# Bezdrátové sítě: výhody, režimy a base station, příklady.

* kdekoliv (GPS), kdykoliv, bez omezení (drátu), snadnost použití (i cenou)
* bezdrátová LAN (Wi-Fi): + snadnost instalace, rozšiřitelnost, původně pro vnitřní použití, rychle i vnější (připojení k internetu, hotspot), počítače, spotřební elektronika, domácí spotřebiče
* bezdrátová PAN (Bluetooth): bezdrátové propojení (mobilních) zařízení "všeho druhu", počítače, spotřební elektronika, periferie
* "bezkontaktní" (RFID/NFC): prezence, identifikace (platby) aj., "čipy"
* senzorové sítě: vestavěná zařízení (senzory) pro sběr dat o okolí
* stanice bezdrátově připojené k base station nebo mezi sebou
* base station: řízení přenosů připojených (asociovaných) stanic
* volitelně připojený do ostatní (typicky drátové) sítě = infrastruktury a zprostředkovávající ji stanicím 🡪 přepínač+most = infrastrukturní režim
* jinak propojení stanic přímo mezi sebou = ad hoc režim
* např. access point (AP, Wi-Fi), BTS (mobilní)
* 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), geostacionární (36 tis. km, zpoždění signálu stovky ms), nízkoorbitální (LEO, do 2 tis. km)

# 2. Bezdrátové sítě: přenosové médium, šíření signálu a SNR, modulace bitů do signálu (přehledově), multiplex přenosů do pásma (přehledově), problémy skryté a vystavené stanice, bezpečnost.

* přenosové médium elmag vlny (rádio) -- průchod materiály, mobilita zařízení, velká vzdálenost
* ale závislost na prostředí (odrazy, tzv. Fresnelova zóna) a vzdálenosti, interference, omezení vyzářeného výkonu (např. Wi-Fi stovky mW, norma ČTÚ)
* problémy:
  + klesající úroveň signálu se vzdáleností a průchody materiály = path loss
  + interference a šum na stejném frekvenčním pásmu, např. na 2.4 GHz Wi-Fi, Bluetooth, RFID, dálkové ovládání, (bezdrátové) telefony, mikrovlnné trouby aj.
  + více cest s různým signálem kvůli odrazům a interferencím = multipath propagation, fading -> více frekvencí (modulace), antén, opakování přenosu aj.
  + horší s vyšší frekvencí => více chyb -> nejen CRC, i znovu zasílání dat
* signal-to-noise ratio (SNR): uzel přijímá kombinaci degradovaného signálu od odesílatele a šumu prostředí, poměr "sil", v dB (= 10log\_10 poměr)
* vyšší = výrazně nižší chybovost (bit error rate), ale limit (výhodnost, výkon, interference)
* pro stejnou SNR výrazně vyšší pro rychlejší přenosy (modulace signálu) => dynamický výběr modulace signálu (a rychlosti) dle aktuálního SNR
* šíření signálu ve frekvenčním pásmu -- pásmo jako okruh (circuit) = rezervace pro relaci mezi komunikujícími stranami, pro odolnost proti klesání úrovně a interferenci:
* frequency hopping spread spectrum (FHSS): pseudo-náhodné přeskakování mezi (nosnými) frekvencemi (stovky Hz), např. vojenství (obtížná detekce a rušení), Wi-Fi (první), Bluetooth
* direct sequence spread spectrum (DSSS): kódování do (nosných) frekvencí, CDM (multiplex)
* modulace bitů do (analogového) signálu: změna amplitudy (ASK), frekvence (FSK), fáze (PSK) nosné frekvence nebo kombinace (A+P), BPSK (1 bit/symbol), QPSK (2), QAM-16 (4), QAM-64 (6), QAM-256 (8), QAM-1024 (10)
* multiplex více přenosů (paralelních částí nebo různých stanic) do (širšího) frekvenčního pásma:
* frekvenční (FDM) - rozdělení (division) na nepřekrývající se (pod)pásma dané šířky pro přenos, např. rádio, telefon (4 kHz), xDSL (50 kHz/X MHz), kabel/DOCSIS (6/6 MHz), mobilní sítě (kombinace s TDM)
* ortogonální frekvenční (OFDM (A)) - mnoho nosných frekvencí (subcarriers) pro paralelní přenosy s překrývajícími se (pod)pásmy (A přidělované pevné časy, současné využití
* subcarriers), např. Wi-Fi (novější), mobilní sítě (4G, kombinace s FDM i TDM)
* časový (TDM) - disjunktní rozdělení času na (časové) rámce s konstantním počtem slotů pevné délky s daným slotem každého rámce pro přenos, např. mobilní sítě (kombinace s FDM), kabel/DOCSIS (upstream)
* kódový (CDM/CDMA) - kódování přenosů v celém pásmu (chipping/XOR bitů vhodným kódem pro přenos a předpoklad součtu, vyšší chipping rate, např. 11x), např. vojenství (dříve), mobilní sítě (3G), Wi-Fi (starší, Barker, CCK kód)
* frekvenční (pod)pásmo = broadcast sdílené médium – potřeba protokol vícenásobného přístupu (vysílání), centrálně řízeného (PCF) nebo samotnými stanicemi (DCF)
* problémy 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)
* bezpečnost – šíření signálu, propojení s infrastrukturou, příjem "všemi" (neomezený přístup) -> autentizace stanic (vůči base station) a šifrování přenosu (s base station)
* - mobilita – předávání (handoff) stanic mezi base station

# 3. Wi-Fi: standardy a frekvence, antény, BSS, asociace stanice.

* Wi-Fi (IEEE 802.11, Wireless Fidelity)
* IEEE, 1997, Wi-Fi Alliance -- certifikace
* bezdrátová LAN/MAN, původně pro vnitřní použití (desítky až stovky m), rychle i vnější (připojení k Internetu, hotspot, až jednotky km), jednotky Mb/s až Gb/s: počítače, spotřební elektronika, domácí spotřebiče
* několik standardů (rozšíření): (legacy)/b/g = Wi-Fi 0/1/3 (1997/1999/2003, 2.4 GHz, až 2/11/54 Mb/s, běžně cca polovina), a/ac = 2/5 (1999/2013, 5 GHz, až 54 Mb/s/6.9 Gb/s), n/ax = 4/6 (2008/2019, 2.4 a 5 GHz, až 0.6/9.6 Gb/s), ax = 6E (2020, 6 GHz, až 9.6 Gb/s), zpětná kompatibilita, ad/ay ~ WiGig (2012/2021, 60 GHz, až 7/40 Gb/s)
* bezlicenční pásma (ISM): 2.4-2.4895 GHz -- 75/13+1 výrazně se překrývajících /22/20/40 MHz (/b/g+n+ac+ax/n+ac+ax, FHSS/DSSS/OFDM) pásem/kanálů po 5 MHz. mezi nepřekrývajícími se alespoň4/3/7 (b/g/n)
* 5.03-5.99 GHz -- 38/15/7/3 nepřekrývajících se 20/40/80/160 MHz (a+n/n/, ac+ax, OFDM) pásem/kanálů
* 57.24-70.20 Ghz (V band) -- 6/5/4/3 ne/překrývajících se 2.16/4.32/6.48/8.64 GHz (ad/ay, OFDM) pásem/kanálů
* licencované pásmo 5.945-7.125 GHz -- 59/29/14/7 nepřekrývajících se 20/40/80/160 MHz (ax, OFDMA) pásem/kanálů
* multiple input multiple output (MIMO): více vysílacích i přijímacích antén s různým současným signálem, nasměrování vysílání k příjemci, n/ac+ax+ad (4/8), multi user (MU): více proudů, ac+ax+ay
* antény:
  + všesměrové -- všechny směry v horizontální rovině kolmé na tyčovou anténu + mírně nahoru a dolů
  + (sektorové) směrové – různě široká kulová výseč před a v menší míře i za (síťovou) parabolickou, panelovou nebo šroubovice (Yagi) anténou
* různé polarizace signálu (horizontální, vertikální, kruhové)
* vestavěné i venkovní -- VF koax kabel a konektor SMA nebo N
* infrastrukturní i ad hoc režim (včetně point-to-point)
* basic service set (BSS): stanice a případně base station = access point (AP), identifikovaná SSID ("jméno sítě", MAP AP nebo řetězec znaků až 32 B), kanál
* MAC adresa síťového rozhraní stanice (včetně base) jako u Ethernetu
* asociace stanice k (jednomu) AP: nutná, komunikace jen s ním
* AP periodicky (100 ms) vysílá majákové (beacon) rámce s (volitelně) SSID (až 32 B) a MAC adresou AP (a info k zabezpečení, rychlostem/modulacím aj.)
* stanice skenuje kanály, pasivně nebo aktivně (vyšle probe request rámec a od AP response), a výběr (nestandardizovaný, typicky s nejvyšším SNR!) -- association request k AP (nutné SSID) a od něj response
* může být vyžadována autentizace stanice (viz dále, jinak otevřená, možný přístupový seznam MAC adres, komunikace jen s AP), pak až datové rámce, např. DHCP

# 4. Wi-Fi: CSMA/CA, linkový rámec a adresy.

* CSMA: náhodný vícenásobný přístup (multiple access) ke sdílenému médiu (kanálu)
* čekání na klid (carrier sense) a vysílání (které se nějakou dobu šíří)
* CD: při detekci kolize (collision detection) náhodná pauza a znovu vysílání -- kolize na straně vysílajícího!, nejvýše jedno současné vysílání
* Obr. KR-6.13
* CSMA/CA: předcházení kolizím (collision avoidance) -- náročné/nemožné zároveň přijímat (naslouchat) a vysílat (výrazně slabší přijímaný signál) = (polo)duplexní přenos a problém
* skryté/vystavené stanice -- kolize na straně příjemce!, více současných vysílání (různým "nevidícím se" příjemcům)
* pozitivní potvrzování a znovu zaslání rámce -- kvůli vyšší chybovosti
* 1. při klidu chvíle čekání (distributed inter-frame spacing, DIFS), jinak náhodná pauza (jednotky ms, v iteracích zdvojnásobované maximum, binary exponential backoff), odpočítávaná při klidu! (po DIFS)
* 2. vyslání celého rámce, příjemce po chvíli od přijetí (short inter-frame spacing, SIFS) potvrdí ACK rámcem, pokud do určité doby (jednotky ms) ne, znovu (= iterace), po několika (15) pokusech chyba, "obsazení" média pro rámec i ACK
* Obr. KR-7.10, TFW-4.25
* volitelná rezervace média pro (delší, RTS threshold > MTU) vysílání stanice (ne AP) -- pro další zamezení kolizím a kvůli problému skryté (ne vystavené) stanice (podobně jako původní MACA)
* request to send (RTS) rámec s časem pro přenos dat a potvrzení místo datového
* AP vyšle po SIFS clear to send (CTS) rámec rezervující médium na čas
* vyslání dat a potvrzení (CSMA/CA 2., po SIFS), ostatní po čas nezkouší vysílat
* možné kolize (krátkých) RTS/CTS -- CSMA/CA 1.
* Obr. TFW-4.27, KR-7.12
* linkový rámec: data (až 2312 B, obvykle do 1500, LLC), CRC32 rámce, před ním záhlaví fyzické vrstvy (rádia) -- modulace (rychlost), kanál aj., záhlaví:
* Obr. KR-7.13
* až 4 MAC adresy: 1. přijímající stanice, 2. vysílající stanice
* 3. odesílatel/příjemce v infrastruktuře -- BSS je v ní zahrnutá, AP funguje jako (netransparentní) most, příjemce/odesílatel = přijímající/vysílající stanice, nebo v jiné přímo připojené BSS nebo v ad hoc režimu
* 4. příjemce/odesílatel v ne infrastruktuře
* čas "obsazení" a rezervace média (NAV, Network Allocation Vector), pořadové číslo rámce (a ID fragmentu) -- pro rozlišení a seřazení znovu zaslaného a dalšího rámce (jako v TCP)
* verze (00), typ a subtyp pro rozlišení control (ACK, RTS, CTS, bez dat), management (beacon, probe, association, autentizační) a datových rámců, od a do pro význam adres (3.,4.), více fragmentů, opakování rámce, power management (spaní), další rámce, šifrování (dat) rámce
* mobilita v (W)LAN (ve stejné IP síti): mezi více BSS (AP), se stejným SSID = extended service set (ESS), pro zvýšení rozsahu pokrytí, propojených např. přepínačem nebo point-to-point (i Wi-Fi, tzv. distribuční systém, 802.11f), ne směrovačem
* zachování IP adresy a spojení (TCP aj.)
* stanice při slábnoucím signálu od AP aktivně skenuje a deasociuje se a asociuje k silnějšímu (handoff, reasociace)
* přepínač: samoučení! -- při prvním rámci přes nový AP od stanice, jinak po asociaci broadcast rámec od nového AP se zdrojovou MAC stanice (hack!) nebo protokol mezi AP (802.11f)
* adaptace rychlosti (modulace signálu dle SNR): nestandardizované, např. při dvou rámcích bez potvrzení následující nižší, při 10 potvrzených nebo vypršení času od posledního snížení vyšší
* podobně jako řešení zahlcení sítě v TCP
* kratší rámce = fragmenty: nestandardizovaná délka, vysílány za sebou s ACK (a SIFS)

# 5. Wi-Fi: mobilita, adaptace rychlosti a správa energie, zabezpečení.

* zabezpečení: původní specifikace WEP (Wired Equivalent Privacy, 1999, "průšvih"), dočasné WPA (Wi-Fi Protected Access, 2002) -> WPA2 (802.11i, 2004), WPA3 (2018)
* autentizace stanice vůči AP:
* na základě sdíleného hesla -- Personal, WEP: před asociací, až 4 40/104 b, šifrování a dešifrování náhodné výzvy!, WPA (2/3): generování pre-shared key (PSK) ~ MK = PMK z hesla 8 až 63 B a SSID
* autentizační protokol -- Enterprise, WPA (2/3), 802.11i: EAP (TLS, TTLS, PEAP, MD5 aj., certifikáty, jméno, heslo aj., EAPoL/802.1X, volitelně šifrované, autentizace uživatele), může
* řešit autentizační server (RADIUS, DIAMETER, šifrované, AP relay pouze s ním), dohoda na metodě, (vzájemná) autentizace a vygenerování sdíleného master key (MK), vytvoření pairwise MK (PMK) z MK a předání AP ze serveru (distribuce klíče, včetně sdíleného pro broadcast/multicast), volitelná "předběžná" k jinému AP (handoff, WPA2/3)
* šifrování rámců (dat a CRC) mezi stanicí a AP:
* symetrická šifra RC4 -- proudová, WEP: klíč sdílené heslo + 24b! IV za záhlavím různý pro každý rámec, WPA = TKIP/WEP-fix: 128 klíče vybírané z IV, pořadového čísla rámce a klíče relace PTK vytvořeného z PMK, MAC a náhodných výzev, 64b kód integrity celého rámce MIC za daty šifrováním ~ dig. podpis, z původních a šifrovaných dat možno snadno odvodit klíč, u WEP možné nešifrované CRC aj. problémy
* AES/Rijndael -- bloková, WPA2/3 = CCMP: klíče jako u WPA, ale jen z PTK, kód integrity jako u WPA
* Obr. KR-8.30
* WPS (Wi-Fi Protected Setup): automatická konfigurace nejlepšího zabezpečení stanic z AP (generování a distribuce SSID a sdíleného hesla, PIN od AP)
* Mobilita
* mezi IP sítěmi (VLAN): propojenými směrovačem -- jiná adresa, možné narušení spojení (TCP aj.)
* nalezení mobilního zařízení, jeho adresace a směrování k němu, předání (handoff)
* mobile IP
* správa energie: nestandardizované, minimalizace doby funkce stanice (ne AP)
* stanice nastaví power management bit v rámci k AP a spí dokud AP nepošle beacon rámec (nastavený "budík" těsně před)
* AP rámce pro ni ukládá do bufferu a v beacon rámci pošle seznam stanic "v bufferu"
* stanice v seznamu si rámce vyžádá, jinak případně opět spí
* ukládání rámců AP pro stanici do bufferu a zaslání jen po obdržení rámců od stanice, která jinak spí (APSD, n), rozvrhování vysílání stanic AP (ax)
* prioritizace provozu (QoS, různé IFS, TXOP, 802.11e), omezení vyzářeného výkonu (regionální) aj.

# 6. Bluetooth: charakteristika, piconet, profily, vrstvy, párování zařízení.

* Bluetooth (IEEE 802.15.1)
* Ericsson, 1994, + IBM, Intel, Nokia, Toshiba, 1998, jméno po vikingském/dánském králi
* bezdrátové propojení různorodých 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 (sluchátka, přehrávače, hodinky, senzory apod.) -- "náhrada kabelů", bezdrátová PAN
* 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 (ISM), 79 1MHz pásem/kanálů, TDM (slot 625 us) s FHSS (adaptivní s vyloučením využívaných pásem), modulace FSK (1 b/symbol, 1 Mb/s, basic rate), PSK (verze 2, 2/3 b/symbol, 2/3 Mb/s, enhanced rate, pouze data rámců)
* piconet: až 8 aktivních (komunikujících) zařízení, ostatních až 255 zaparkovaných (uspaných, nekomunikujících)
* jedno master: např. počítač, mobil, řídí komunikaci -- určuje časování (sloty), frekvence (FHSS), adresy zařízení, kdo kdy vysílá aj., může vysílat v každém sudém slotu, (de)aktivace Zařízení
* ostatní slave -- komunikace jen s master, vysílání jen když v předchozím slotu příjem od master
* scatternet: více propojených piconetů přes zařízení slave v jednom a master v druhém (most), zařízení může být ve více piconetech
* profily: různá použití (aplikace) a protokoly, 20+
* základní/generic: zjištění služeb, správa spojů/links, výměna dat, emulace sériové linky aj.
* PAN (ad-hoc, připojení k jiné, např. Wi-Fi přes AP), dial-up (připojení k telefonní síti přes modem), A/V (streaming, headset, hands-free, intercom), HID, přenos souborů (speciálně obrázků), remote control, synchronization aj.
* vlastní protokolová architektura: vrstvy radio ~ fyzická, link control (baseband) ~ MAC -- využití TDM, link manager (správa spojů/links a energie, párování, šifrování), L2CAP (rámce, jejich potvrzování a znovu zasílání, multiplexing pro profily, QoS), a profily využívající L2CAP nebo napříč vrstvami
* Obr. TFW-4.31
* host controller interface: rozhraní mezi Bluetooth čipem a zařízením, mezi link manager a L2CAP
* párování zařízení: před propojením (vytvořením spoje/link), zadání stejného PIN (4 cifry, starší) nebo potvrzení stejného zobrazeného hesla nebo zadání hesla z jednoho na druhém zařízení (novější)
* spoje/links: synchronní spojované (SCO) pro real-time přenosy (A/V, až tři 64kb/s, pevné sloty, rámce neznovu zasílány, samopopravné kódy) a asynchronní nespojované (ACL) pro paketové přenosy (souborů, PAN aj., jen jeden, rámce z L2CAP)
* CSMA s rezervací média a pozitivním potvrzováním (a znovuzasláním) rámců
* odesílatel vyšle při klidu RTS rámec s časem pro přenos dat a potvrzení
* příjemce vyšle (broadcast) CTS rámec rezervující médium na čas
* vyslání dat a potvrzení (ACK), ostatní po čas nezkouší vysílat
* ?? kolize RTS/CTS/ACK
* linkový rámec: více, 1/3/5 slotů, data (až 2744 b basic rate, 8184 b enhanced rate, volitelně šifrovaná, klíč vytvořený při spojování), před synchronizace a přístupový kód = ID master, záhlaví 3x (platí většinové bity, "omezenost" zařízení):
* Obr. TFW-4.32
* adresa (0 = broadcast), typ (SCO, ACL aj., počet slotů, jaký samoopravný kód), bity flow (slave má plný buffer), ACK a seq (znovuzaslání), CRC-8
* formáty dat pro SCO a ACL rámce dle rate (např. SCO basic 1 slot 240 b, 80/160/240 b + samoopravný kód -- 80 b 3x, 13% využití kapacity)

Zigbee (IEEE 802.15.4)

* ještě méně energetická zařízení než Bluetooth, např. (domácí) senzory, ovladače, desítky až stovky kb/s
* více režimů sítě, zařízení plně funkční ~ master u Bluetooth (může jich být víc v mesh síti) a redukovaně funkční ~ slave
* potvrzování a znovu zasílání rámců, CSMA/CA (~ Wi-Fi), TDM -- super rámec: majákový, aktivní (vysílání, 16 slotů, některé CSMA/CA, některé přiřazené zařízením) a neaktivní perioda (spaní všech)

# 7. NAT: problém a řešení, CGN, popis funkce, problémy/kontroverze.

# 8. NAT: typy a metody, příklady.

* každé zařízení připojené k Internetu potřebuje (unikátní!) IP adresu -- vedle síťové infrastruktury i koncová: počítače, mobily, spotřební elektronika, domácí spotřebiče, auta, infrastruktura, senzory, "věci", ...
* IPv4: omezený počet přidělených adres pro místní síť (LAN/MAN) od poskytovatele připojení k Internetu (ISP) -- zvláště koncovým uživatelům (SOHO), vyčerpaný omezený adresní prostor
* částečné řešení: dynamické jen pro aktuálně připojená odpojovaná zařízení, např. mobilní sítě, dříve telefonní připojení (dialup), v LAN DHCP
* rešení: IPv6 -- "neomezený" adresní prostor, ale pomalý přechod
* = překlad IP adres -- přepisování v paketech (libovolných, unikátních) adres v LAN na přidělené adresy v síti ISP a opačně, pro umožnění komunikace mezi LAN a sítí ISP, basic (one-to-one) NAT, RFC 1631, 2663, 2709, 2766, 2993, 3022, 3027, 3235, 3489, 3715, 4787 aj.
* původně pro odstranění potřeby změny adres zařízení při změně sítě
* téměř výhradně pro IPv4 (ale pro IPv6 je experimentální Network Prefix Translation, NPTv6)
* obvykle provádí (hraniční/přístupový) směrovač mezi LAN a sítí ISP, při přeposílání IP paketů z LAN do sítě ISP a obráceně-- pro ni koncový uzel s adresou (příp. více) v síti ISP, "skrytí" LAN
* vyhrazené rozsahy IPv4 adres pro privátní sítě (RFC 1918): 10./8, 172.16./12, 192.168./16 -- kvůli možné "kolizi" (ostatních) adres v LAN, mezi nimi a v Internetu (jinak jejich překlad na tyto, "interní", ale problém s DNS aj.), 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 (NAT44, NAT64 -- IPv6 v síti ISP), kvůli možné "kolizi" privátních adres v LAN a síti ISP další vyhrazený rozsah pro ISP: 100.64./10 (RFC 6598)
* adresa v LAN se při překladu (v paketu) neuchovává a přidělených (tzv. veřejných) adres v síti ISP je typicky méně než (privátních, současně komunikujících) v LAN -> pro jednoznačnost překladu přepis dvojice [adresa, port] -- port TCP/UDP (NAPT, PAT, one-to-many NAT), z TCP spojení nebo výměny UDP datagramů (adresa socketu) -- jejich překlad
* při přeposlání (úvodního) paketu jedním směrem uložení dvojic [adresa, port] v LAN a v síti ISP do NAT translation table -- pro umožnění stejného překladu pro další pakety v rámci spojení/výměny a následně i opačného překladu u paketů opačným směrem (!)
* source NAT (SNAT): překlad (privátní) zdrojové [adresa, port] u paketů z LAN do sítě ISP a (veřejné) cílové zpět, porty náhodné (volné), 1 (veřejná) adresa v síti ISP = maškaráda ("NAT")
* Obr. KR-4.25
* -> umožnění komunikace z LAN (klient) do sítě ISP (server)
* dynamický: dynamicky náhodná adresa v síti ISP z více, dynamická translation table, jinak statický
* ne plně standardizované metody překladu, různé (nedokumentované) implementace se specifickým chováním:
* full/address+port restricted-cone (in/dependent filtering): zpět jen ze (zdrojové) [adresa, port] jakékoliv / takové, na kterou (cílovou) šel úvodní paket (jen adresu nebo obojí)
* symetrický (dependent mapping): pro různé cílové [adresa, port] různý překlad, restricted cone
* dále zda stejné zdrojové porty, kdy a jak změna překladu aj.
* destination NAT (DNAT): překlad (veřejné) cílové [adresa, port] u paketů ze sítě ISP do LAN a (privátní) zdrojové zpět, port stejný = přesměrování portu (port forwarding), pro pakety z LAN potřeba i SNAT (NAT loopback/reflection/hairpinning)!
* -> umožnění komunikace ze sítě ISP (klient) do LAN (server)
* rozložení zátěže (load distribution): překlad na vybranou z více adres v LAN
* problémy/kontroverze:
* narušení koncové (end-to-end) komunikace -- přenos dat jedním směrem není možný, dokud nezahájený druhým, do té doby neznámé (veřejné) adresy
* problém pro některé aplikační protokoly, např. u P2P sítí, navíc pokud používají přepisovanou IP adresu a/nebo TCP/UDP port, např. A/V telefonie -> 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, NAP PMP, PCP, predikce [adresa,port] v síti ISP (u symetrického SNAT)
* narušení unikátnosti identifikace zařízení připojeného k Internetu IP adresou -- "sdílejí" adresu v ISP síti, v různých LAN mohou mít stejné, rozšíření na [adresa,port], port pro adresaci procesů (aplikací) na zařízení, ne jich
* proměna Internetu z nespojované 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) a závislost na konkrétních protokolech vyšší vrstvy -- využití TCP/UDP portů pro přeposílání IP paketů, pro ICMP pakety využito ID (echo), (část) záhlaví IP paketu v datech (jiné, u time exceeded jen zdrojová IP adresa!)
* omezení počtu aktivních spojení/výměn mezi LAN a sítí ISP -- ~ 60 tis. (volných TCP/UDP portů) x 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 (z tzv. pseudozáhlaví a dat, sestavení fragmentů!) -- výpočetní zdroje
* - u SNAT "bezpečnost" LAN od (ne-bezpečného) Internetu -- nemožnost komunikace ze sítě ISP do LAN, typicky součást firewallu, ale port forwarding/triggering (DNAT) a NAT traversal (zejm. UPnP)!

# 9. IPv6: úvod (problém IPv4) a vlastnosti, síťový paket.

# 10. IPv6: adresy (druhy, typy), ID síťového rozhraní (metody určení). 11. IPv6: přehledově SLAAC, DHCPv6, NDP, přechod z IPv4.

Internet Procotol verze 6 (IPv6)

* první polovina 90. let rozmach Internetu (komercionalizace) + mobilní sítě+ IoT => potřeba mnoho (unikátních) IP adres
* -> vyčerpávání adresního prostoru IPv4 => nedostatečný, "setření" (CIDR, NAT), na (nejvyšší) úrovni IANA-RIR vyčerpaný 2/2011, na úrovni RIR-LIR 11/2019 -> černý trh s (globálními, veřejnými) IPv4 adresami
* Obr PS-1.1
* uživatelé Internetu od institucí (v USA) přes firmy a jednotlivce k "věcem" celosvětově, konvergence telekomunikačních a TV/rádio sítí k datovým v Internetu -> změna rozsahu a způsobu využívání (množství přenosů, real-time)
* = následovník IPv4 (ST-2 ~ IPv5 zrušen), IPng: otevřený vývoj IETF od 1991 (odhady vyčerpání IPv4 2008+, ale potřeba dlouhé doby nasazení), 1995 RFC 1883 základ, neustálý vývoj dalšího 1998 RFC 2460 a další, např. 2004/2011 mobilita, 2017 RFC 8200 a další aktuální (Happy Eyeballs)
* příležitost řešení více nedostatků IPv4 (např. nejednotné adresní schéma pro Internet a LAN - NAT), před ním návrh např. OSI CLNP (160b adresy, podobný IPv4, "ale OSI"), původní SIPP (Simple Internet Protocol Plus, 64b adresy)
* jediné dlouhodobé řešení problémů
* nejen větší adresní prostor (delší adresy), nový pohled na síťový paket, adresy a protokol:
* zjednodušení záhlaví paketu -- pro rychlejší zpracování směrovačem
* automatická konfigurace zařízení (adresa, síť, brána, DNS aj.) a objevování sousedů
* podpora QoS, real-time přenosů -- tok/flow paketů
* zabezpečení (autentizace a šifrování) -- IPsec, zpětně přidány i do IPv4
* mobilita -- s využitím tzv. domácích agentů ("zastupující" směrovač v domácí síti, přeposlání prvních dat a oznámení nové adresy), bez změny adresy, se zachováním TCP spojení při změně sítě
* volitelná další záhlaví -- flexibilita, rychlejší zpracování směrovači
* při zachování podstaty IP (nespojovost, hop-by-hop doručení paketu) a kompatibility s dalšími protokoly (TCP/UDP, ICMP, IGMP -> MLD, OSPF, BGP, DNS aj.)
* síťový IPv6 paket: před daty záhlaví 40 B, položky jen nejnutnější
* Obr. KR-4.16 vs. KR-4.26
* verze 4 b (hodnota 6) -- nadbytečná (záhlaví linkového rámce obsahuje typ dat)
* traffic class 8 b ~ TOS z IPv4 -- priorita doručení/QoS (pro aplikaci nebo v rámci toku) a signalizace zahlcení (ECN, 2 b), v praxi differentiated services
* flow label 20 b -- ID toku/flow paketů = označení "souvisejících" paketů mezi odesílatelem a příjemcem pro stejné zacházení ~ pseudospojení (~ spojení např. v TCP, "related" pakety, ale porty nemusí být dostupné), může i směrovač na cestě, využití např. pro směrování (rozhodnutí jen u prvního paketu toku, rozkládání zátěže do více cest), rezervaci přenosové kapacity (QoS, real-time, protokol RSVP), např. pro streamovaný A/V přenos, prioritní uživatel apod.
* délka dat 16 b (v B) != 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 ~ TTL z IPv4 -- snižování směrovačem o 1
* adresy odesílatele a příjemce 128 b (2^128 ~= 3.4\*10^38) -- "aby už nikdy nedošly"
* z IPv4 záhlaví zrušena: délka záhlaví (pevná)
* ID paketu, vlajky a offset pro fragmentaci (fragmentace paketu směrovači na cestě náročná) -- pouze odesílatelem, (periodické) zjištění max velikosti MTU paketu (např. pro TCP) algoritmem PMTUD (min 1280 B): směrovač velký paket zahodí a zašle odesílateli ICMP zprávu "velký paket" s MTU
* kontrolní součet záhlaví (potřeba na každém směrovači na cestě přepočítat min kvůli TTL) -- jsou na transportní a linkové (CRC) vrstvě
* volitelná záhlaví (rozšíření ~ volby z IPv4): posloupnost více, v každém první položka typ následujícího (v posledním číslo protokolu z IPv4 v datech, včetně žádného 59), druhá délka záhlaví 8 b (v 8B, mimo 8 B), další proměnlivé, typy v pořadí:
* Obr. PS-2.3, PS-2.4
* volby pro všechny (hop-by-hop) 0 -- pro směrovače na cestě, položky typ 8 b (první 2 b při neznalosti přeskočit, paket zahodit, + ICMP odesílateli, + pokud ne skupině), délka 8 b (mimo 2 B), hodnota, např. výplně1 (jen typ) a více B, upozornění směrovače (např. o RSVP), rychlý start (přenosová rychlost např. u 1. segmentu TCP), jumbogram (64 kB < velikost paketu < 4 GB, délka dat v povinném záhlaví = 0, ne fragmentace), aj.
* volby pro cíl (destination) 60 -- i za ESP (pro příjemce), např. výplně, PDM (měření zpoždění), domácí adresa aj.
* směrování 43 -- typ 0 ~ explicitní směrování z IPv4 (seznam adres směrovačů k příjemci, postupně jako cílové) 2007 zrušen, typ 2 pro mobilitu (domácí adresa po doručení)
* fragmentace (odesílatelem) 44 ~ z IPv4 -- délka 8 B, jen bit více fragmentů, ID 32 b, všechna záhlaví (i transportní) v prvním, ve všech záhlaví před fragmentačním, fragmenty se nesmí nepřekrývat, jinak zahození
* Obr. PS-2.9
* autentizace (odesílatele, i integrita paketu) AH 51
* šifrování (dat, odesílatelem nebo směrovačem, poslední záhlaví) ESP 50 -- + AH = IPsec
* další volitelné, např. mobilita 135, Shim6 140 aj.
* problém firewally -- neznají hlavičky (měly by), paket zahodí
* adresy (RFC 4291): pro síťové rozhraní více, všichni v LAN stejná (pod)síť, 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. pro router v síti, DNS dotaz nebo HTTP požadavek
* notace 8 čtyřciferných čísel v šestnáctkové soustavě oddělených :, např. 2001:0718:1401:0050:0000:0000:0000:000d, zkrácený (kanonický) zápis (vynechání úvodních 0 a jedné maximální/první posloupnosti více 0 mezi :, malá písmena) 2001:718:1401:50::d, v URL v [] (RFC 3986)
* síťový prefix ~ adresa sítě/maska z IPv4 (maska = počet bitů 1 = délka prefixu, CIDR), např. 2001:718:1401:50::/64
* unicast až 64 b síť: globální (zatím) 2000::/3 (RFC 3587) -- jednoznačné v rámci celého Internetu, dalších 45 b globální (směrovací) prefix sítě: 32 b RIR (má /12, přiděluje /29 až /32, např. RIPE 2001:0600::/29 až 2001:07f8::/29) a 16/24/32 b LIR (přiděluje /48, /56 nebo /64), 16/8/0 b ID podsítě zákazníků (výjimečně ještě pro dvoubodové linky /127)
* Obr. PS-3.1, PS-3.22
* 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 (kvůli směrování mezi podsítěmi se stejnou ID) globální ID, 16 b ID podsítě, dříve fec0::/10 = site local -- v rámci "místní" sítě (54 b ID podsítě, ale problém více "míst" jedné organizace), obdoba (link a unique local rozšíření) vyhrazených rozsahů adres pro privátní sítě z IPv4, NAT netřeba (dostatek globálních adres), ale existuje NPTv6 (RFC 6296, bezstavový obousměrný překlad síťových prefixů)
* pro dokumentace 2001:db8::/32 -- obdobné i u IPv4
* 64 b ID rozhraní (unicast): vlastní (přidělené), náhodné stálé (RFC 7217, posledních 64 b RID = hash síťového prefixu, ID rozhraní a LAN, čítače a tajného klíče), kryptografické (CGA, RFC 3972, z veřejného klíče vlastníka)
* původně modifikované IEEE EUI-64 (= MAC adresa 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), pak navíc náhodné krátkodobé (Privacy Extensions, RFC 4941, problém dočasnosti, návrh polovina stálá) pro odchozí komunikaci
* link local adresy automaticky vždy, často ještě s %ID rozhraní (na linkové vrstvě, tzv. zóny) za
* TODO
* multicast ff00::/8 -- první 4 b druhého byte rozsah skupiny, např. 1 rozhraní, 2 LAN, 5 místo, 8 organizace, E globální, 112 b ID skupiny -- několik typů, vyhrazené adresy např. ff0x::1 broadcast rozhraní/LAN, ff0x::2 směrovače
* anycast z prostoru unicast
* ::1/128 = loopback, ::/128 (0) = neurčená (rozhraní nepřidělena)
* auto konfigurace zařízení (SLAAC): bezstavová (DHCP stav na serveru), "samopřidělení" IP adresy, ID rozhraní náhodné nebo kryptografické (dříve z EUI-64), z oznámení směrovače (RA) získán síťový prefix, adresa brány aj., kontrola jedinečnosti (v LAN) pomocí žádosti o a oznámení o linkové adrese (NS, NA), obdoba u IPv4 rozsah 169.254./16
* zabezpečení RA Guard, SEND (aymetrická kryptografie, CGA adresy), SAVI, access listy na přepínači
* DHCPv6: jako DHCPv4, bezstavové = DNS servery, domény aj., ne adresa, prefix a brána - SLAAC, stavové = vše kromě brány - RA, místo MAC je DUID - identifikace uzlu, 3 typy, využití link local adres
* ICMPv6 (RFC 4443): formát jako u IPv4, zprávy z ICMPv4, nové zprávy, např. "velký paket" nebo "neznámé volitelné záhlaví"
* Neighbor Discovery Protokol (NDP): objevování sousedů ~ "překlad" IPv6 adresy na linkovou adresu (místo ARP a RARP u IPv4) = žádost
* o a oznámení o linkové adrese (neighbor solicitation a advertisement, NS a NA), žádost o a oznámení směrovače (router solicitation a advertisement, RS a RA), povolení SLAAC, aj., speciální multicast ff02::1:ff00:0/104, využití link local adres
* podpora v protokolech (adresy): směrovacích (RIPng, OSPF, IS-IS, BGP, PIM), DNS
* IPsec -- předmět KMI/BEPS
* náročné nasazení: ne "přepnutí Internetu z IPv4 na IPv6", postupný přechod sítí, zpočátku propojených (IPv4) tunely -- 6bone, dnes přímo
* podpora v OS a HW -- certifikace IPv6 Forum program Ready (stříbrné logo základ, dnes už jen zlaté) a u služeb -- program Enabled (web a ISP), i přes podobnost nekompatibilní s IPv4, nové protokoly nezávislé na IPv4
* Obr. PS-1.3
* uživatelé i organizace (i menší ISP) "váhají" s přechodem z IPv4 (slepice vs vejce), nasazují velcí poskytovatelé obsahu a připojení (potřeba mnoha adres) - World IPv6 Launch Day (6. 6. 2012), politická podpora (EU 2002, 2008, např. projekt 6NET, ČR 2009, 2015 ministerstva/eGovernment po IPv6)
* -> dnes (2022) cca 1/4 až 1/3 koncových zařízení celosvětově (ČR 10-15 %)
* přechod z IPv4: dual stack = používání obou
* tunely IPv6 v IPv4: statické tunely tunel server (IPv4 do IPv6 sítě) a tunel broker (registrace na tunel serveru), např. Freenet6, SixXS aj.
* dynamické 6to4 (2002::/16, v LAN 2002:ab:cd::/48 pro veřejnou IPv4 a.b.c.d (16), 6to4 relay do IPv6 sítě na anycast 192.88.99.1, např. NIC.cz), 6over4 a ISATAP (IPv4 adresy součást IPv6 adres v LAN, relay ve firemní síti), Teredo (adresy 2001::/32 v LAN, příp. za NAT, skládající se z IPv4 adresy veřejného serveru, např. u Microsoftu, adresy NAT směrovače a UDP portu, UDP zapouzdření IPv6, veřejný Teredo relay) aj.
* mapování adres mezi IPv6 a IPv4: SIIT (Stateless IP/ICMP Translation, mapovaná ::ffff:a.b.c.d pro IPv4 a.b.c.d a dočasná IPv4 w.x.y.z pro překládané ::ffff:0:w.x.y.z), NAT-PT (Protocol Translation), NAT64 a DNS64 (NAT IPv6 na IPv4 včetně mapování v DNS dotazech (u NAP-PT i pro spojení z IPv4), prefix::a.b.c.d pro IPv4 a.b.c.d), TRT (Transport Relay Translator, transportní proxy z IPv6 do IPv4), BIS (Bump in the Stack), SOCKS64 ("NAT" IPv4 na IPv6 v OS) aj.