (StateLess Address AutoConfiguration, SLAAC)

- součást ND: **zjišťování směrovačů v LAN a dalších údajů sítě** (prefix, DNS aj.)

→ žádost o a oznámení směrovače – zprávy **router solicitation (RS)** a **router advertisement (RA)** – směrovače rozesílají (náhodně) periodicky, obě na (multicast) adresu všech směrovačů v LAN

- **„samopřidělení“** unicast (individuální) **adresy**:
  1. pro globální z RA, popř. s předchozí RS, získány údaje sítě
  2. vytvoření ID rozhraní – generované
  3. kontrola jedinečnosti v LAN – detekce duplicitní (ND)
     - pro globální (prefix) může být v RA „zakázáno“, link local vždy

Autokonfigurace rozhraní

Bezstavová (StateLess Address AutoConfiguration, SLAAC)

- součást ND: **zjišťování směrovačů v LAN a dalších údajů sítě** (prefix, DNS aj.)

→ žádost o a oznámení směrovače – zprávy **router solicitation (RS)** a **router advertisement (RA)** – směrovače rozesílají (náhodně) periodicky, obě na (multicast) adresu všech směrovačů v LAN

- **„samopřidělení“** unicast (individuální) **adresy**:
  1. pro globální z RA, popř. s předchozí RS, získány údaje sítě
  2. vytvoření ID rozhraní – generované
  3. kontrola jedinečnosti v LAN – detekce duplicitní (ND)
  - pro globální (prefix) může být v RA „zakázáno“, link local vždy

DHCPv6

- zprávy jako u DHCPv4, používání link local adres (a speciálních multicast)
- **stavové** = údaje sítě kromě směrovače – z RA, přidělení addresy
- **bezstavové** = údaje sítě kromě směrovače a prefixu – nepřidělení adresy → SLAAC
- identifikace uzlu (ne rozhraní!) **DUID** – 3 typy

Nasazení

= **postupný přechod**, ne „přepnutí Internetu“ z IPv4 na IPv6

- zpočátku (1996–2006) lokální IPv6 sítě propojené IPv4 tunely = síť 6bone, dnes přímo

? uživatelé a organizace (i menší ISP) „váhají“ – problém „slepice vs. vejce“

→ velcí poskytovatelé obsahu a ISP – potřeba mnoha adres, World IPv6 Launch Day 6. 6. 2012

- politická podpora – EU 2002, 2008, 2013, . . . , např. projekty 6NET, GEN6 aj., ČR 2009, 2015 výzva ministerstva/eGovernment po IPv6 . . .
- 2023 cca 40+ % (Internet Society, Google) koncových zařízení/sítí celosvětově, ČR cca 20+ %

Nasazení

= **postupný přechod**, ne „přepnutí Internetu“ z IPv4 na IPv6

- zpočátku (1996–2006) lokální IPv6 sítě propojené IPv4 tunely = síť 6bone, dnes přímo

? uživatelé a organizace (i menší ISP) „váhají“ – problém „slepice vs. vejce“

→ velcí poskytovatelé obsahu a ISP – potřeba mnoha adres, World IPv6 Launch Day 6. 6. 2012

- politická podpora – EU 2002, 2008, 2013, . . . , např. projekty 6NET, GEN6 aj., ČR 2009, 2015 výzva ministerstva/eGovernment po IPv6 . . .
- 2023 cca 40+ % (Internet Society, Google) koncových zařízení/sítí celosvětově, ČR cca 20+ %

Implementace

- i přes podobnost **nekompatibilní s IPv4**, nové protokoly nezávislé na IPv4
- 1996–2000 experimentální (Linux), 2000+ vlna „podporujeme IPv6“, 2005+ podpora výrobci HW a SW
- certifikace **IPv6 Forum** programy Ready pro hardware a systémy a Enabled pro služby (web a ISP) [PS-1.3]

„Přechodové mechanizmy“ (z/na IPv4) [SAMOSTUDIUM]

- **dual stack** = podpora současně IPv4 i IPv6
- **tunelování IPv6 v IPv4 a opačně**
  - manuální – tunel server (IPv4 do IPv6 sítě) a tunel broker (registrace na tunel serveru), např. Freenet6, SixXS aj.
  - automatické: dříve 6to4, Teredo, 6over4, ISATAP, dnes **6rd** (IPv6 Rapid Deployment), **DS** (Dual-Stack) **Lite**, **lw4o6** (Lightweight 4over6), MAP-E
- **překlad (adres a DNS) mezi IPv6 a IPv4**: základ **SIIT** (Stateless IP/ICMP Translation), starší NAT-PT (NAT – Protocol Translation), novější **NAT64 a DNS64**, **464XLAT**, MAP-T, TRT (Transport Relay Translator), BIH (Bump-in-the-Host), SOCKS64