

X36PKO IPv6

Obsah

- historie,
- motivace,
- formát datagramu,
- adresace,
- objevování sousedů,
- automatická konfigurace,
- IPsec,
- mobilita.

Historie a požadavky

- počátek 90. let – studie o vyčerpání adres IPv4 během deseti let,
- 1995 – rfc1883 – Steven Deering, Robert Hinden,
- pomalé pronikání do praxe,
- požadavky
 - větší adresní prostor, zvýšení bezpečnosti, QoS, automatická konfigurace, mobilita,
- 1998 – rfc2460.

Formát datagramu

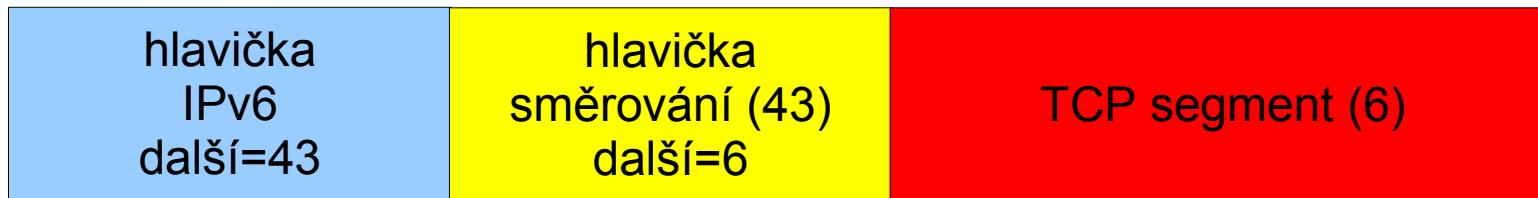
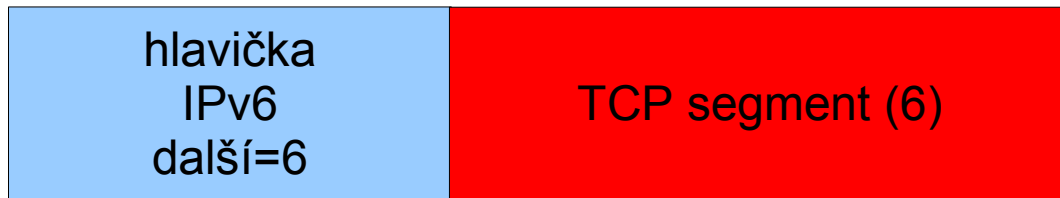
- minimalizace položek,
- konstantní délka hlavičky,
- odstranění přepočítávání kontrolního součtu,
- volitelné položky – samostatné hlavičky,
- upraveno pořadí hlaviček,
- zjednodušení zpracování datagramu,
- koncepce toku.

Formát datagramu II

verze	třída provozu	značka toku	
délka dat		další hlavička	dosah
adresa odesílatele			
adresa příjemce			

- verze – 6
- třída provozu – podpora pro QoS
- značka toku – proud datagramů se společnými vlastnostmi
- délka dat - počet byte za hlavičkou
- další hlavička – hlavička/typ dat následující za hlavičkou
- dosah – obdoba ttl
- oproti IPv4 chybí délka hlavičky (vždy stejná), rozšiřující volby (další hlavičky), kontrolní součet (ponechán nižší vrstvě), fragmentace (přesunuta do dalších hlaviček)

Řetězení hlaviček



Řetězení hlaviček II

- rozšiřující hlavičky
 - 0 volby pro všechny, 43 směrování, 44 fragmentace, 50 šifrování, 51 autentizace, 59 poslední hlavička, 60 volby pro cíl, 62 mobilita.
- typ dat
 - 6 TCP, 8 EGP, 9 IGP, 17 UDP.
- pořadí hlaviček
 - základní hlavička, volby pro všechny, volby pro cíl, směrování, fragmentace, autentizace, šifrování, volby pro cíl (poslední ve směrování).

Fragmentace

- provádí se pouze u odesilatele,
- informace o fragmentaci v rozšiřující hlavičce,
- hlavičky až k fragmentační – nefragmentovatelné,
- doporučené MTU pro IPv6 je 1280B,
- vyhledávání MTU cesty
 - ICMPv6,
 - pravidelné opakování (cca 10min),
 - nemusí se implementovat.

další hlavička	rezerva (0)	posun fragmentu	rez.	M
identifikace				

Jumbogramy

- maximální délka 65535B,
- volba pro všechny - Jumbo obsah – 4GB,
- MTU > 64KB,
- uzly s menším MTU – nemusí jumbogramy podporovat,
- UDP – úprava protokolu (vynulování délky, délku definuje IP vrstva),
- TCP – MSS = MTU – 60.

Adresace

- délka adresy – 128b
- druhy adres
 - individuální (unicast)
 - skupinové (multicast)
 - výběrové (anycast)
- broadcast adresy nejsou podporovány
- zápis adres
 - FEDC:1234:0000:ABCD:0F12:0000:0000:4567
- zkracování
 - FEDC:1234::ABCD:F12:0:0:4567
 - FEDC:1234:0:ABCD:F12::4567
- prefixy
 - FEDC:1234:0000:ABC0:0000:0000:0000:0000/60
 - FEDC:1234:0:ABC0::/60

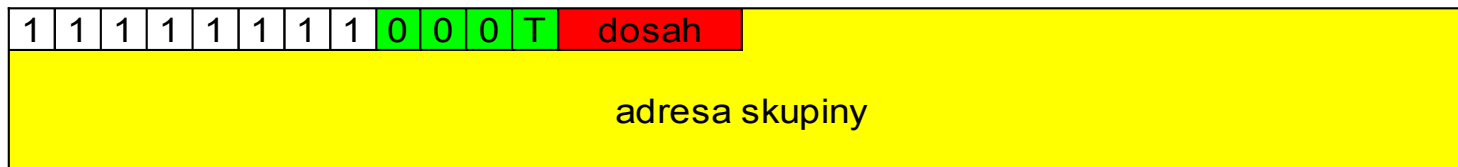
Adresy

- `::/128` nedefinovaná
- `::1/128` loopback
- `FF00::/8` skupinová
- `FE80::/10` individuální lokální linková
- `FEC0::/10` individuální lokální místní - obsolete!
- `FC00::/7` unikátní individuální lokální místní
- ostatní individuální globální (vč. výběrových)

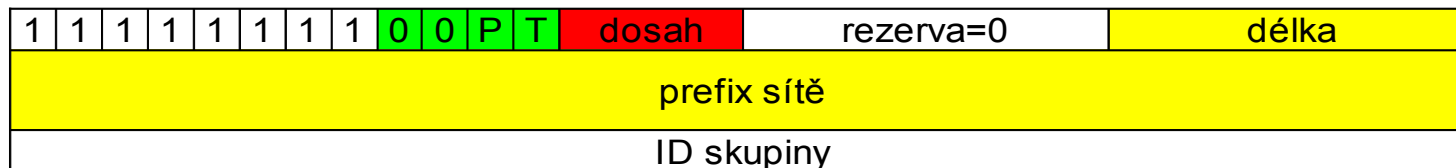
001	globální prefix 45b	subnet 16b	interface ID 64b
-----	------------------------	---------------	---------------------

- identifikátory rozhraní – IEEE EUI-64
- 00:40:D0:7D:6A:86
- 0240:D0FF:FE7D:6A86

Skupinové adresy



- T – 0 dobře známá, 1 dočasná
- dosah – 1 rozhraní, 2 linka, 3 podsít', 4 správu, 5 místo, 8 správu, E globální
 - FF01::101 NTP server na rozhraní
 - FF02::101 NTP servery ve stejné fyzické síti
 - FF05::101 NTP servery v daném místě
 - FF0E::101 NTP servery v Internetu
- skupinové adresy založené na individuálních



Adresy rozhraní

- uzel
 - lokální linková,
 - loopback,
 - individuální a výběrové,
 - skupinová pro všechny uzly,
 - skupinová pro skupiny jejichž je členem,
 - skupinová pro vyzývaný uzel (objevování sousedů).
- směrovač
 - jako uzel,
 - skupinová pro všechny směrovače,
 - výběrová pro směrovače v podsíti,
 - všechny přidělené výběrové adresy.

Objevování sousedů

- rozšířená náhrada ARP
- využívá ICMPv6
 - výzva směrovači, ohlášení směrovače, výzva sousedovi, ohlášení souseda, přesměrování
- poskytuje
 - zjišťování linkových adres v lokální síti
 - rychlou aktualizaci změn a neplatných položek
 - hledání směrovačů
 - přesměrování
 - detekci duplikovaných adres
 - ověřování dosažitelnosti sousedů
 - zjišťování údajů pro automatickou konfiguraci

Hledání linkové adresy

- výzva sousedovi s vyhledávanou IP adresou
- skupinové adresy
 - FF02:0:0:0:0:1:FF00::/104,
 - posledních 24b vyhledávané adresy.
- ohlášení souseda s linkovou adresou
- aktualizace
 - nevyžádané ohlášení na FF02::1 pro aktualizaci cache.
- detekce dosažitelnosti souseda
 - vypršení platnosti,
 - informace z vyšších vrstev,
 - výzva sousedovi,
 - smazání z cache.

Automatická konfigurace

- stavová konfigurace – DHCPv6
- nevyužívá broadcast
- DHCP Unique Identifier (DUID)
 - jednoznačně identifikuje uzel,
 - linková adresa a čas,
 - přiděleno výrobcem,
 - linková adresa.
- Identity Association (IA)
 - jednoznačně identifikuje rozhraní.
- vyhledání všech serverů (FF02::1:2 – adresa agenta)
 - *solicit - advertise*
- oslovení zvoleného serveru podle DUID (FF02::1:2)!
 - *request – reply*
- obnovení *renew, rebind, release, confirm*
- rekonfigurace vyvolaná serverem *reconfigure*

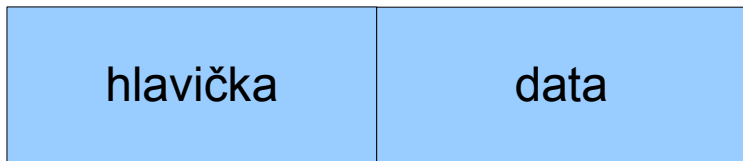
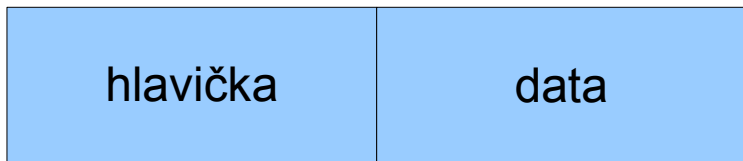
Automatická konfigurace II

- bezstavová konfigurace – nevyžaduje konfiguraci
 - ohlášení směrovače
 - zasílání náhodně každým směrovačem,
 - ICMPv6,
 - životnost implicitního směrovače, maximální počet skoků, stavová konfigurace adres, stavová konfigurace ostatních parametrů, trvání dosažitelnosti, interval opakování,
 - volby
 - linková adresa, MTU, prefix.
 - určení adresy
 - lokální linková adresa,
 - detekce duplicitních adres (objevování souseda),
 - ohlášení směrovače.
 - konfigurace směrování
 - implicitní směrovače,
 - prefixy,
 - cache – ICMPv6 přesměrování.

Bezpečnost

- povinná implementace IPsec
- autentizace
 - Authentication Header (AH)
- šifrování
 - Encapsulating Security Payload (ESP)
- transportní režim
 - vložení bezpečnostních hlaviček
- tunelující režim
 - zabalení datagramu do datagramu s bezpečnostními hlavičkami

Bezpečnost II



Bezpečnostní asociace

- Security Association (SA)
- informace potřebné pro šifrované spojení
 - bezpečnostní protokol (AH, ESP)
 - šifrovací algoritmus
 - klíče
 - čítače
 - doba životnosti
 - ...
- jednosměrná (vytváří se ve dvojicích)
- pro AH i ESP jedna dvojice
- na paket se vztahuje svazek SA

Databáze bezpečnostní politiky

- sada pravidel uplatňovaná na všechny pakety
 - zahodit
 - zpracovat bez IPsec – odeslat, přijmout
 - zpracovat IPsec – databáze vydá svazek SA
- manuální konfigurace
- automatizovaná správa - ISAKMP

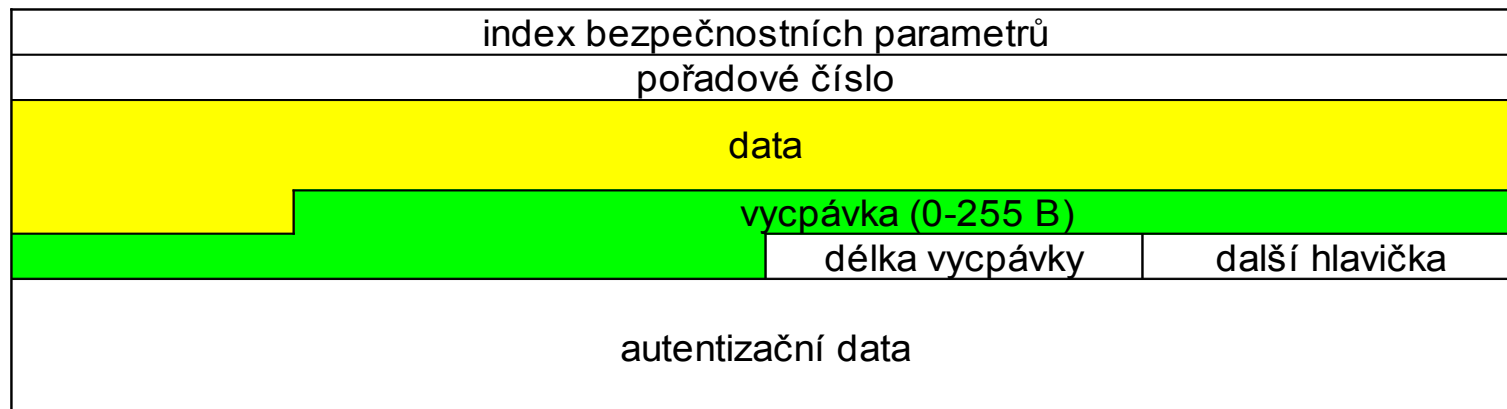
Authentication Header

- slouží pro autentizaci odesilatele
- umožňuje ochranu proti opakování
- postup
 - vložení AH hlavičky
 - vyplnění položek (autentizační data vynuluje)
 - výpočet autentizačních dat (dočasná úprava dat)

další hlavička	délka	rezerva
index bezpečnostních parametrů		
pořadové číslo		
autentizační data		

Encapsulating Security Payload

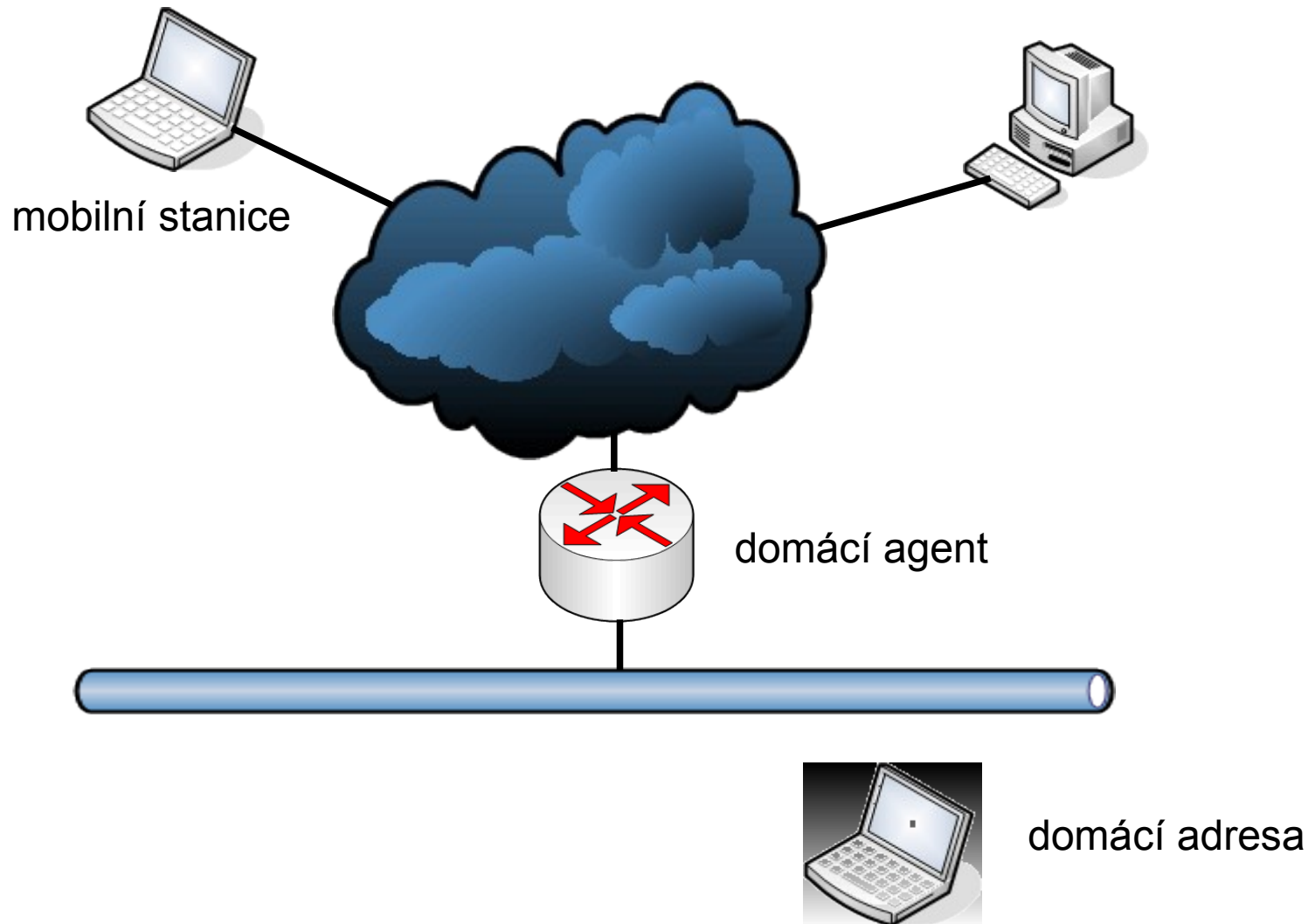
- slouží pro šifrování obsahu (i služby AH)
- data a další hlavičky jsou obsah ESP hlavičky
- postup
 - umístění ESP hlavičky, vycpávky, šifrování
 - vytvoření pořadového čísla
 - vytvoření autentizačních dat (je-li požadována autentizace a kontrola integrity)
- fragmentace až po šifrování



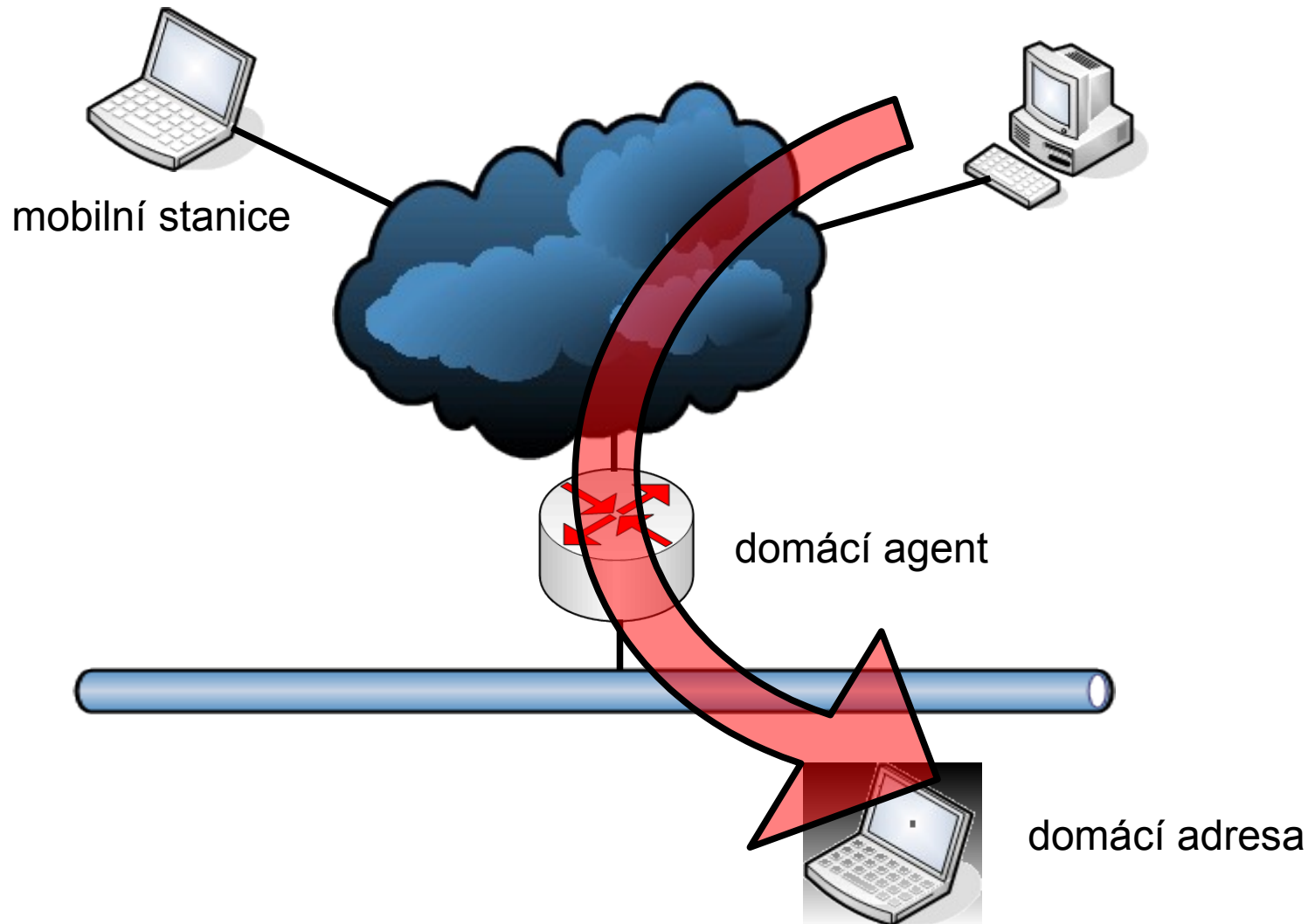
Mobilita

- 6/2004 – rfc3775
- princip domácí adresy a domácího agenta
- vytvoření tunelu mezi mobilním zařízením a agentem
- optimalizace cesty

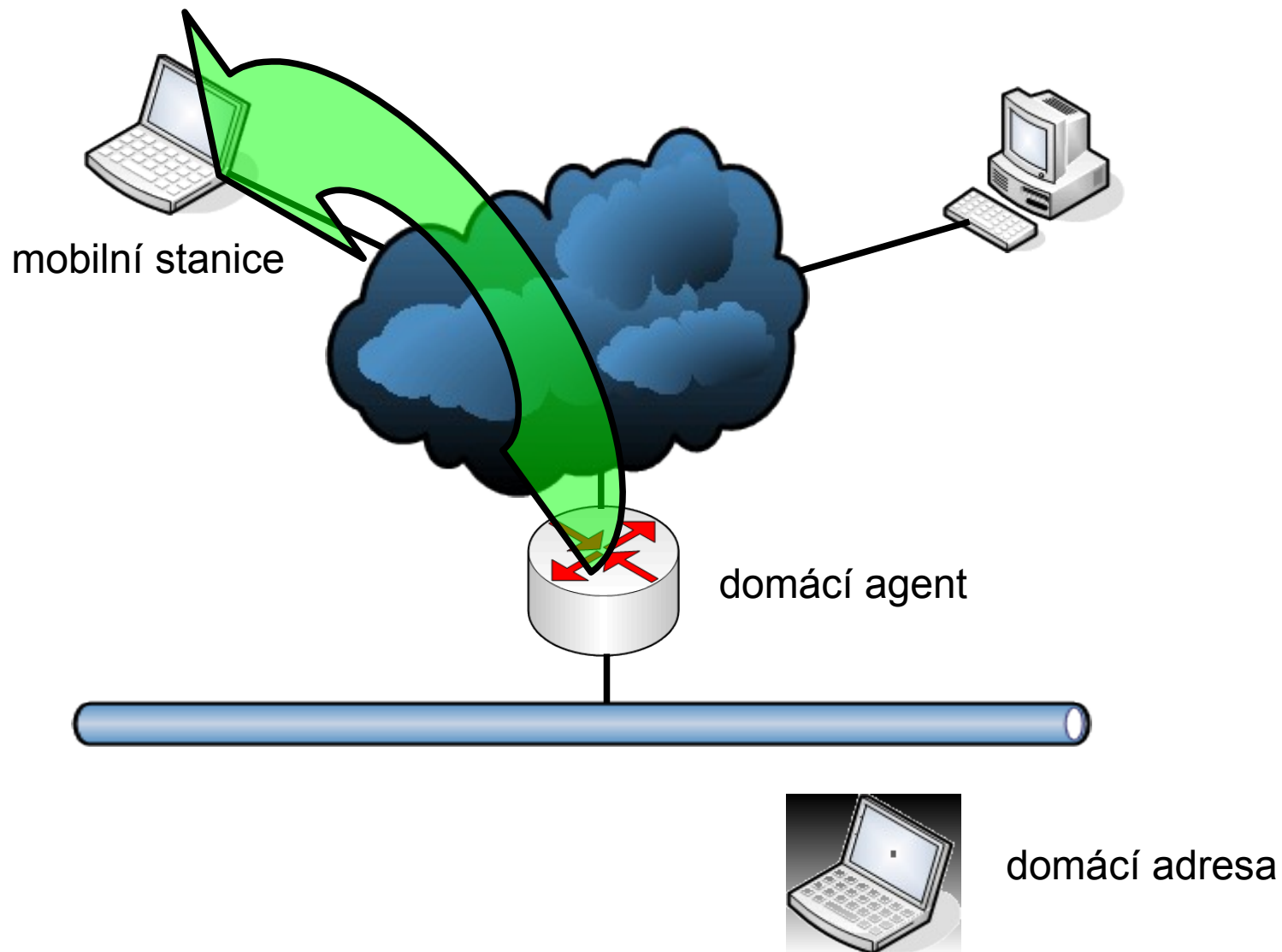
Mobilita



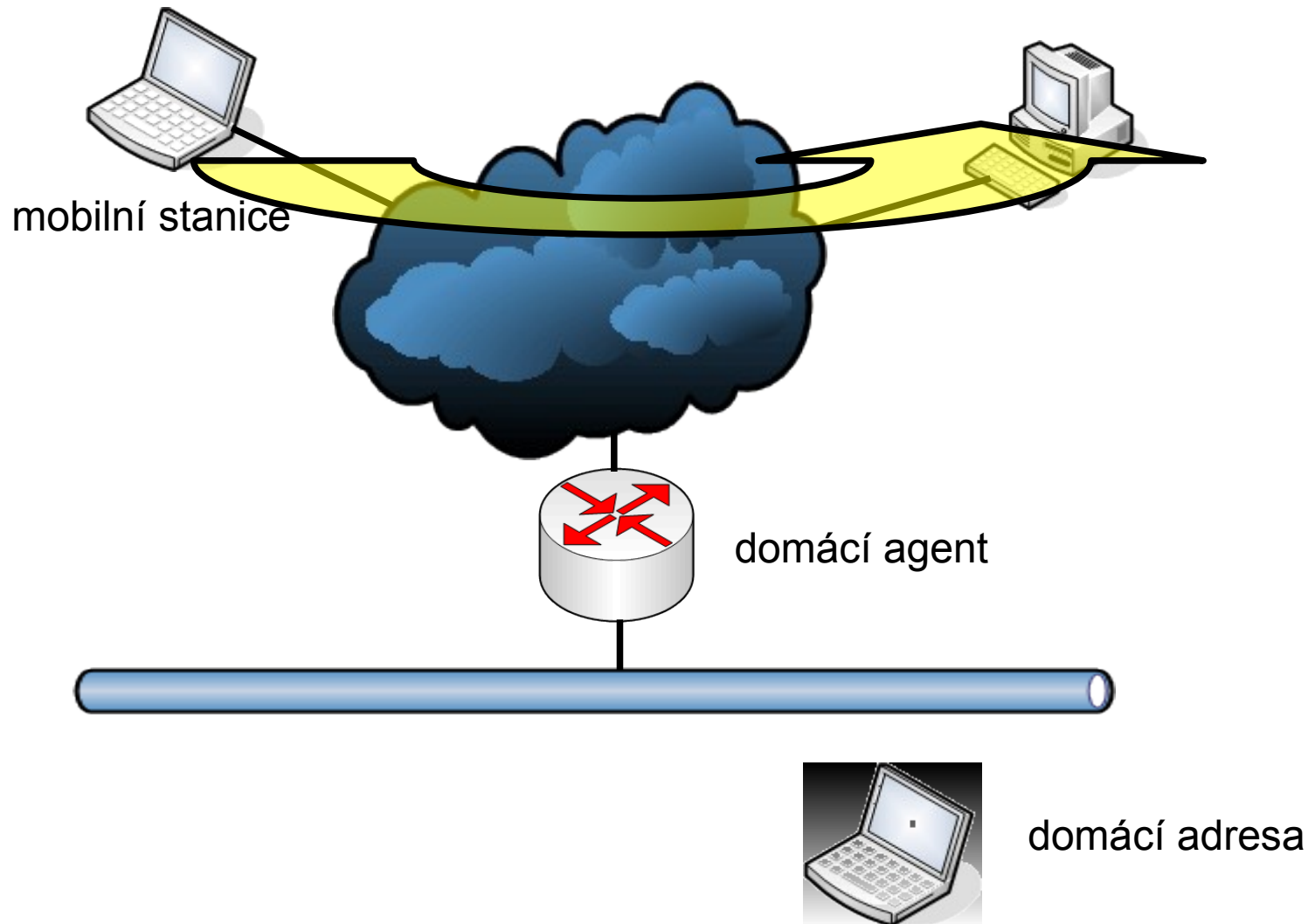
Mobilita otevření spojení



Mobilita vytvoření tunelu



Mobilita optimalizace cesty



multicast
implementace
programové rozhraní
DNS

...