

Počítačové sítě

Pavel.Satrapa@tul.cz

<http://www.nti.tul.cz/~satrapa/>

<http://elearning.tul.cz/>

Literatura (1)

- Andrew S. Tanenbaum: **Computer Networks**
6. vydání, Prentice Hall, 2021
- W. Richard Stevens: **TCP/IP Illustrated, Vol. 1**
Addison-Wesley, 2011
- Eric A. Hall: **Internet Core Protocols**
O'Reilly & Associates, 2000
- Charles E. Spurgeon: **Ethernet**
O'Reilly & Associates, 2014

Literatura (2)

- Mathew S. Geist: **802.11 Wireless Networks**
O'Reilly & Associates, 2005
- Jiří Peterka: archiv článků, zejména seriál
Co je čím v počítačových sítích
<http://www.earchiv.cz/>

Úrovně integrace počítačů

- **Samostatné počítače**

- mohou být víceuživatelské – lze omezeně komunikovat

- **Počítačová síť**

- počítače propojeny, mohou spolupracovat
- zachovávají si vlastní identitu

- **Distribuovaný operační systém**

- skupina počítačů, která se chová jako kompaktní celek
- vnitřní struktura transparentní vůči uživateli

Využití sítě

- sdílení prostředků
- komunikace
- vyšší spolehlivost
- úspora nákladů

Sdílení prostředků

- **periferie**

- drahé a zřídka používané
- velkoplošný plotter, zálohovací zařízení apod.

- **kapacity**

- výpočetní – uživatelský počítač zajišťuje grafické rozhraní, náročné výpočty provádí vzdálený stroj
- úložné – cloudy a spol.

- **datové soubory**

- sdílené databáze

Komunikace

- **mezi uživateli**

- elektronická pošta, chat, videokonference, hry,...
- snadný kontakt i na velké vzdálenosti

- **mezi programy**

- distribuované aplikace – řešení společného úkolu
- rezervační systémy

Vyšší spolehlivost

- **zálohování**

- běžně se zálohuje na vzdálená specializovaná zařízení
- páskové jednotky, hierarchická úložiště,...

- **redundance**

- u síťové služby nepoznáte, který stroj službu poskytuje – může jich být víc, výpadek jednoho nemá vliv
- ochrana proti rizikům – nutno zvážit: pravděpodobnost rizika, jeho následky a cenu ochrany

Úspora nákladů

- **vysoký výpočetní výkon levněji**
 - u špičkových technologií roste cena mnohem rychleji než výkon
 - superpočítače se pohybovaly na hraně možností
 - hejno menších počítačů podá vyšší výkon levněji
 - klastry a gridy
 - nutné paralelní algoritmy

Local Area Network – LAN

- malý rozsah – místnost až areál
- vlastní kabeláž (kroucená dvojlinka, optické vlákno, bezdrátová síť)
- vysoké rychlosti 10 Mb/s až 100 Gb/s
- nízká chybovost (u drátěných)
- původně zejména pro sdílení prostředků
- např. LIANE

Wide Area Network – WAN

- dálková – oblast až planeta
- pronajatá kabeláž (přenosové služby, optická vlákna, mikrovlnné trasy, satelity)
- velké rozpětí rychlostí, 65 kb/s až 100 Gb/s
- chybovost závislá na technologii
- původně pro vzdálený přístup a komunikaci mezi uživateli
- např. CESNET2

Struktura sítě

- **komponenty**

- připojené počítače a zařízení
- spoje (linky, kanály)
- aktivní (přepojovací) prvky

- **topologie**

- vzájemné uspořádání komponent
- vychází z vlastností použitých spojů (dvoubodové/sdílené)

Nejběžnější topologie

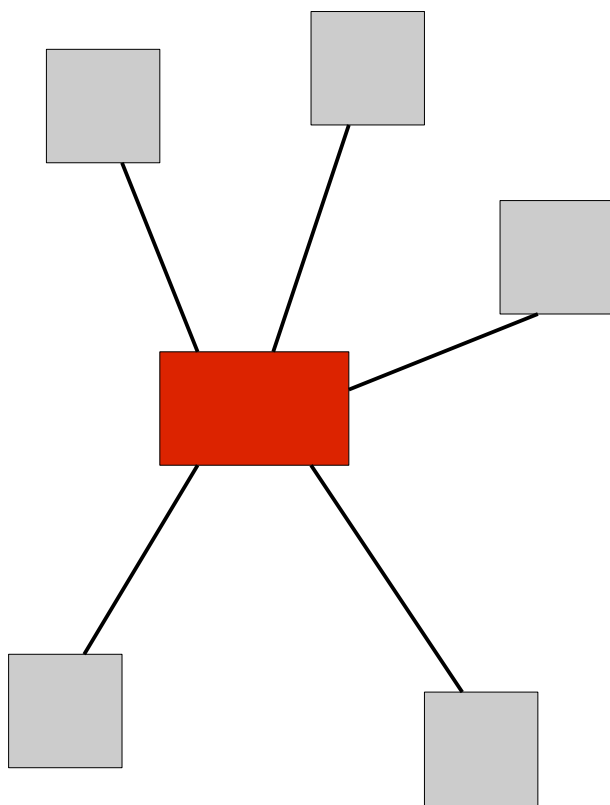
- **dvoubodové spoje**

- hvězda
- kruh
- strom
- obecný graf

- **sdílené spoje**

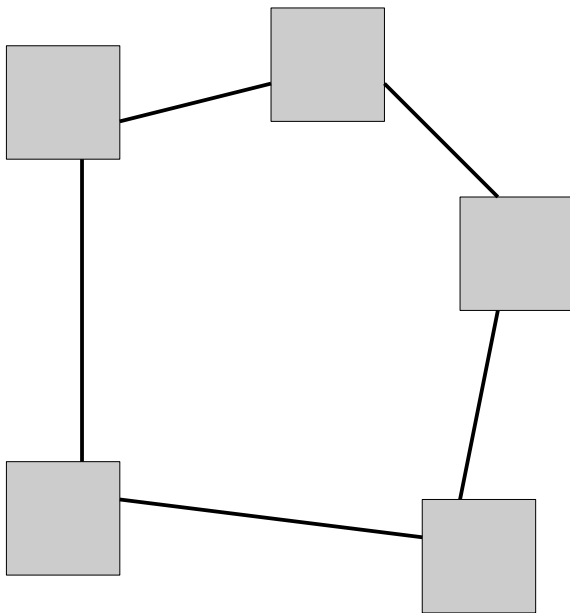
- sběrnice
- s centrálním vysílačem

Hvězda



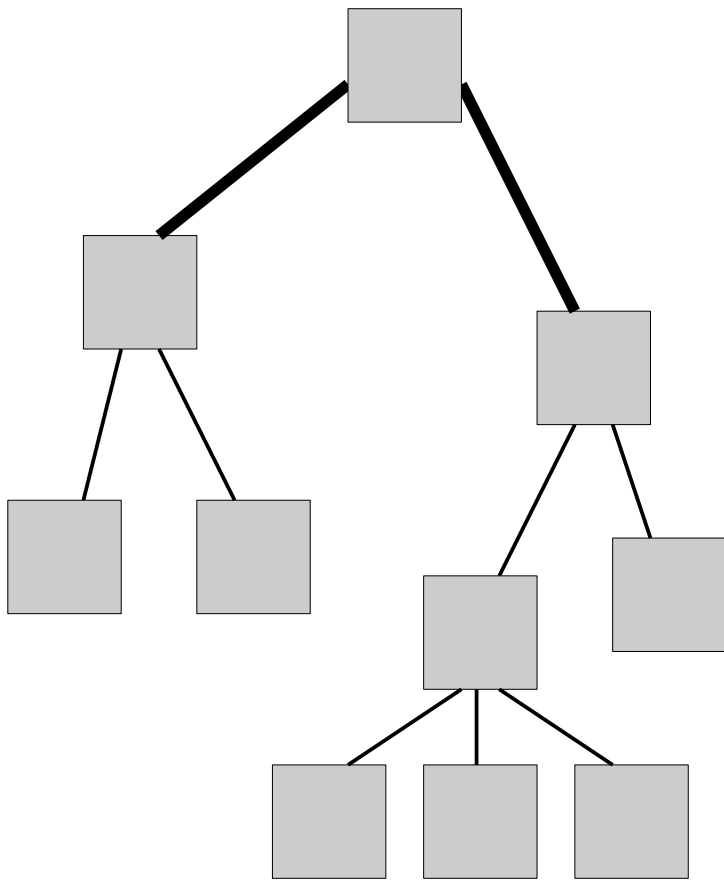
- výpadek kabelu odstaví jediný počítač
- lze oddělený provoz
- lze paralelní provoz
- spousta kabelů
- výpadek středu fatální
- Ethernet na kroucené dvojlince

Kruh



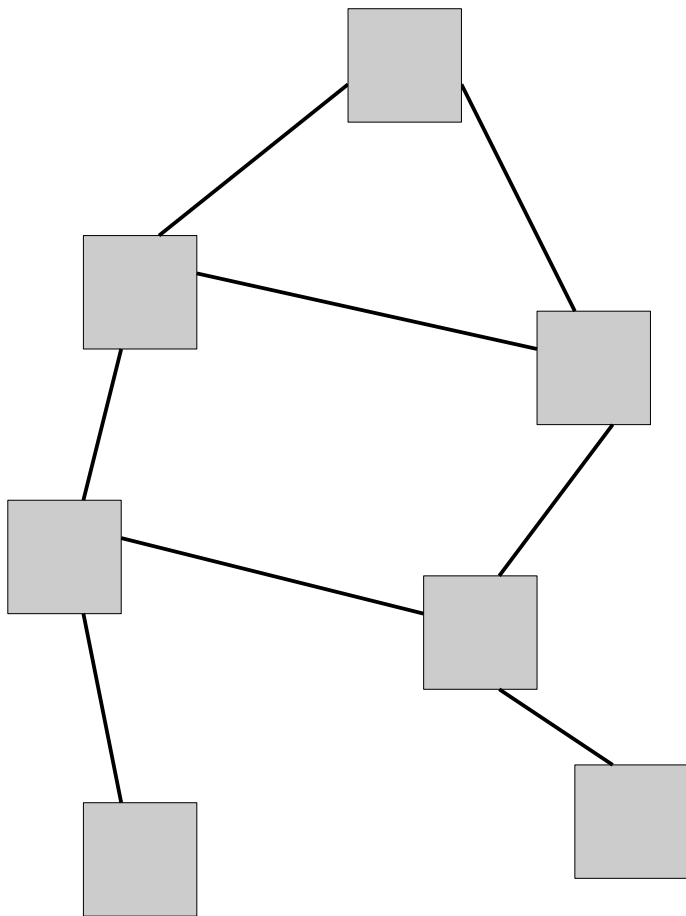
- triviální následnictví – jednoduché protokoly
- výpadek kabelu fatální
- nepružné
- Token Ring, FDDI

Strom



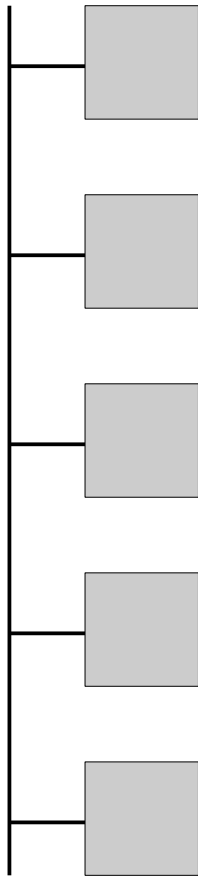
- zobecnění hvězdy
- běžný ve středně velkých sítích
- lze oddělovat provoz
- výpadkem kabelu/uzlu se rozpadne
- reálný výkon závisí na topologii
- Ethernet na kroucené dvojince

Obecný graf



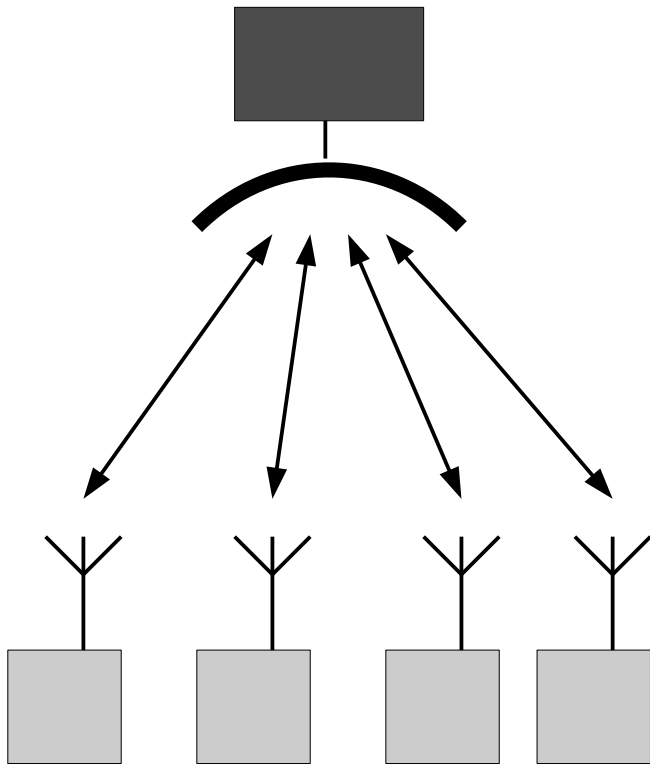
- zpravidla redundantní
 - odolné proti výpadku
 - lze rozkládat provoz
- větší nároky na aktivní prvky – musí hledat cestu
- typický pro WAN

Sběrnice



- jednoduché a pružné
- málo drátů
- výpadek kabelu rozdělí
(v lepším případě)
- Ethernet na koaxiálním kabelu

S centrálním vysílačem



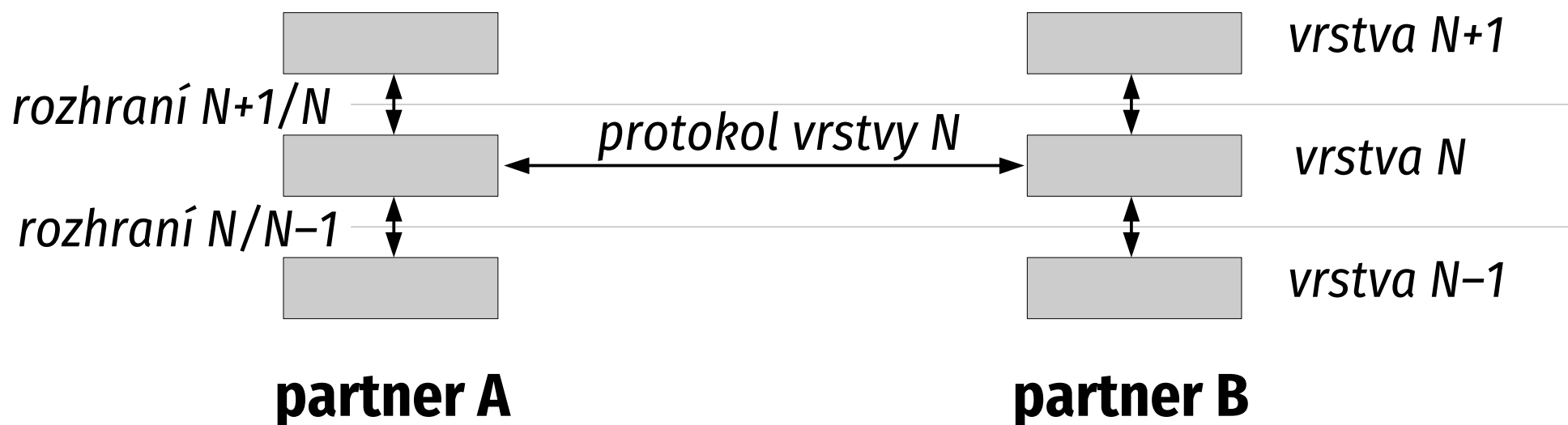
- satelitní či bezdrátová síť
- jako sdílená hvězda
- účastníci se neslyší přímo
- nepotřebuje kabelovou infrastrukturu
- výpadek centra fatální
- satelit má velké zpoždění – nevhodné pro interaktivní práci

vytvořeno s podporou
projektu ESF



Architektura sítě (1)

- zpravidla organizována do úrovní (vrstev)
- jedna vrstva řeší vždy vymezenou část problému
- rozkládá komunikaci na jednodušší podproblémy



Architektura sítě (2)

■ protokol

- jak se domlouvají dva partneři na stejné vrstvě (hlavičky, dotazy, odpovědi, příkazy,...)
- nezávislý na implementaci, umožňuje interoperabilitu

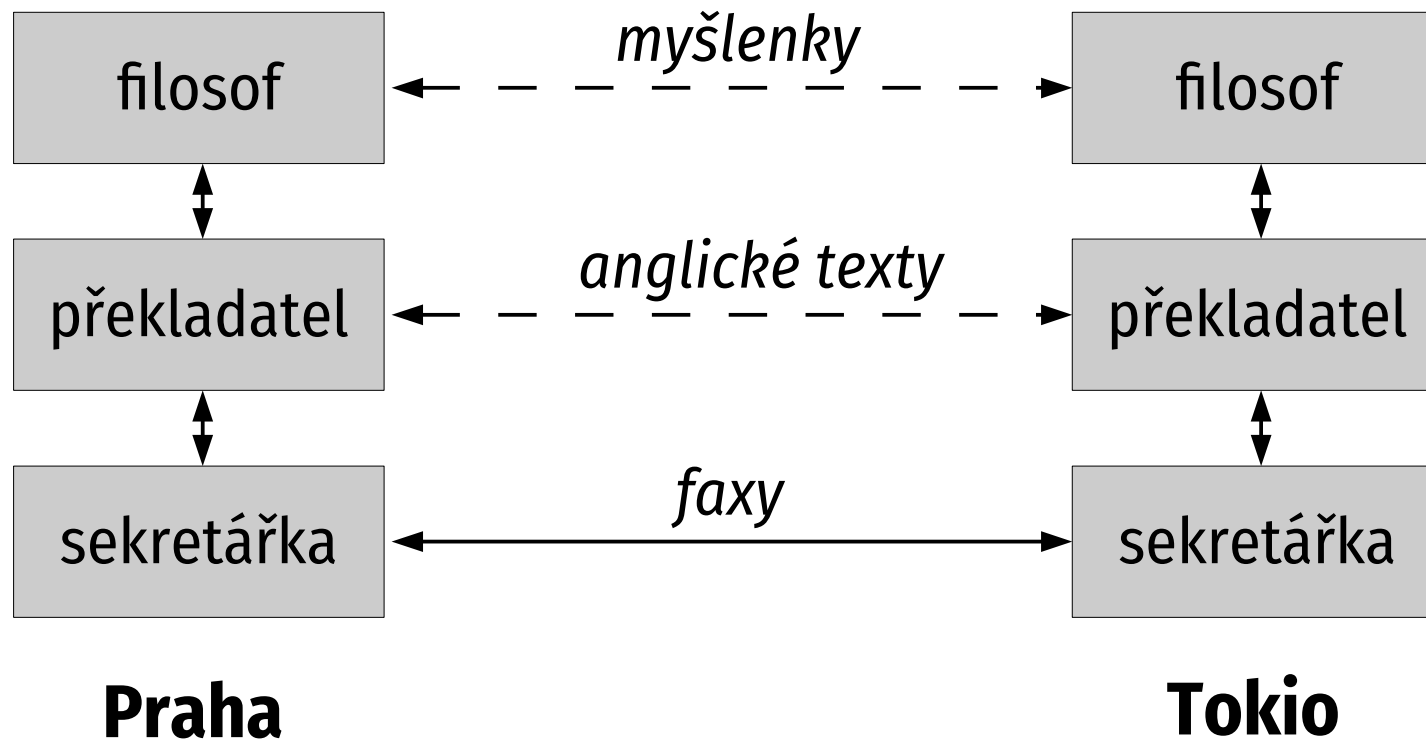
■ rozhraní

- definice služeb nabízených nadřízené vrstvě
- implementace je skryta uvnitř vrstvy
- rozhraní závisí na implementaci (OS)

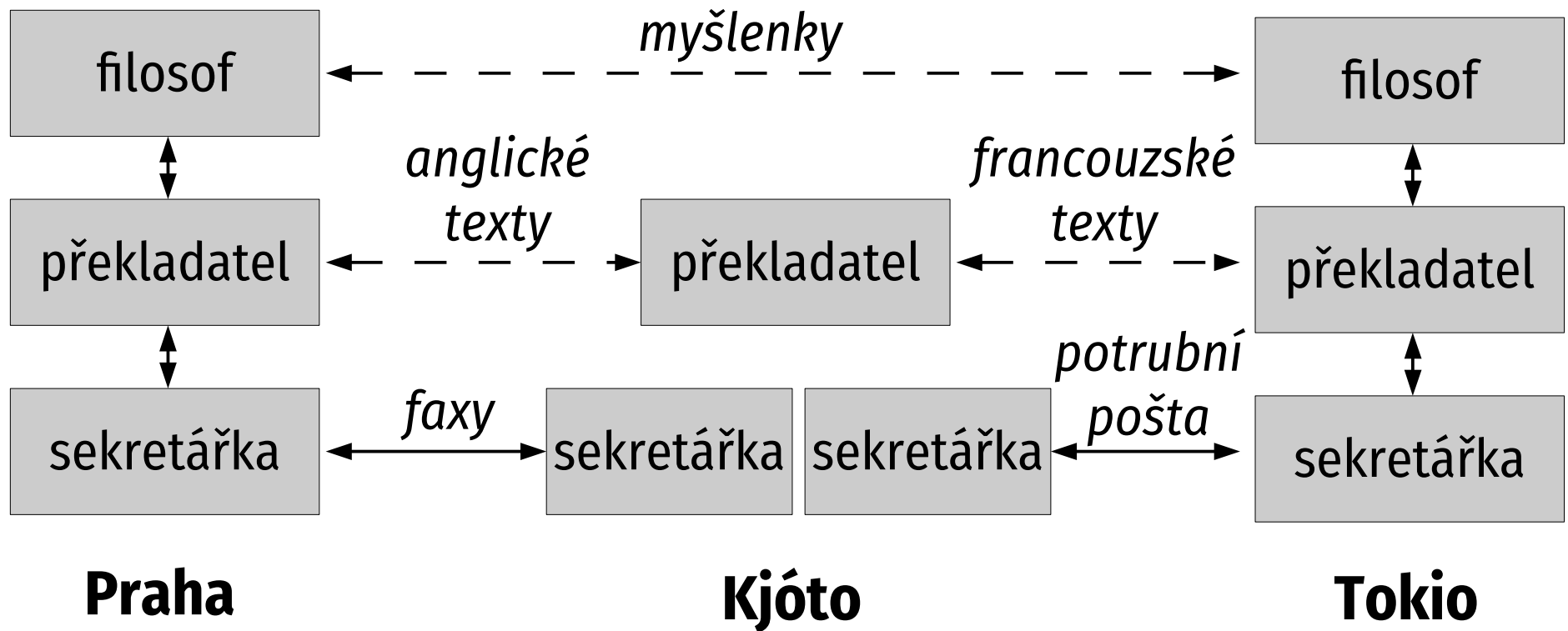
Vlastnosti vrstvené architektury

- navzájem komunikují komponenty ve stejné vrstvě
- vytvořené zprávy předávají k doručení podřízené vrstvě (skutečný přenos zajišťuje nejnižší vrstva)
- od vyšší vrstvy dostávají data k doručení (nerozumí jim)
- vrstvy jsou navzájem nezávislé – změna protokolu v jedné z nich se ostatních nedotkne

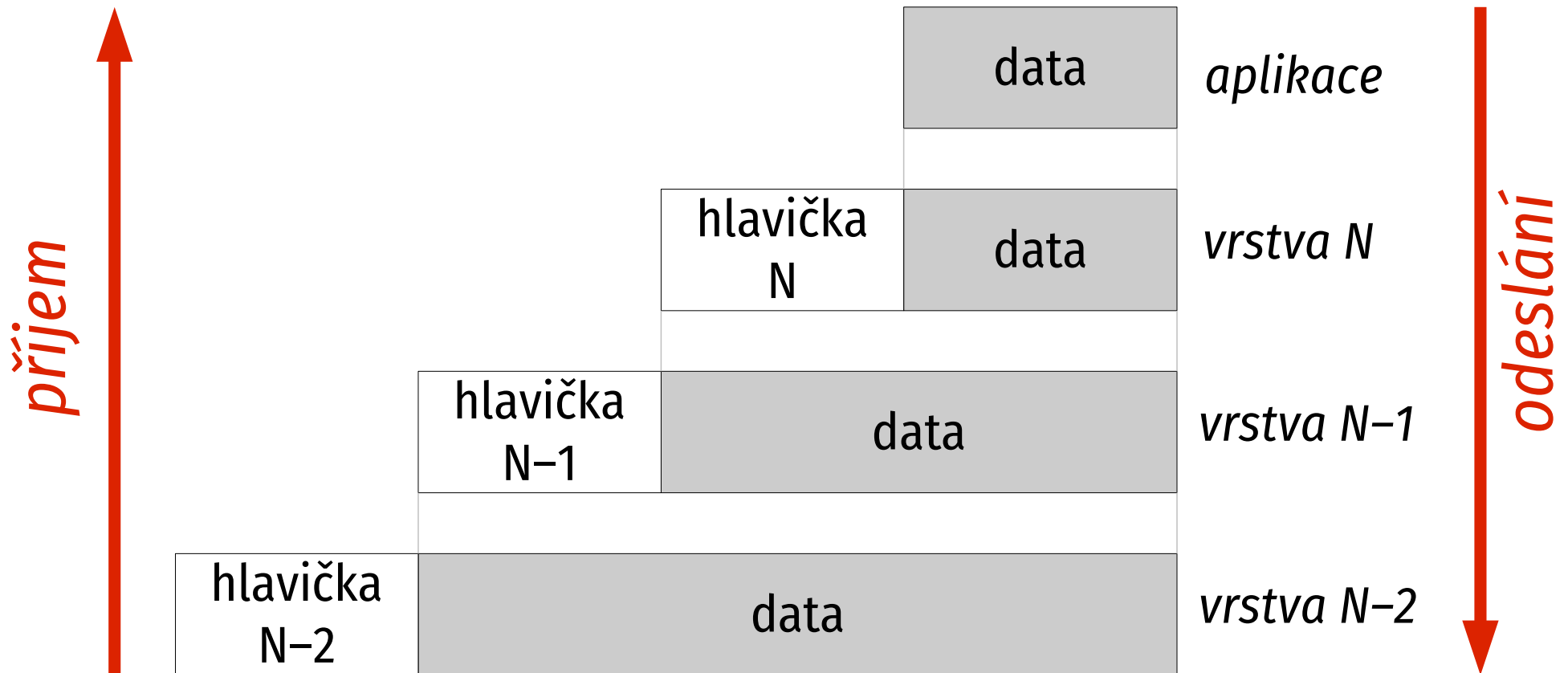
Příklad: Rozmluva filosofů



Překrytí rozdílů v nižších vrstvách



Přidávání/odebírání hlaviček



Referenční model OSI

- **Open Systems Interconnection**
- vytvořila ISO v roce 1983
- cíl: sada standardních komunikačních protokolů nezávislých na výrobci
- 7 vrstev
 - kompromis mezi složitostí vrstev a jejich počtem
- nejsou konkrétní protokoly, jen vymezení funkcí

Vrstvy OSI RM (1)

1) Fyzická (physical)

- vlastní přenos bitů
- mechanické, elektrické a procedurální záležitosti
- konektory, kabely, napětí, kódování signálu,...

2) Spojová (data link)

- řízení a logika přenosu
- paketizace, pravidla přístupu k médiu, detekce chyb,...

Vrstvy OSI RM (2)

3) Síťová (network)

- směrování (hledání cest, vyvažování zátěže)
- řízení sítě (např. účtování)

4) Transportní (transport)

- implementována v počítači, může přizpůsobit vlastnosti sítě (vrstev 1–3) potřebám aplikace
- rozlišení aplikací
- zpravidla bezchybný kanál zachovávající pořadí
- správa spojení

Vrstvy OSI RM (3)

5) Relační (session)

- doplňuje drobnosti (přidána později)
- přátelské ukončení spojení
- řízení dialogu (poloduplex), aktivity, synchronizační body

6) Prezentační (presentation)

- zabývá se významem přenášených dat
- jak reprezentovat data a struktury (ASN.1) a jak je přepravovat (BER.1)
- kódování dat (ASCII, UTF), šifrování, komprimace,...

Vrstvy OSI RM (4)

7) Aplikační (application)

- protokoly konkrétních služeb a aplikací
- elektronická pošta, přenos souborů, vzdálený přístup,...

Protokoly OSI RM

- definovány později podle pravidel OSI RM
- X.25 – síťová vrstva
- X.400 – elektronická pošta
- X.500 – certifikáty (jeden z mála úspěšných)

Problémy OSI RM

- v 80. letech všeobecně považováno za budoucnost sítí, oficiálně podporováno vládou USA
- přesto neuspělo
 - schizma mezi spojovanými a nespojovanými službami
 - nekompatibility různých verzí
 - nepružné procedury, pomalý vývoj
 - nedostatek a vysoká cena implementací
 - zůstalo jako obecný model

Spojované/nespojované služby

- **spojované služby (connection oriented)**
 - naváže spojení, jím pak protékají data (à la telefon)
 - menší nároky
 - dodržuje pořadí
- **nespojované služby (connectionless)**
 - každý paket přepravován samostatně (à la dopisy)
 - pružnější a robustnější, reaguje na změny v síti
 - univerzálnější
 - lépe odpovídá charakteru sítí

OSI RM versus Internet (TCP/IP)



Architektura Internetu (1)

- **existující nižší vrstvy**
 - nemá cenu vynalézat kolo
 - proměnlivé v čase (stejně jako hardware a OS)
- **vrstva přizpůsobení médiu**
 - jak přenášet IP po dané technologii nižší vrstvy
 - nová technologie – stačí definovat, jak po ní přepravovat IP a lze ji používat

Architektura Internetu (2)

■ **síťová vrstva**

- Internet Protocol (IP) – nespojovaný, bez záruk
- společný jazyk celého Internetu (interoperabilita)

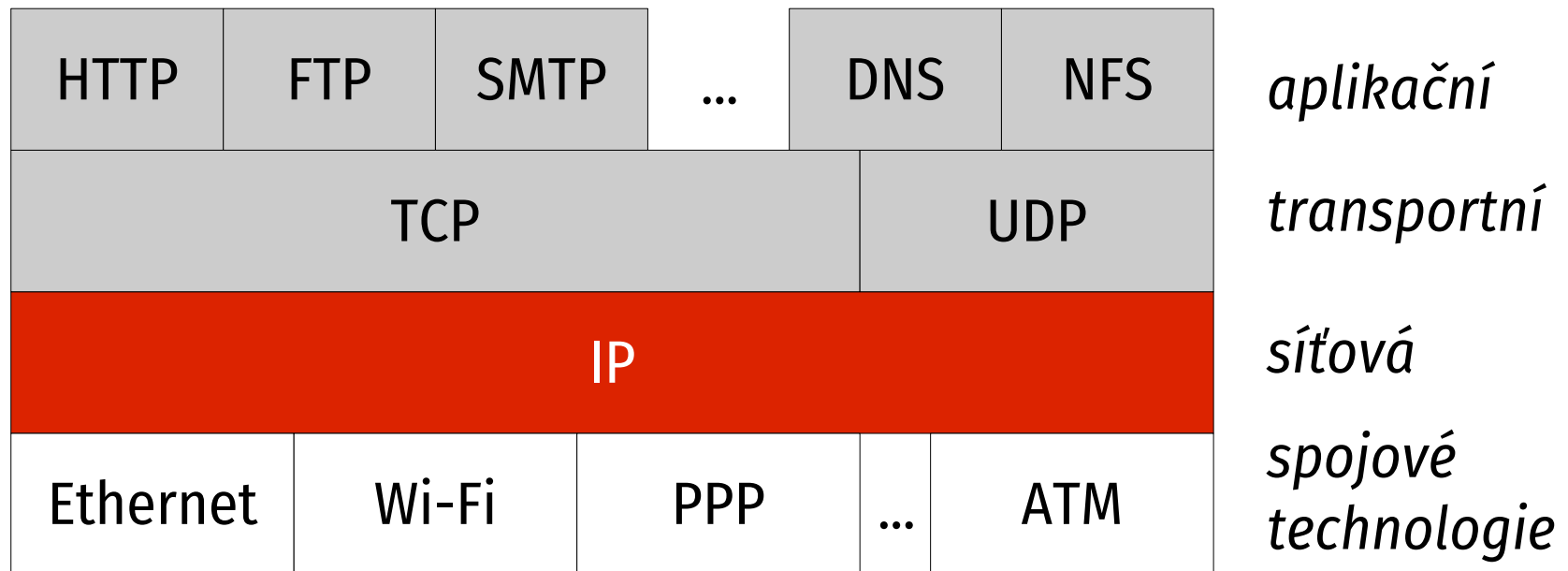
■ **transportní vrstva**

- přizpůsobuje služby potřebám aplikace
- Transmission Control Prot. (TCP) – spojovaný, spolehlivý
- User Datagram Protokol (UDP) – nespojovaný, bez záruk

■ **aplikační vrstva**

- protokoly konkrétních služeb

Rodina TCP/IP



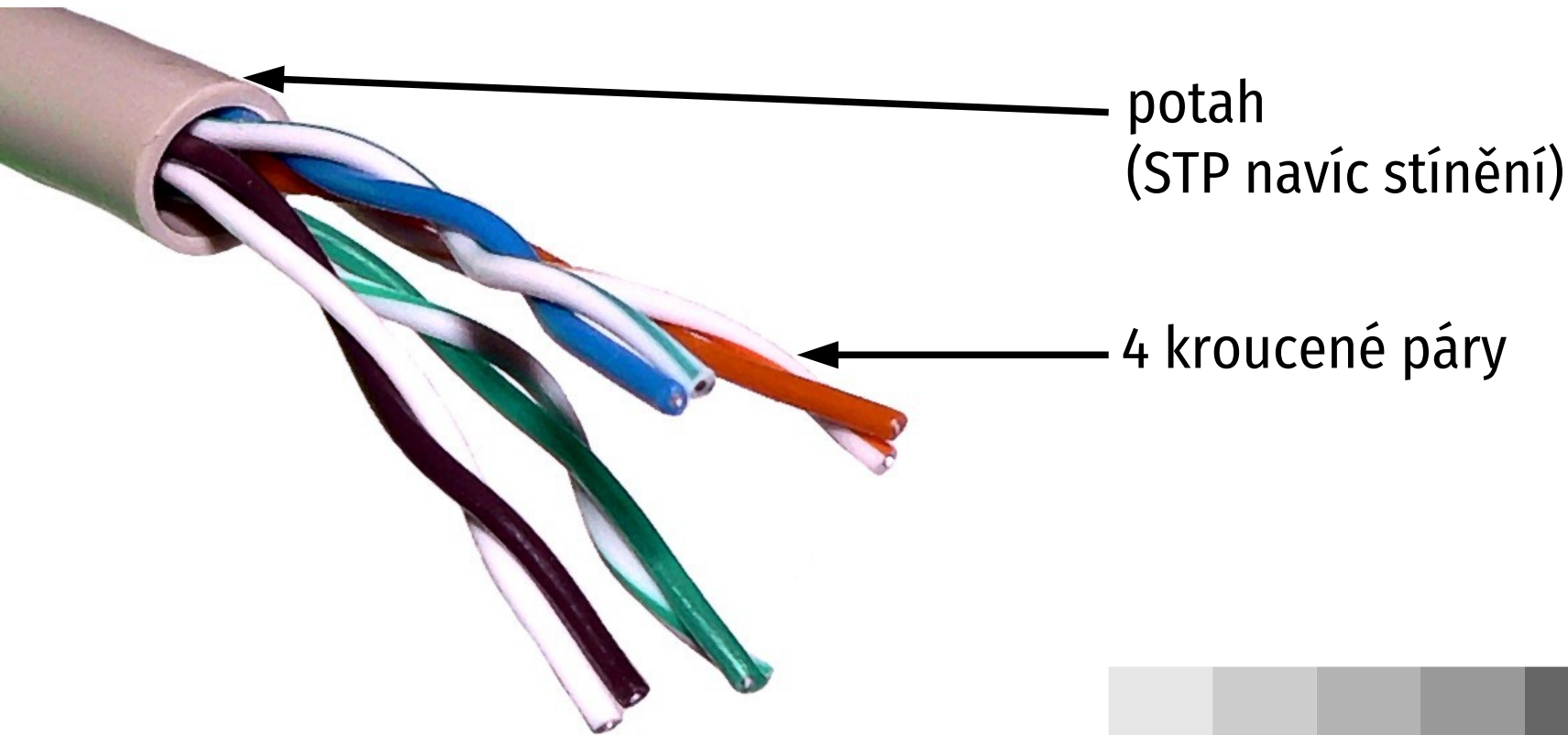
vytvořeno s podporou
projektu ESF



Fyzická vrstva

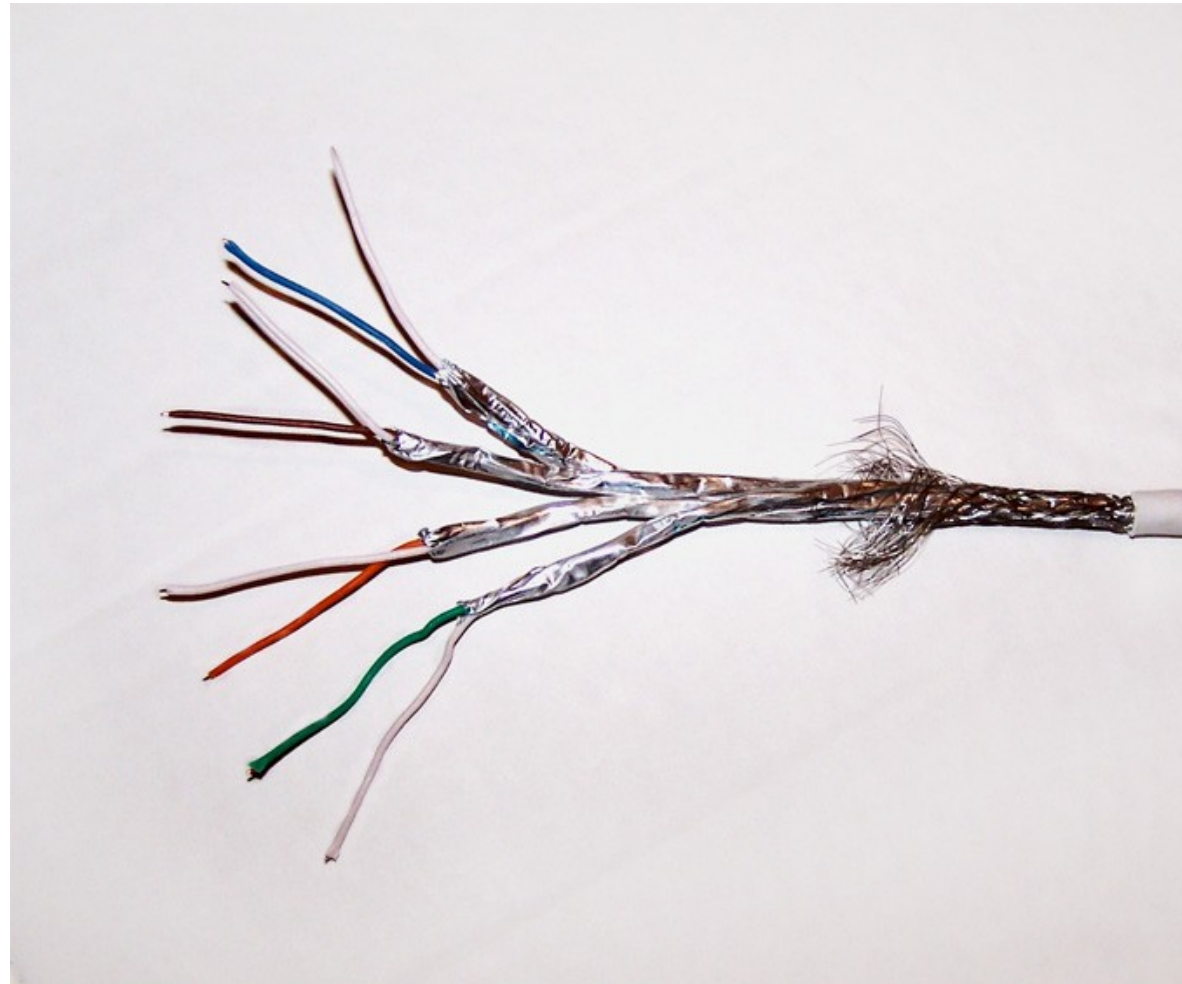
Kroucená dvojlinka

- původně telefonní kabel, pro sítě začalo používat IBM (Token Ring)
- kroucením sníženo rušení



Kroucená dvojlinka

- dva typy:
 - nestíněná – **Unshielded Twisted Pair (UTP)**
výrazně častější
 - stíněná – **Shielded Twisted Pair (STP)**
vnitřní a/nebo
vnější stínění



Charakteristiky

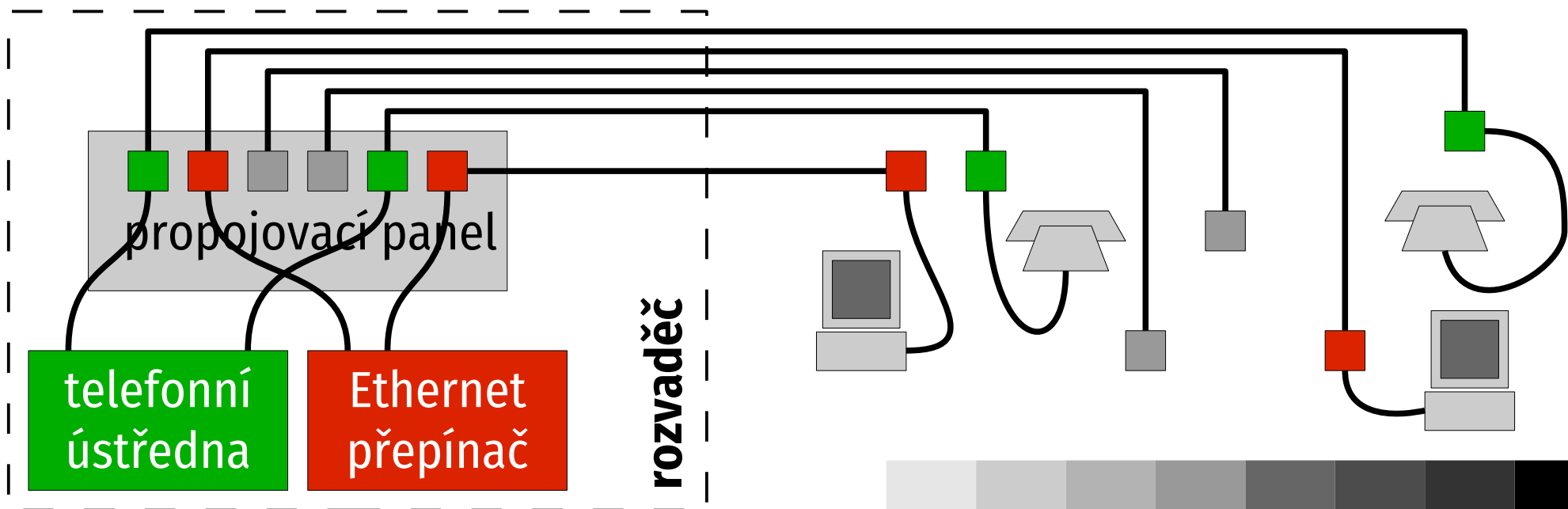
- typicky dvoubodový spoj
 - hvězdy, stromy
 - kruhy
- velmi populární, standardní médium současnosti

Kategorie

- vyjadřují kvalitu – fyzikální vlastnosti a použitelné přenosové rychlosti
 - **5** – do 100 MHz, 100 Mb/s (omezeně 1 Gb/s)
 - **5e** – do 100 MHz, 1 Gb/s
 - **6** – do 250 MHz, 1 Gb/s (omezeně 10 Gb/s)
 - **6a** – vnější stínění, do 500 MHz, 10 Gb/s
 - **7** – plně stíněná, do 600 MHz, 10 Gb/s, nepoužívá se
 - **8** – do 2 GHz, 25 a 40 Gb/s, dosah 30 m

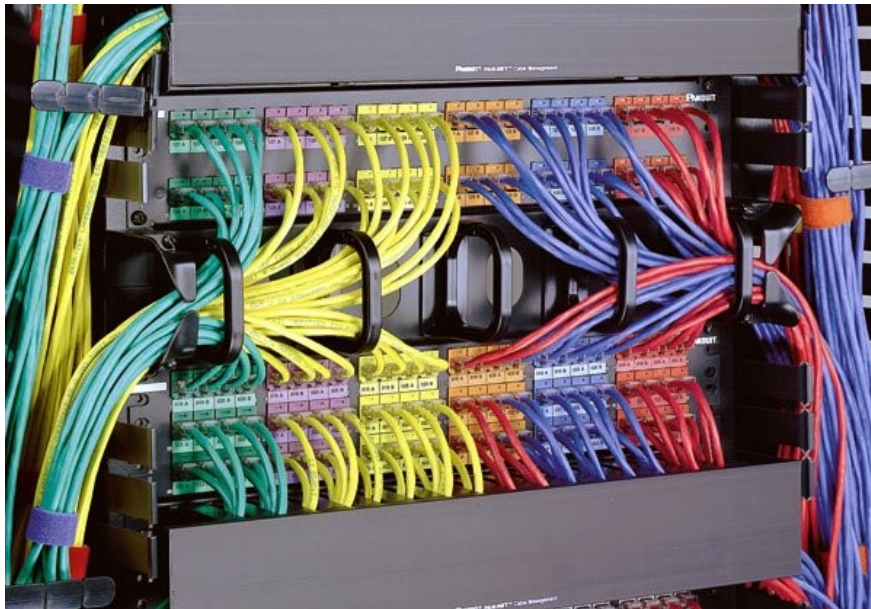
Strukturovaná kabeláž

- společná UTP kabeláž pro data a telefony
- svedena do jednoho centra, umožňuje pružně přepojovat a přizpůsobovat topologii potřebám
- zásuvka se může stěhovat s uživatelem



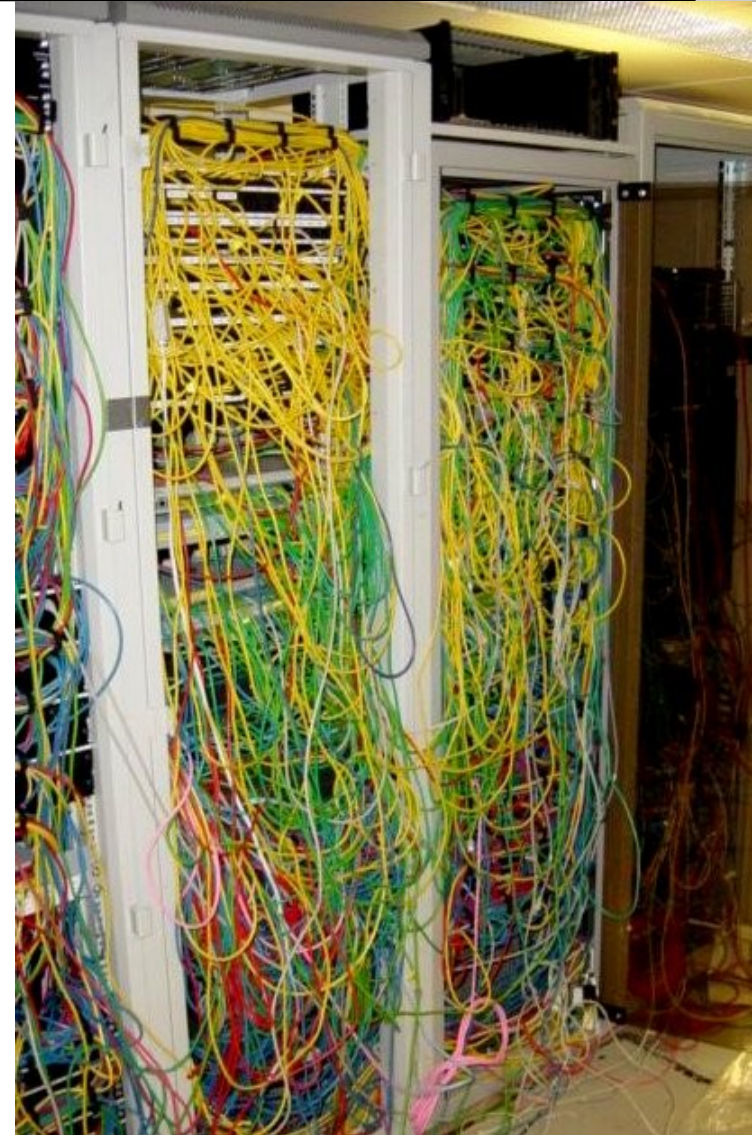
Strukturovaná kabeláž

ideál

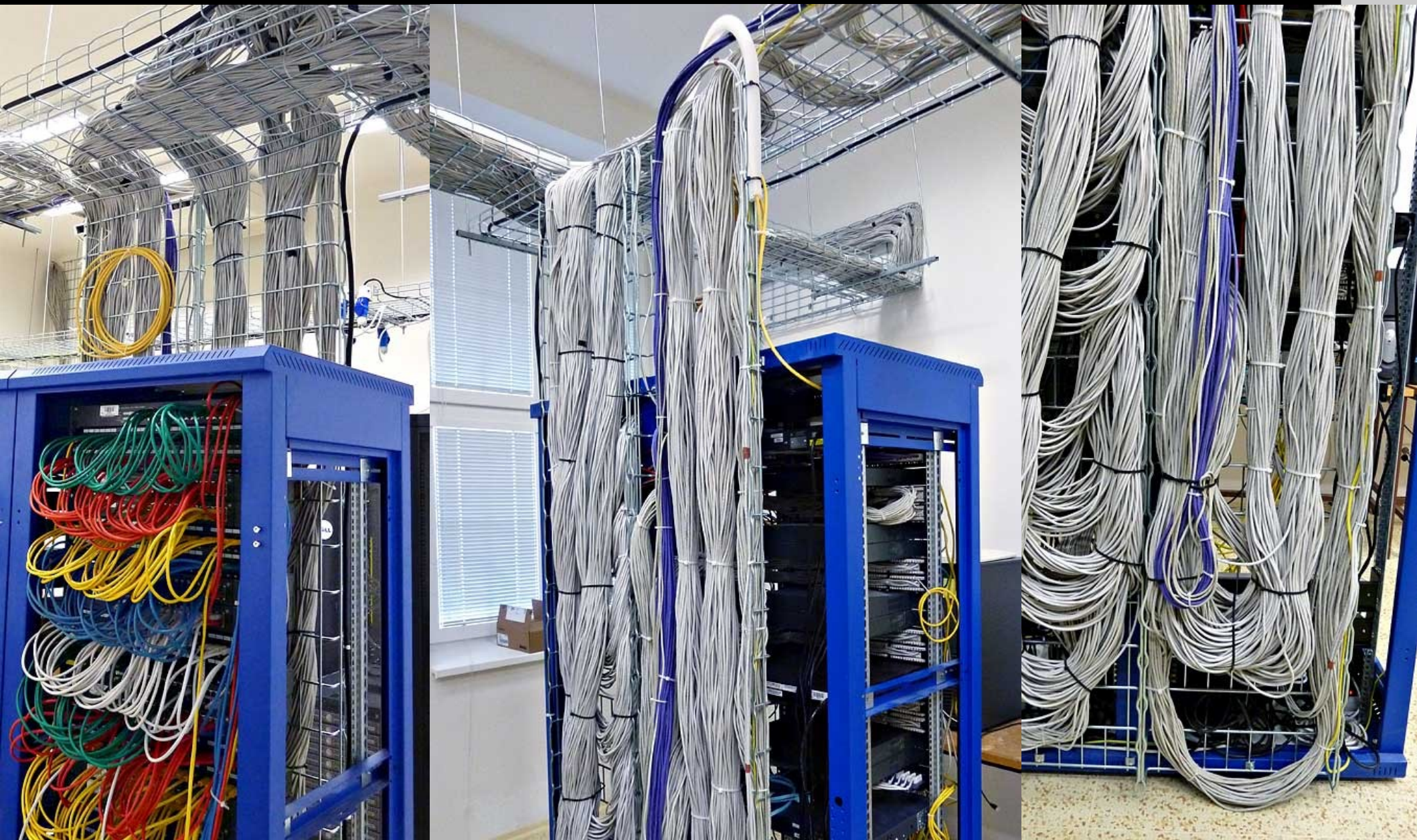


versus

realita

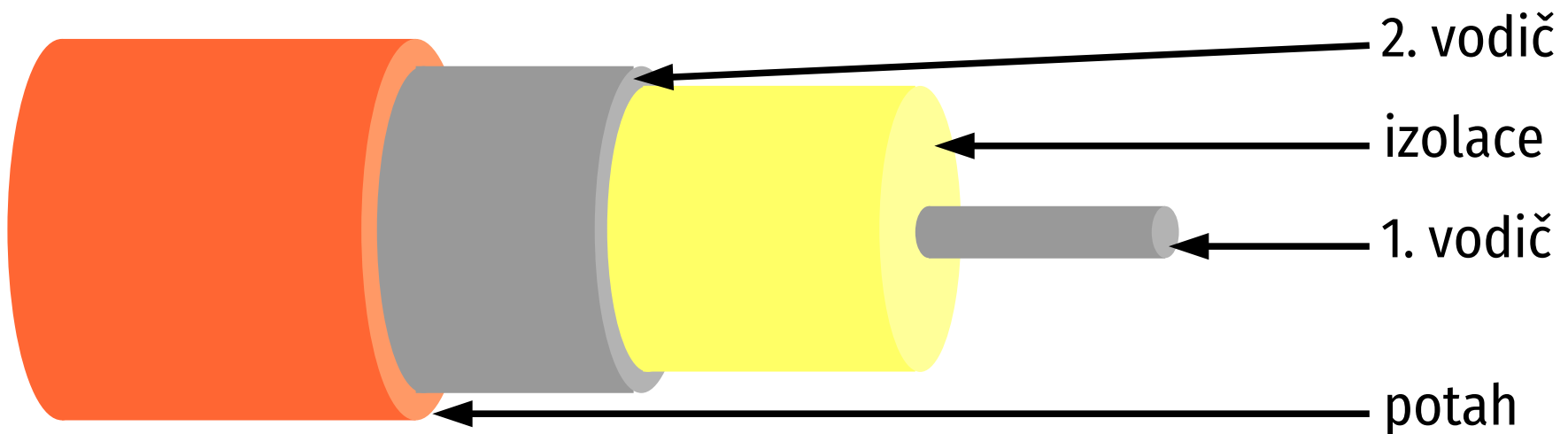


Příklad: budova A



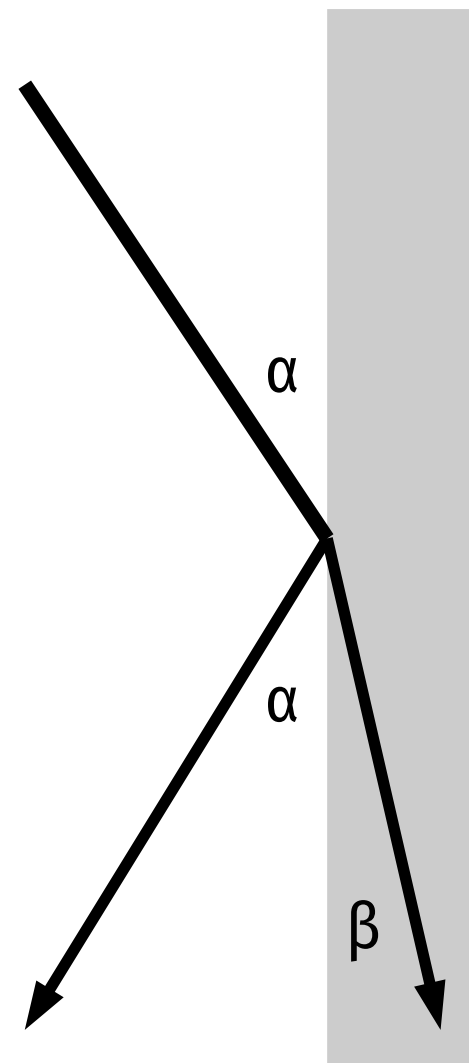
Koaxiální kabel

- typicky 50 Ohmů
- svého času populární, dnes historie
- velká šířka pásma, nízký šum
- rychlosti kolem 10 Mb/s na 1 km



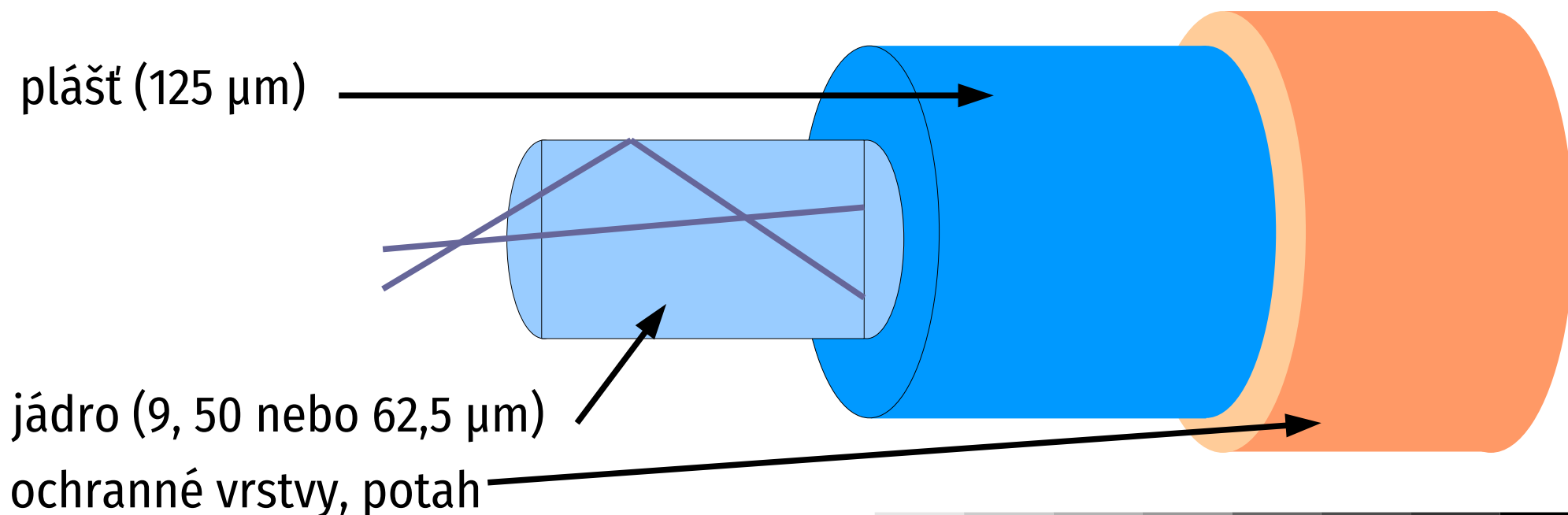
Dopad a lom světla

- znáte ze středoškolské fyziky
- úhel odrazu α roven úhlu dopadu
- úhel lomu β závisí na úhlu dopadu a poměru indexů lomu obou prostředí
- při vhodném poměru indexů lomu leží β v původním prostředí – žádné světlo nepronikne do druhého prostředí
- princip optického vlákna



Optické vlákno

- dvě vrstvy (jádro a plášť) z materiálů s vhodnými indexy lomu – světlo se udrží uvnitř jádra
- uvádí se průměr jádra a jeho pláště

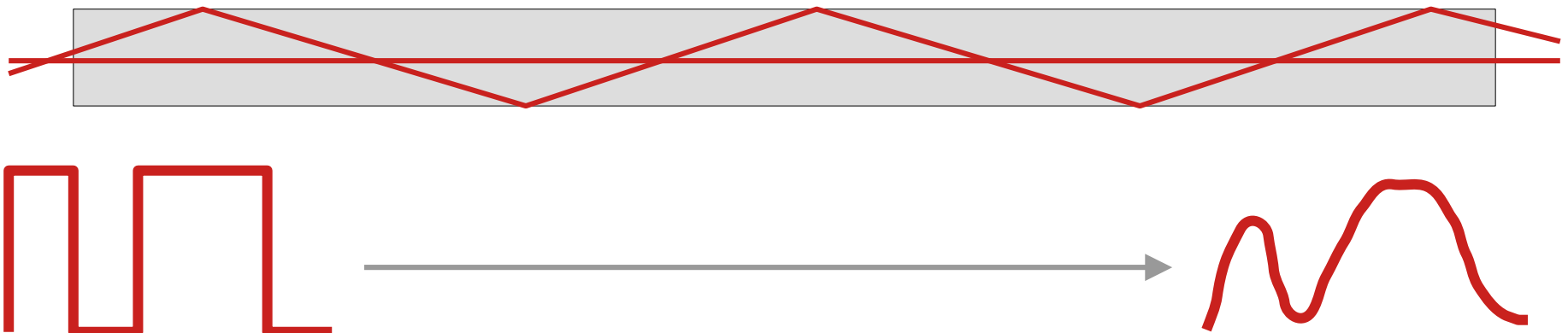


Vlastnosti optického vlákna

- obrovská šířka pásma (terabity)
- bez interakcí s okolím – nevyzařuje, signál není rušen, neindukuje se (nutné pro venkovní spoje)
- dvoubodový spoj, odbočka nebyla uspokojivě vyřešena
- méně pružné
- dražší, ale dostupné
- 2 typy: vícevidová a jednovidová

Vícevidová vlákna

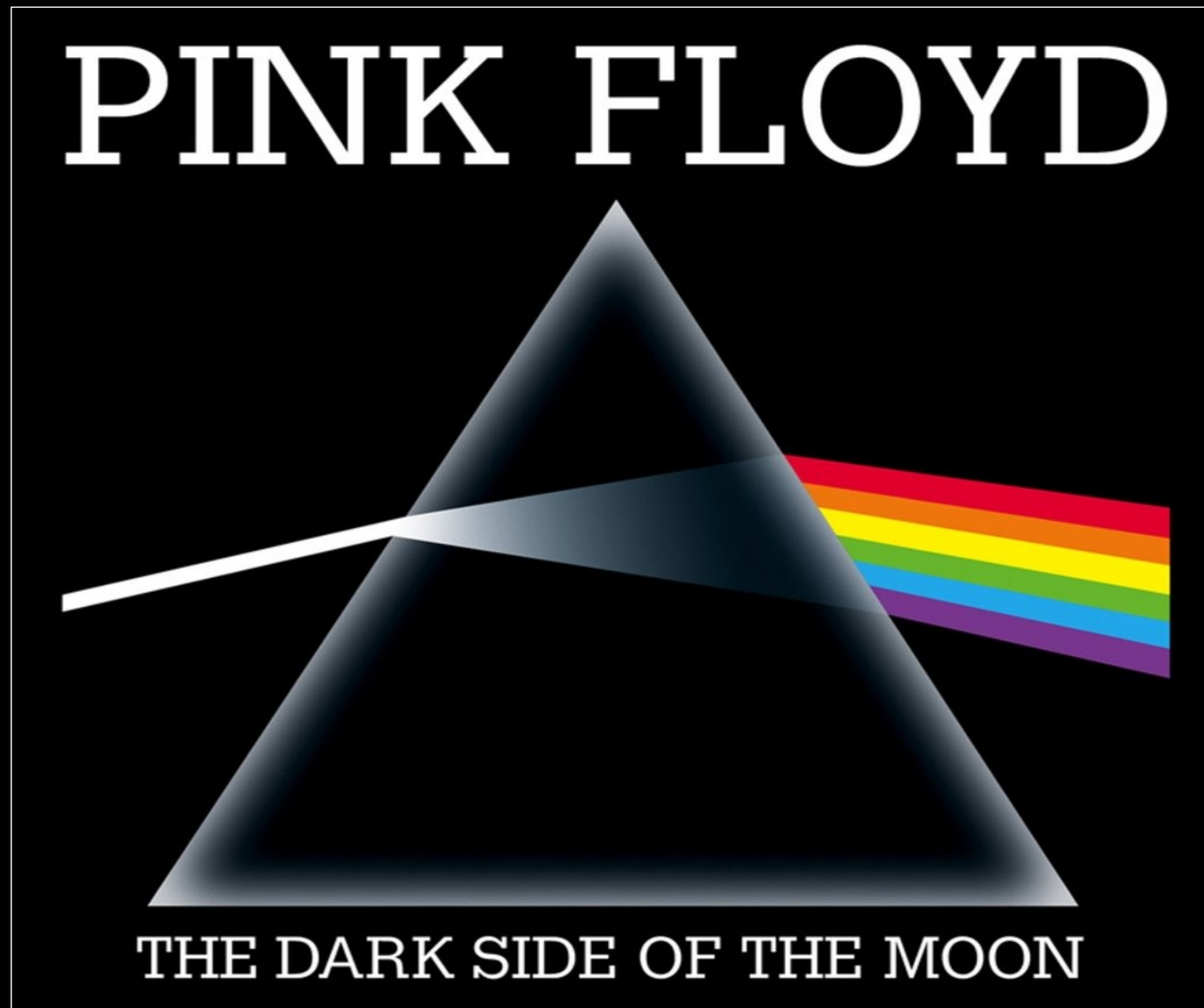
- **multi-mode, MM**
- průměr 50/125 nebo 62,5/125 μm
- světelným zdrojem LED, paprsky různoběžné \rightarrow rozostření signálu \rightarrow omezuje dosah a přenosovou rychlost
- dosah stovky metrů až kilometry



Jednovídná vlákna

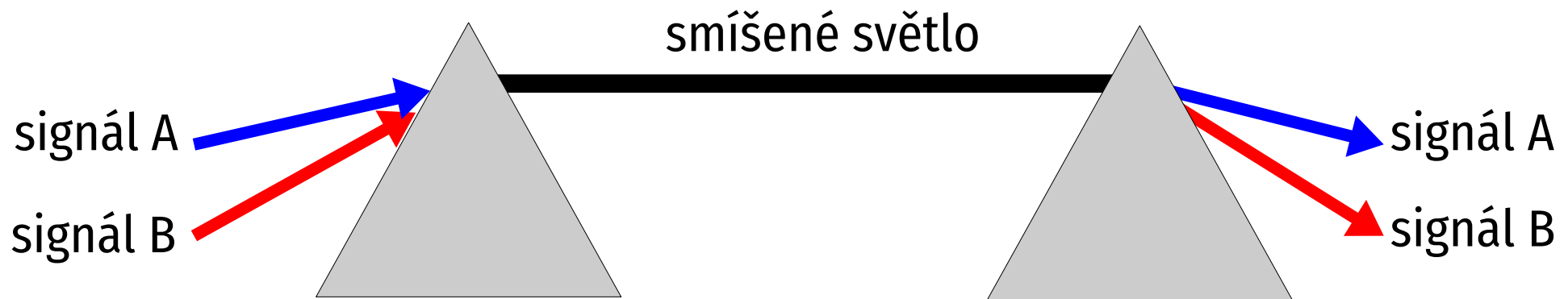
- **jednovídné (single-mode, SM)**
- průměr 9/125 μm
- světelným zdrojem laser (pozor na oči!), paprsky rovnoběžné
- dosah stovky kilometrů
- dražší, ale dnes již dostupné
- pro vysoké přenosové rychlosti (od 10 Gb/s) de facto jediná možnost

Wavelength Division Multiplexing



Wavelength Division Multiplexing

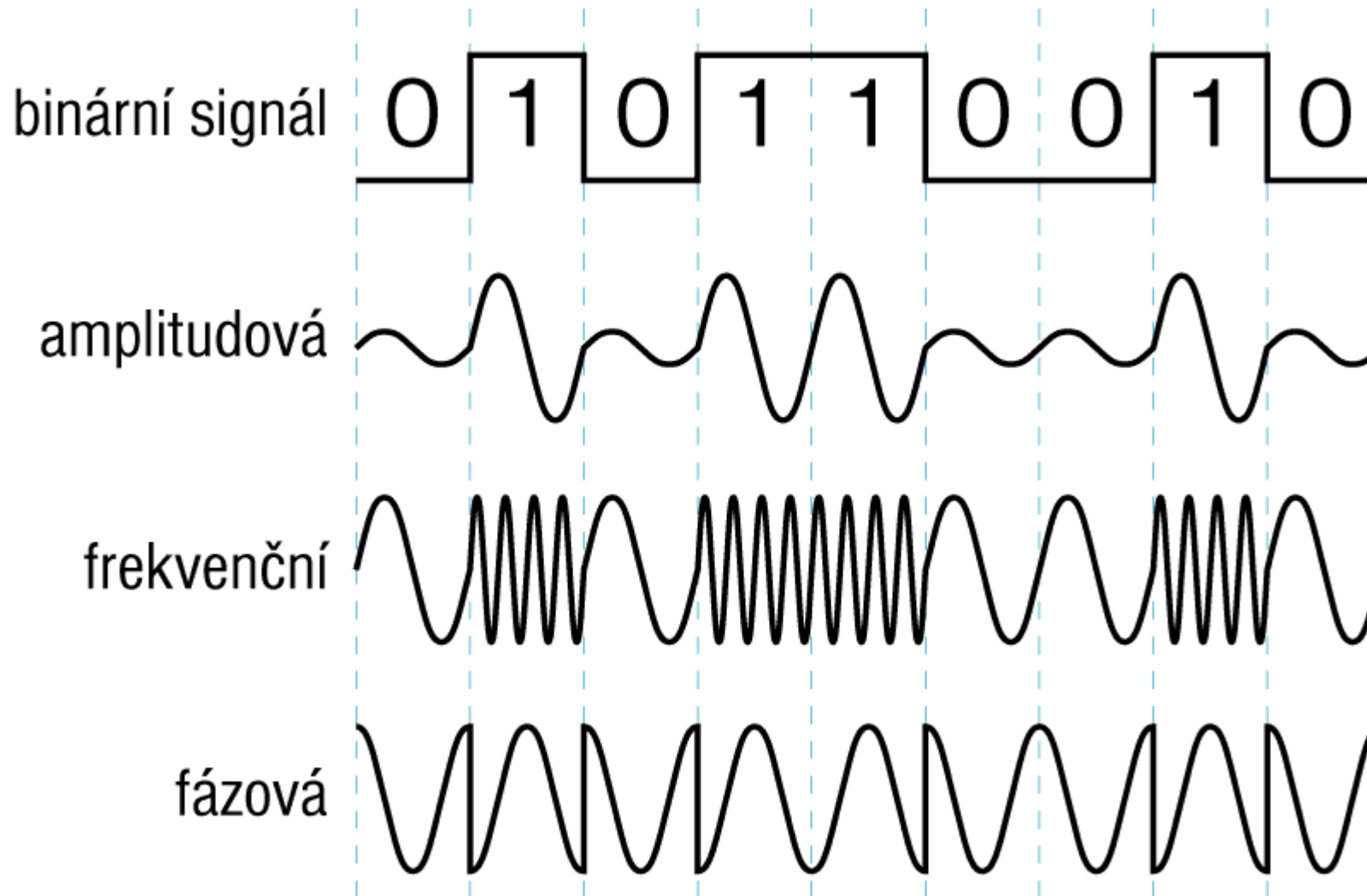
- několik nezávislých signálů v jednom vlákně
- optický hranol – smíchá/rozloží různé barvy světla (index lomu závisí na frekvenci světla)
- znásobuje kapacitu vlákna



Data na telefonní lince

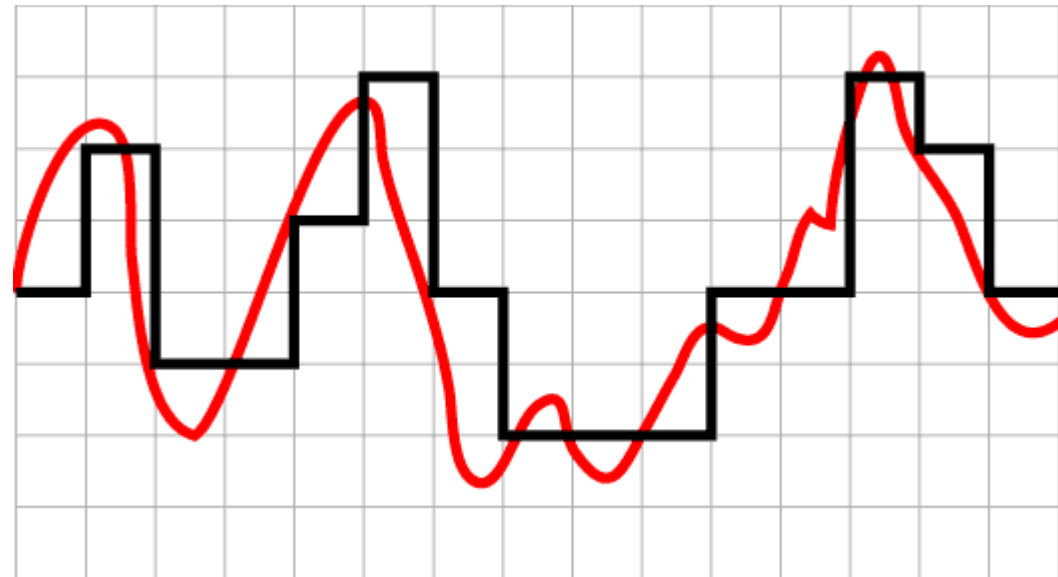
- telefonní síť velmi rozlehlá – mnoho uživatelů
- telefon je analogový – data nutno převést na zvuk
- tzv. **modulace**
- realizuje **modem** (MOdulator/DEModulator)
 - interní: vestavěn v počítači (karta, na základní desce)
 - externí: samostatné zařízení (dražší, ale flexibilnější)
 - Winmodem: část funkcí realizuje počítač

Principy modulace



Digitální přenos hlasu

- kvalitnější, signál se restauruje do původní podoby
- kabel lze snadno sdílet (časový multiplex)
- **Pulse Code Modulation (PCM)**
 - realizuje **codec** (COder/DECoder), opak modemu
 - 8000× za sekundu změří signál a vyjádří číslem
 - kanál 64 kb/s



Digitalizace telefonní sítě

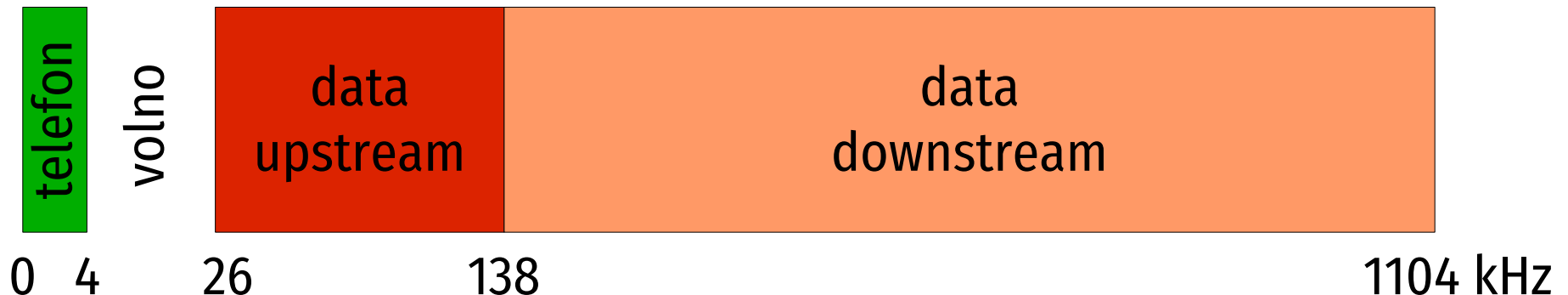
- většina ústředen je digitálních, komunikace mezi nimi též
- analogové jsou už jen místní smyčky k telefonům
- přenos dat vede k absurditám
 - digitální signál
 - modem převede na analogový
 - po přenosu místní smyčkou ústředna digitalizuje
 - na druhém konci opačně

ISDN

- **Integrated Services Digital Network**
- digitální telefon s přidanými službami (data, fax, elektronická pošta, databáze, signalizace)
- základem kanál 64 kb/s (kanál B), několik kanálů časově multiplexováno na společném kabelu
- neuspělo
 - pomalá standardizace, vysoká cena
 - 64 kb/s je zbytečně mnoho pro hlas, ale málo pro data a obraz

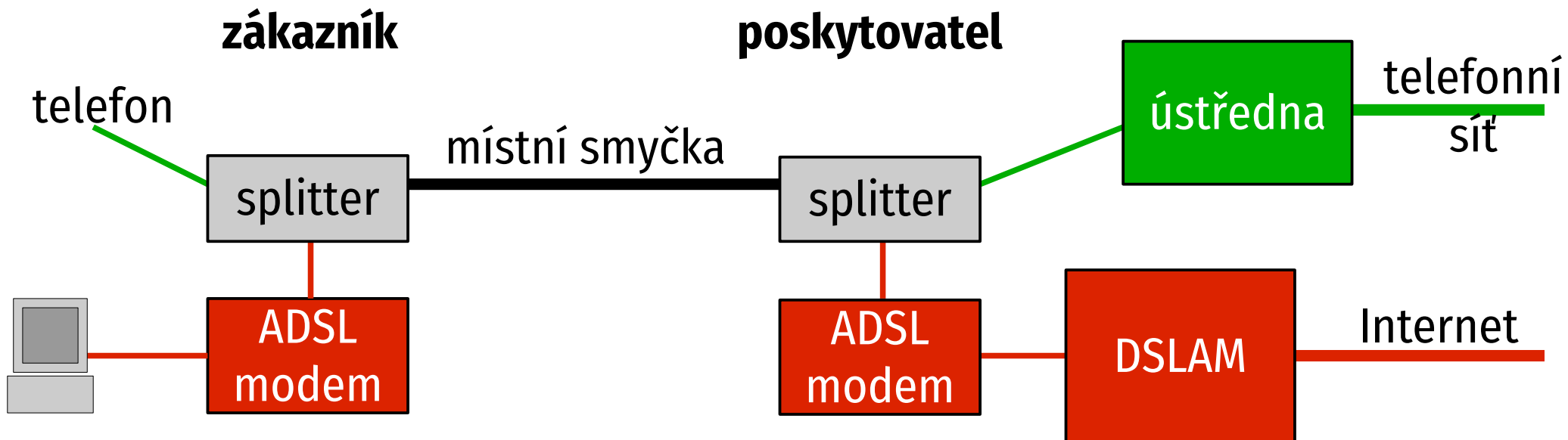
ADSL (1)

- **Asymmetric Digital Subscriber Line**
- šířka pásma telefonu uměle omezena (filtry), místní linka dokáže přenášet mnohem více
- dostupné pásmo rozděleno na kanály (cca 4 kHz) pro telefon, downstream a upstream



ADSL (2)

- **splitter** směšuje/odděluje telefonní a datový signál
- **ADSL modem** zajišťuje odpovídající konverzi signálu



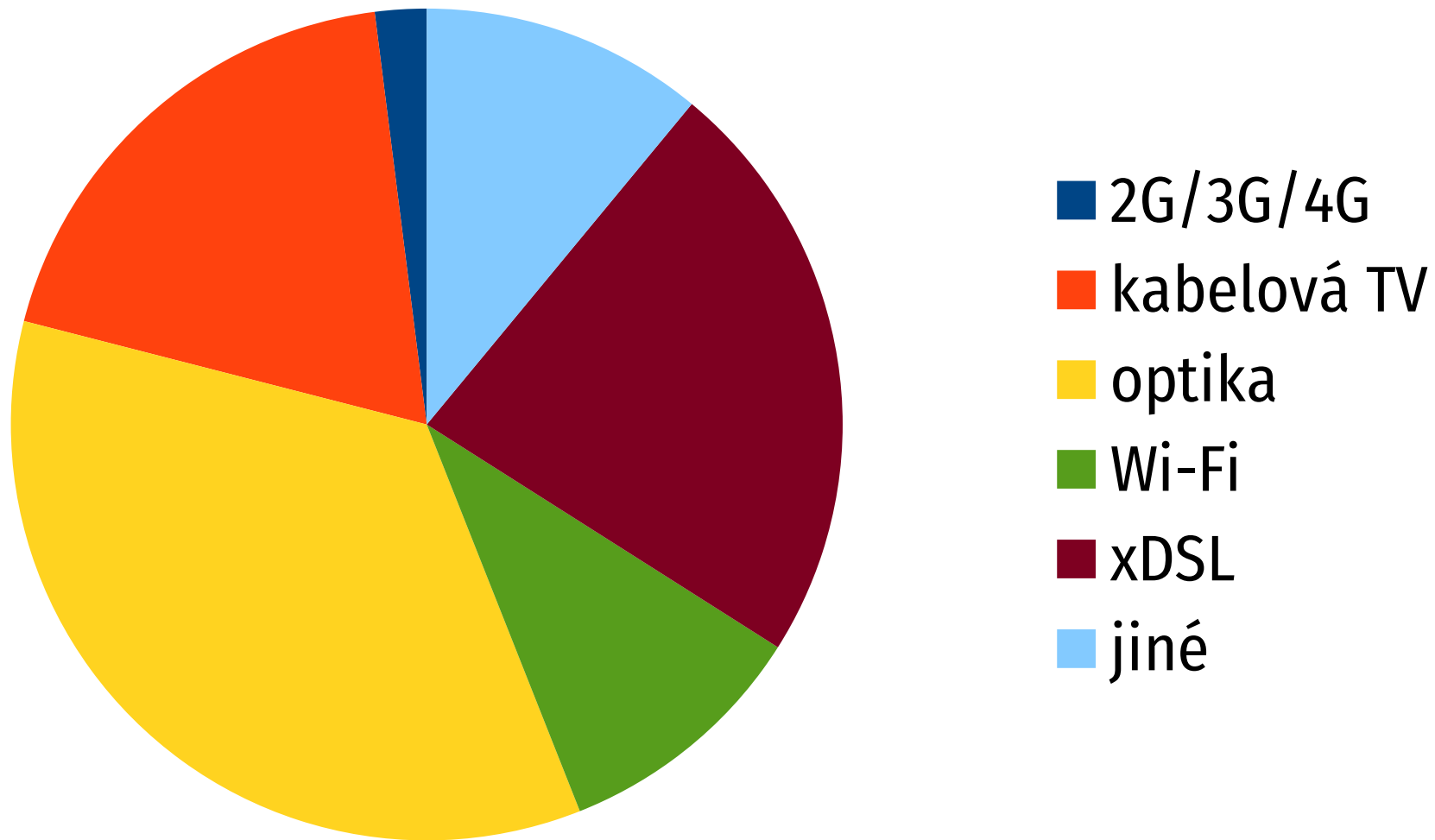
ADSL (3)

- **asymetrické** – rychlost oběma směry se liší
- různé specifikace:
 - ADSL až 8:1 Mb/s
 - ADSL2 až 12:3,5 Mb/s
 - ADSL2+ až 28:3,5 Mb/s
- **VDSL (Very-high-bit-rate DSL)**
 - VDSL až 55:3 Mb/s
 - VDSL2 až 100:100 Mb/s

ADSL (4)

- konkrétní rychlost závisí na:
- **vlastnostech místní smyčky**
 - délka, kvalita kabelu
 - prakticky neovlivnitelné
- **použitém vybavení**
 - na obou stranách
- **smlouvě s poskytovatelem**
 - často různé varianty

Domácí připojení (EU 2017)



vytvořeno s podporou
projektu ESF





Ethernet



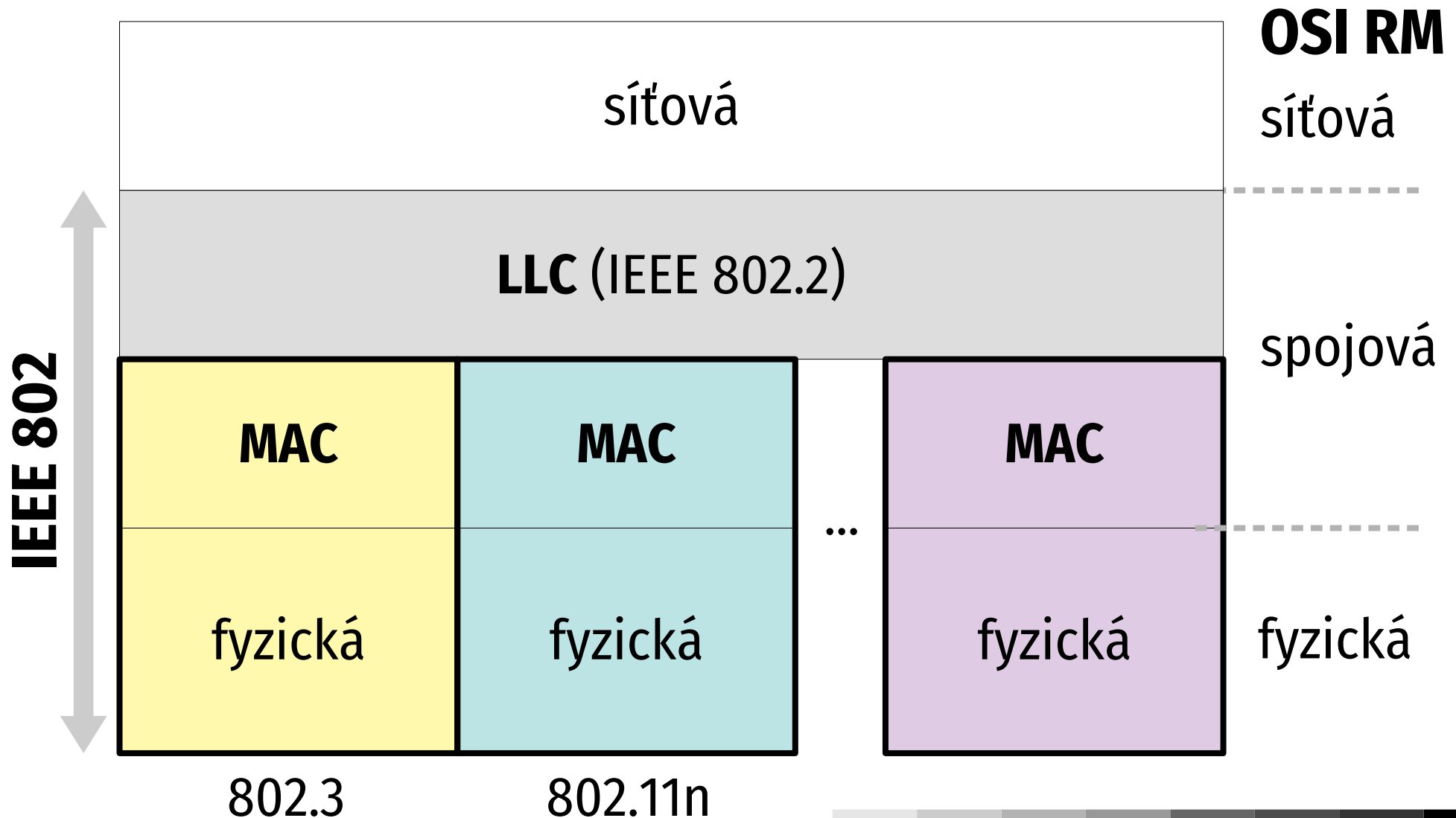
Vznik Ethernetu

- 1980 – DIX konsorcium (Digital, Intel, Xerox)
- určen pro kancelářské aplikace
- sběrníková topologie na koaxiálním kabelu, přístup k médiu řízen metodou CSMA/CD
- přenosová rychlost 10 Mb/s
- později IEEE 802.3 – nekompatibilní standard
- Ethernet v2 – některé prvky přizpůsobeny IEEE 802.3 (ale stále nekompatibilní)

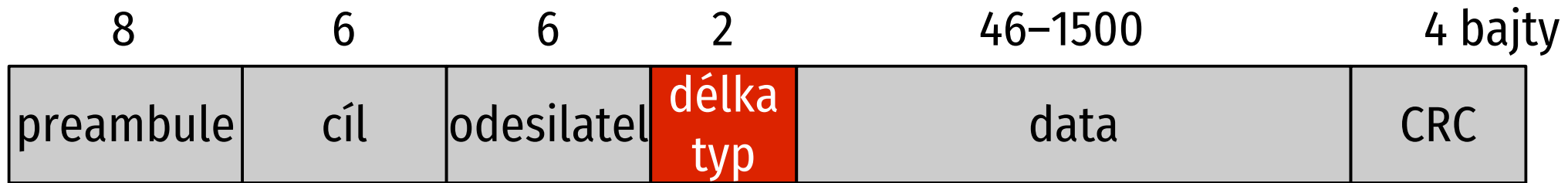
Skupina IEEE 802

- **Institute of Electrical and Electronics Engineers**
- skupina 802 – standardy pro lokální sítě
 - 802.3 CSMA/CD (Ethernet)
 - 802.11 bezdrátové sítě
- podvrstvy
 - **Logical Link Control (LLC)** – sjednocuje, IEEE 802.2
 - **Media Access Control (MAC)** – konkrétní technologie
- <http://standards.ieee.org/getieee802/>

Podvrstvy LLC a MAC



Formát rámce



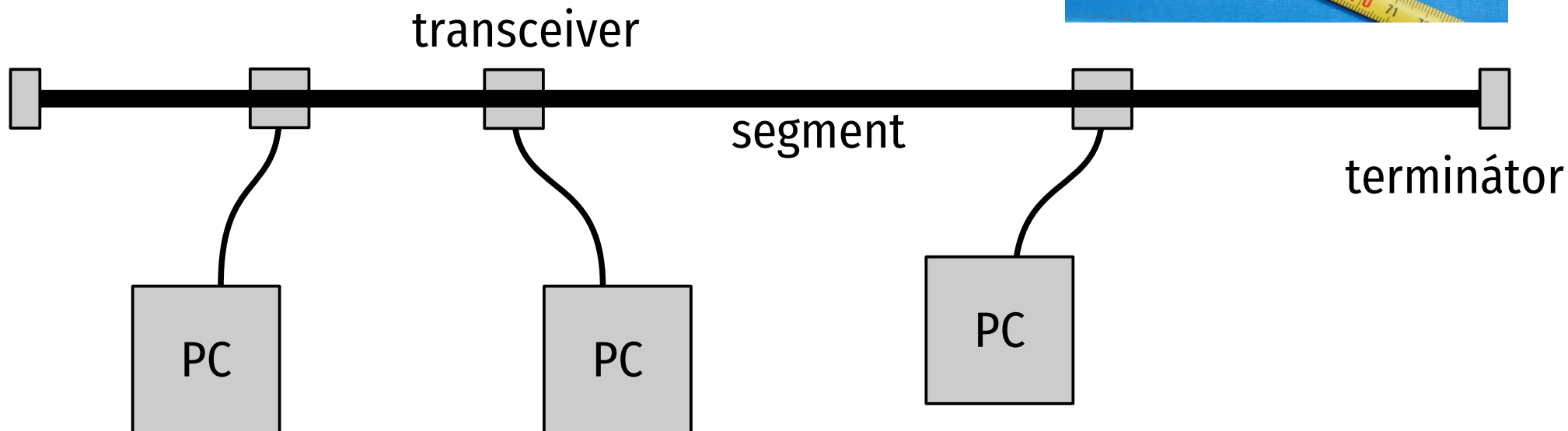
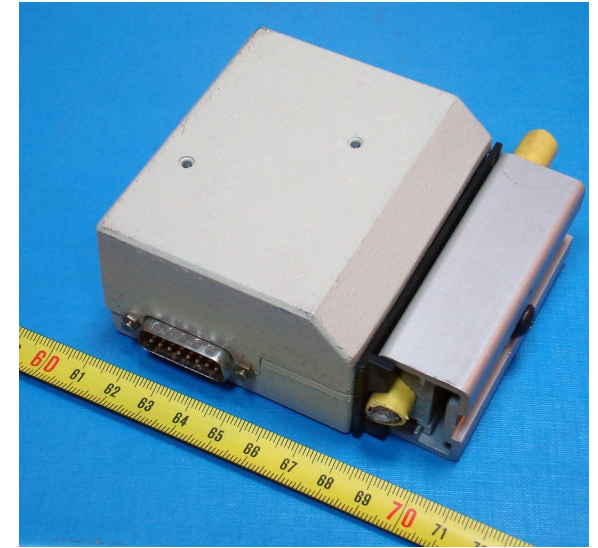
- **preamble:** 101010 ... 101011
- **cíl, odesílatel:** MAC adresy příjemce a odesílatele
- **délka:** délka nesených dat (IEEE 802.3)
typ: druh přepravovaných dat (Ethernet v2)
- **data:** nesená informace, případně doplněná vatou
- **CRC:** kontrolní součet

MAC adresy

- 48 bitů (6 bajtů)
- zapisovány jako 6 dvojic šestnáctkových číslic:
00-02-c3-67-a8-3f
- **celosvětově jednoznačné:**
 - první polovinu přiděluje výrobci centrální autorita
 - druhou polovinu přiděluje výrobce a ručí za její jednoznačnost

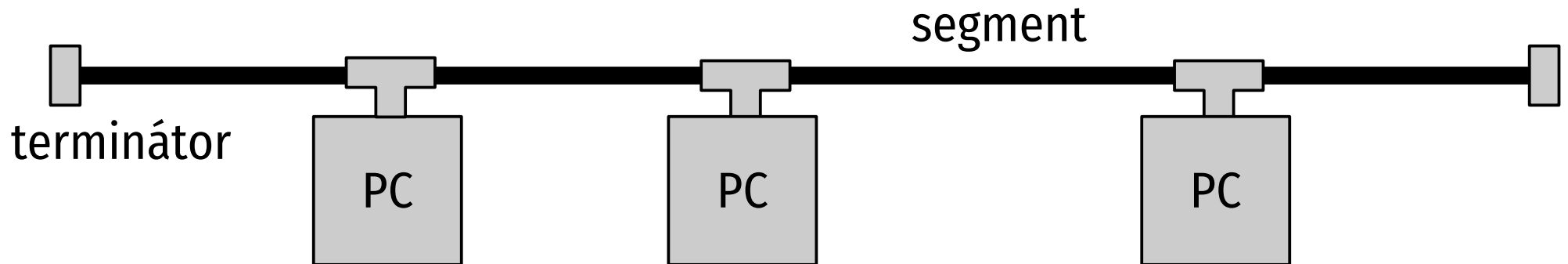
Historie: Koaxiální kabel (1)

- **tlustý kabel:** vampýří připojení bez přerušení, transceiver na segmentu, počítač připojen AUI kabelem (až 50 m)



Historie: Koaxiální kabel (2)

- **tenký kabel (cheapernet):** BNC konektory, segment přiveden k počítači, levné, pružné, choulivé



Algoritmus CSMA/CD (1)

- **Carrier Sense with Multiple Access and Collision Detection**
- popisuje chování vysílajícího při odesílání rámce:
 - chvíli naslouchá
 - je-li volno, začne vysílat (jinak čeká na uvolnění)
 - při vysílání zároveň naslouchá – hlídá kolizi
 - **kolize:** vysílá několik stanic najednou, data znehodnocena

Algoritmus CSMA/CD (2)

- při zjištění kolize:
 - vyšle „jam“ signál (indikace kolize pro ostatní)
 - počká **náhodnou** dobu t_k a opakuje pokus
 - max. 16 pokusů, pak ohlásí neúspěch
- určení doby t_k při k -tém pokusu: $t_k = n \times t_0$
 - $t_0 = 51,2 \mu\text{s}$ (doba vysílání minimálního rámce 512 b)
 - n je náhodné číslo z intervalu od 0 do 2^k (pro $k < 10$), resp. od 0 do 2^{10} (pro k větší)
 - binary exponential backoff

Kolizní okénko



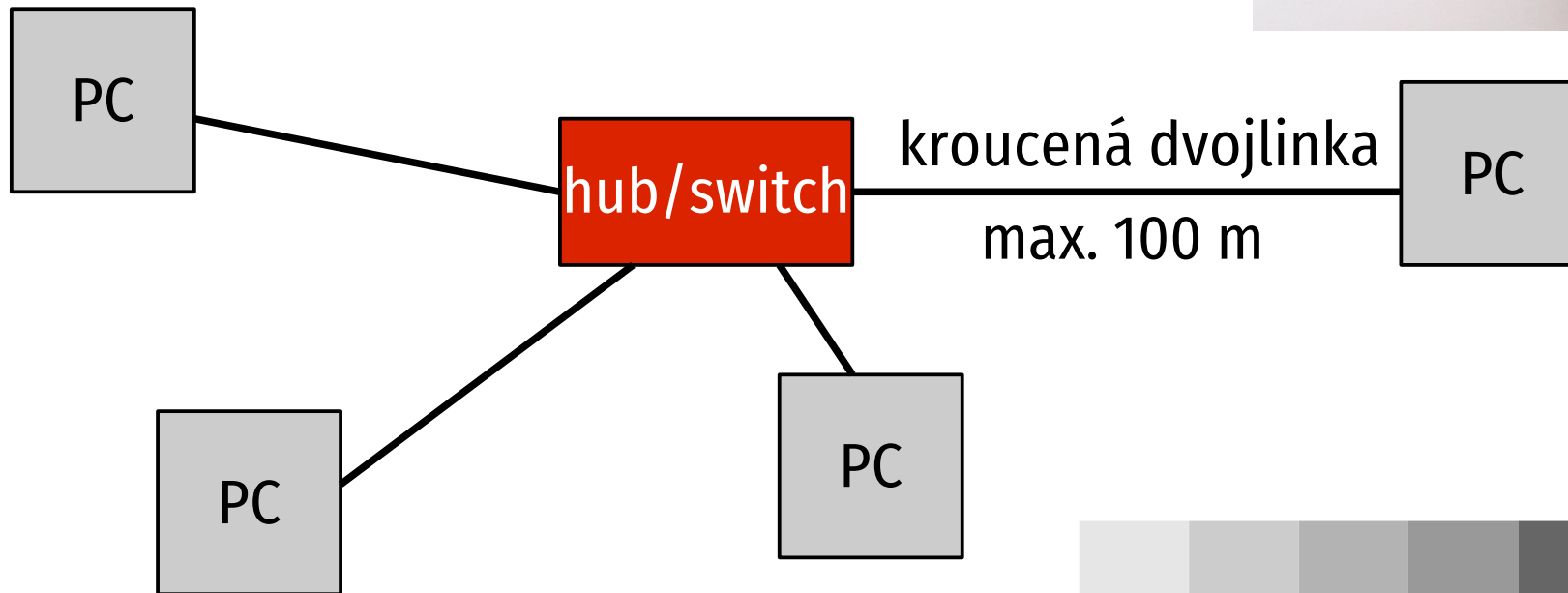
- jakmile signál obsadí médium, kolize nemůže nastat
- **kolizní okénko:** čas od začátku vysílání do obsazení média – jen tehdy může dojít ke kolizi
- **kolizní okénko < doba vysílání nejkratšího rámce**
jinak hrozí neobjevené kolize, komplikuje zvyšování
přenosové rychlosti

Důsledky CSMA/CD

- s opakovanými neúspěchy stanice „řadí“ pokusy – větší šance na úspěch
- odvysílání není zaručeno
- každá kolize znamená promarněný čas – data se musí vysílat znovu
- v době největšího zájmu přibývá kolizí a klesá tak efektivita využití média
- využití závisí na velikosti rámců

Ethernet na kroucené dvojlince

- standardní řešení současnosti
- hvězdicová topologie
- uprostřed hub (rozbočovač) nebo switch (přepínač)



Přepínač (switch)

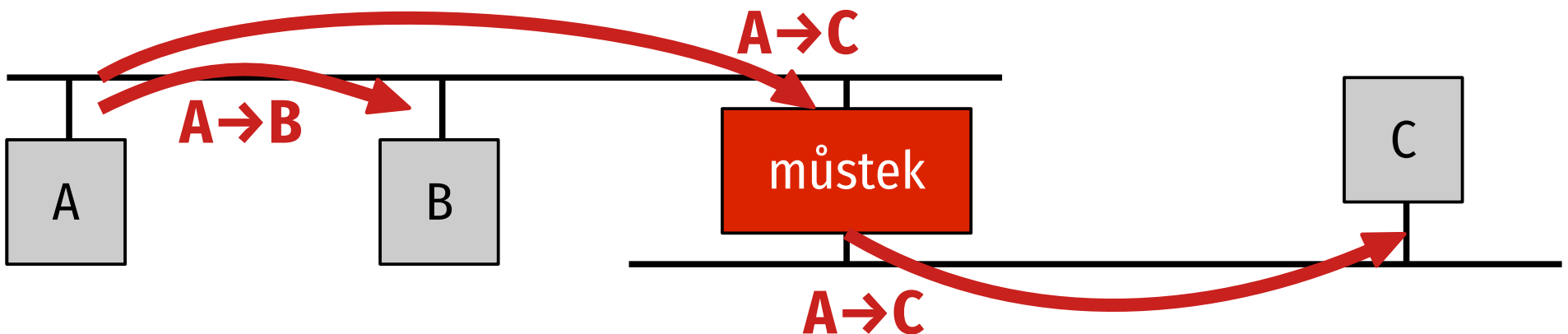


Hub (rozbočovač)

- vznikl s cílem **simulovat sběrnici**
- co přichází z jednoho kabelu rozešle do všech ostatních
- regeneruje signál – jakmile rozpozná 0/1 posílá dál, zpoždění 1 bit
- všechny připojené počítače spolu soutěží o médium algoritmem CSMA/CD
- dnes už historie

Historie: Bridge (můstek)

- eviduje, kam je kdo připojen
- předává jen pakety, které adresát neslyšel
- **store & forward** – uloží do paměti a následně odvysílá → odděluje kolizní domény CSMA/CD



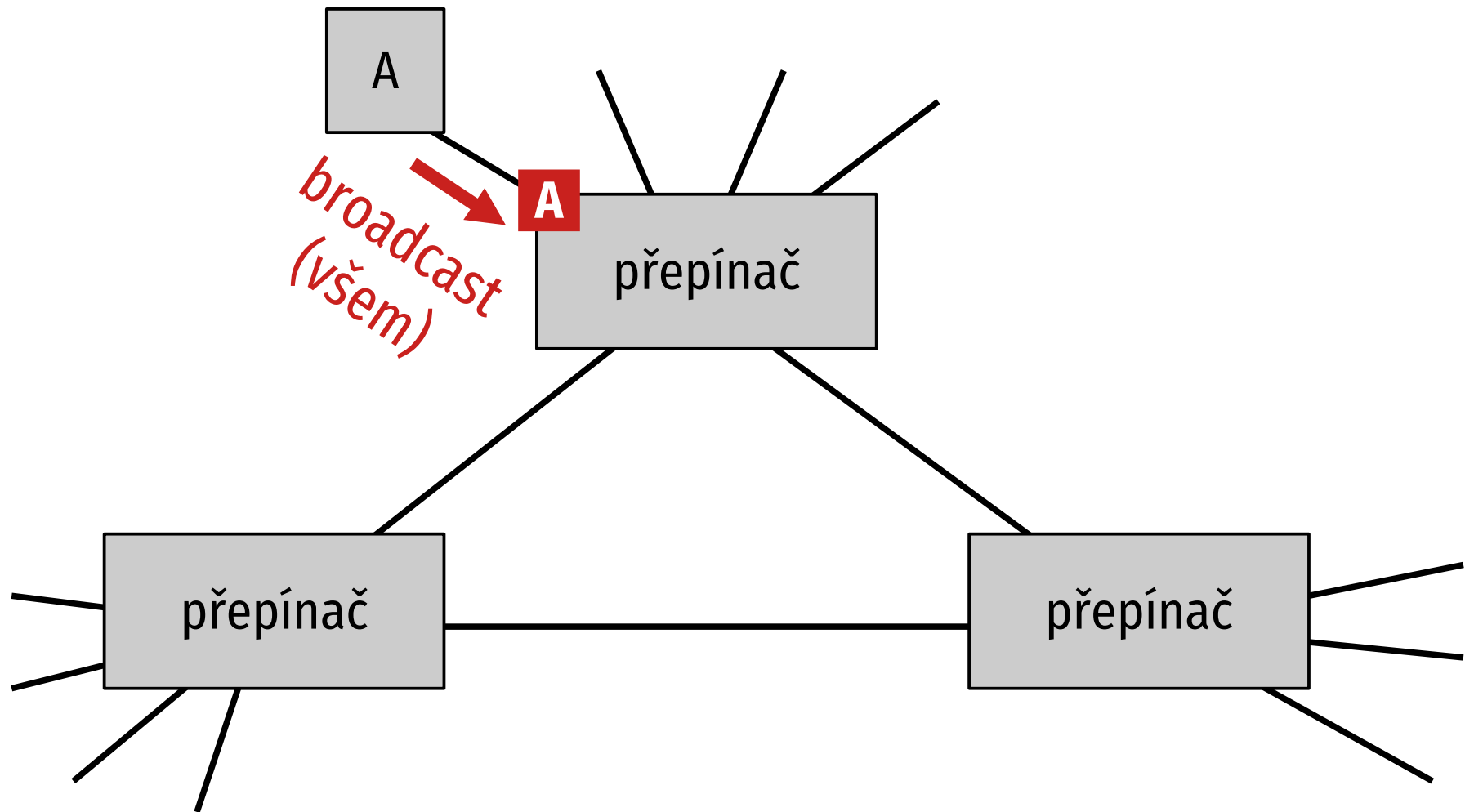
Switch (přepínač)

- vznikl rozšířením rozbočovače o logiku můstku
- **intelligentní** – pošle data jen do kabelu, kde se nachází adresát
- **store & forward** – příjem a vysílání nezávislé
- **odděluje kolizní domény CSMA/CD**
 - počítače na jednom kabelu nesoutěží s počítači jiných kabelech
- dříve drahé, dnes samozřejmostí

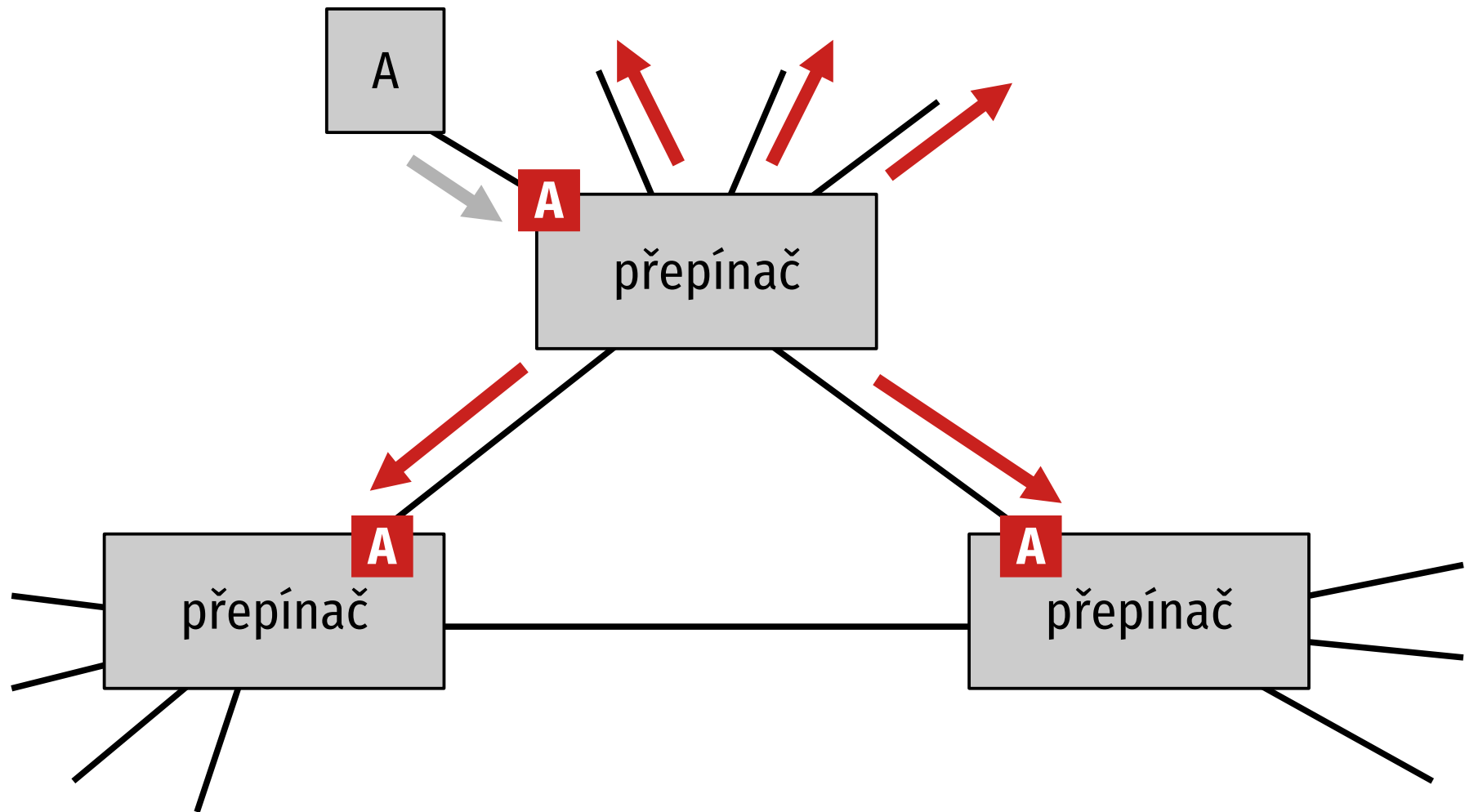
Jak pracuje přepínač

- automatická konfigurace
- **z adresy odesílatele** se dozví, kde kdo sídlí
- rámce určené neznámému adresátovi rozešle všem (jako rozbočovač)
- **problém s cykly** (redundancí) v síti:
 - řeší algoritmus **spanning tree**
 - některé linky deaktivuje a vytvoří strom pokrývající síť
 - při výpadku obnoví
 - problémy s kompatibilitou

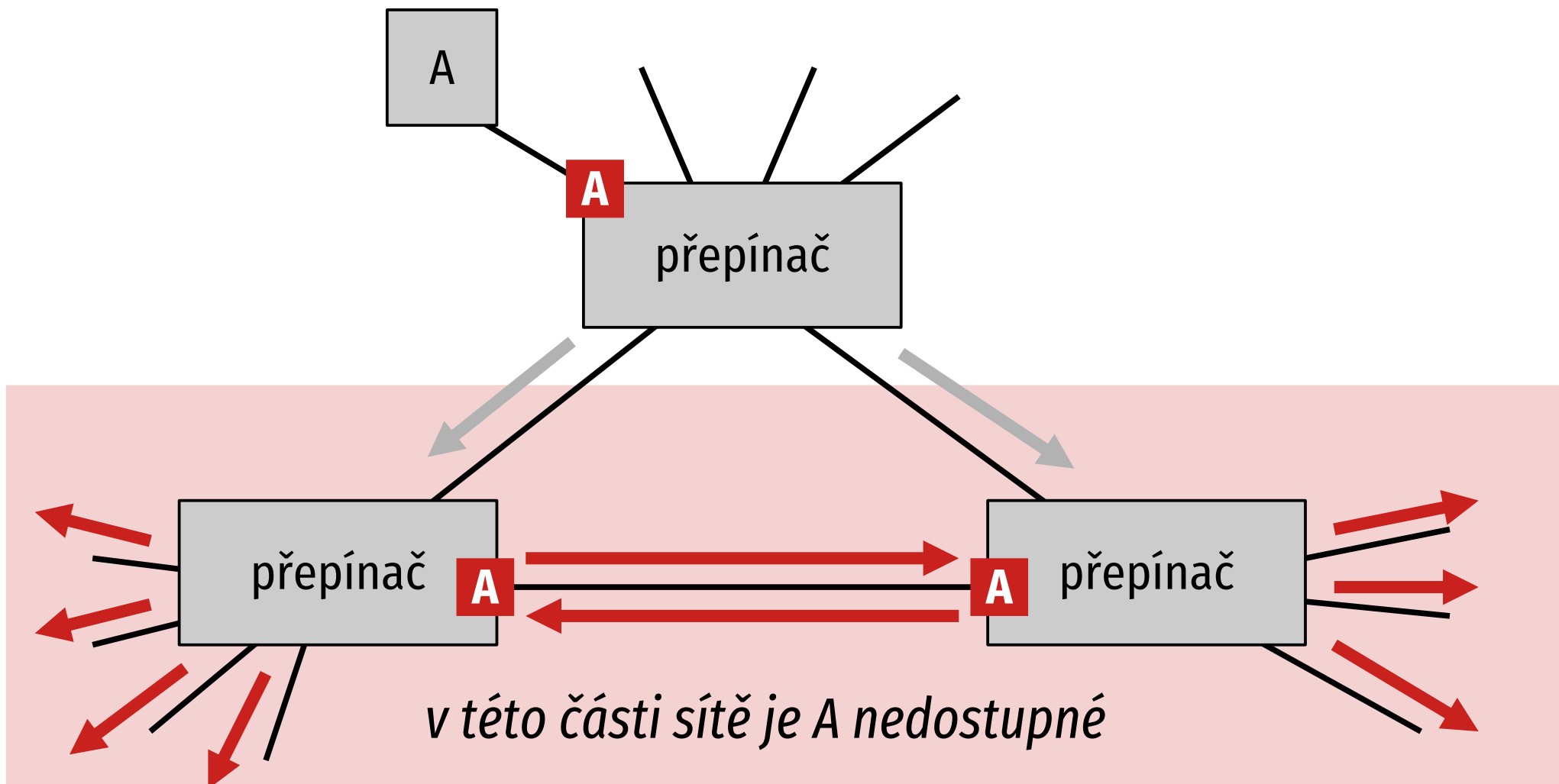
Problém s cykly (1)



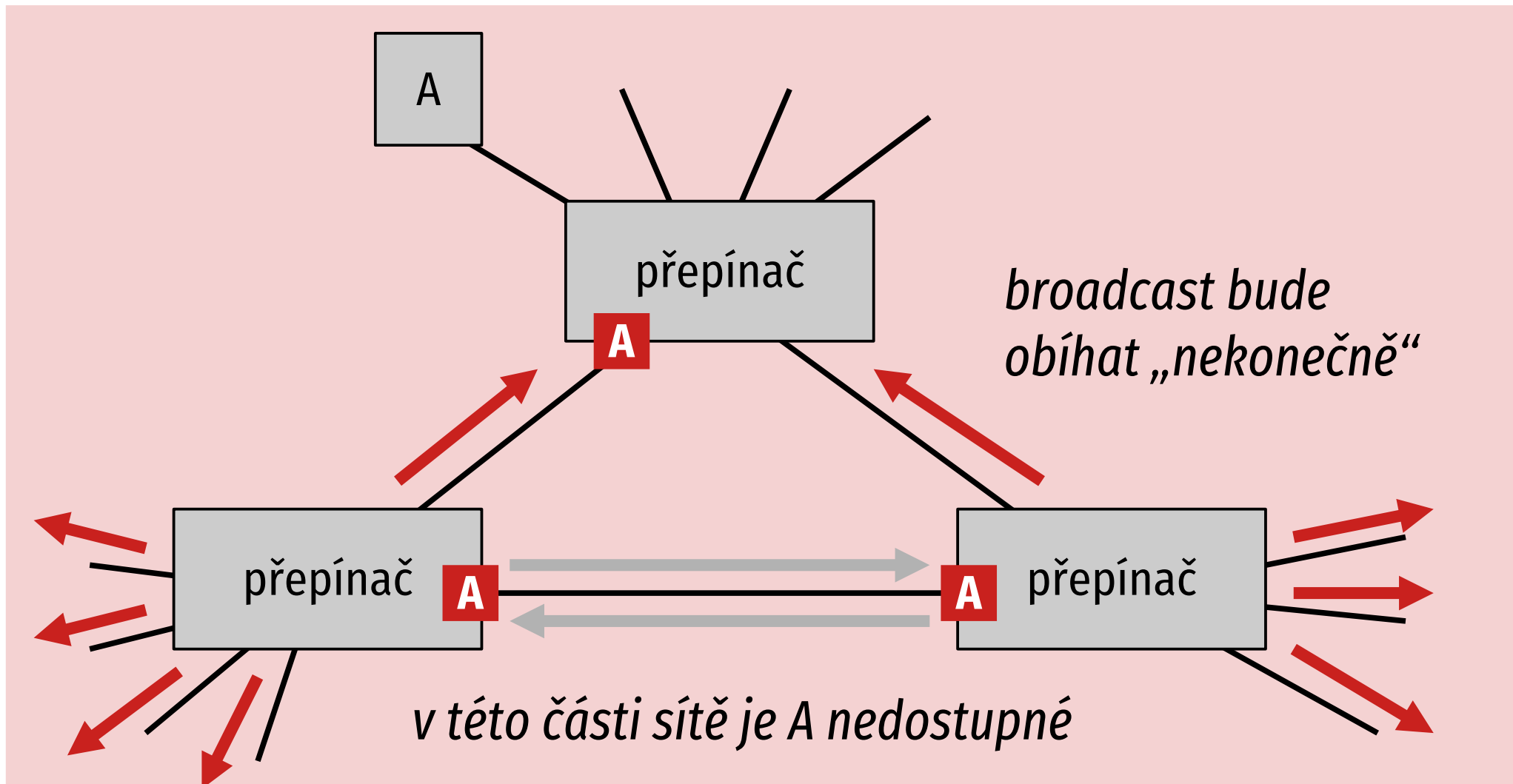
Problém s cykly (2)



Problém s cykly (3)



Problém s cykly (4)




Duplexní provoz (full duplex)

- připojením počítačů k přepínači mizí sdílení média
- lze **současný provoz oběma směry bez CSMA/CD**
- jakmile má rámeček, odvysílá jej; paralelně přijímá data z druhé strany (po jiných vodičích – UTP jich má osm)
- všechny současné karty a přepínače podporují
- autodetekce nebo ruční nastavení

Fast Ethernet

- IEEE 802.3u (1995)
- rychlost 100 Mb/s
- maximum prvků převzato z Ethernetu – **formát rámce, CSMA/CD**
- shodná logika – software vyšších vrstev beze změn
- vzdálenost hub–počítač max. 100 m, na cestě max. 3 huby nanejvýš 10 m od sebe: dosah 220 m
- zařízení „pod obojí“, automatická detekce 10/100

Média pro Fast Ethernet

- standardní značení IEEE: **100BASE-TX**

přenosová rychlost *v základním pásmu* *typ (médium)*
- **100BASE-TX**
 - 2 páry UTP kategorie 5, délka spoje do 100 m
- **100BASE-FX**
 - optické vlákno, 400 m poloduplex (kvůli detekci kolizí), 2 km plný duplex

Gigabitový Ethernet

- IEEE 802.3z (optika), 802.3ab (UTP), 1998
- rychlost 1 Gb/s
- opět **stejný formát rámce a CSMA/CD** (spíše symbolicky, používá se plný duplex)
- původně pro páteře sítí,
dnes běžně na základní desce
10/100/1000
- výměnný modul pro
médiu – **GBIC**



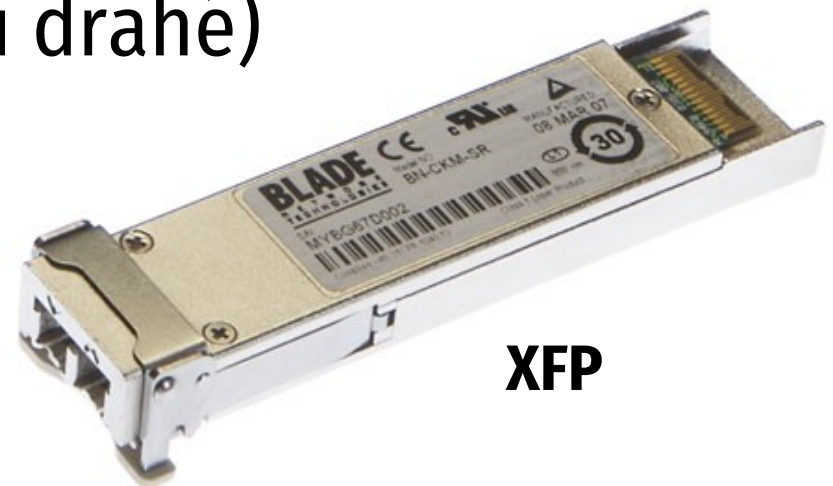
GBIC

Média pro gigabitový Ethernet

- **1000BASE-T**
 - UTP kategorie 5 a lepší, 100 m
- **1000BASE-SX**
 - vícevidové vlákno, 500 m
- **1000BASE-LX**
 - jednovidové vlákno, 2 km
- **1000BASE-ZX**
 - jednovidové vlákno, 70 km

Desetigigabitový Ethernet

- IEEE 802.3ae (optika, 2003), 802.3an (UTP, 2006)
- rychlost 10 Gb/s
- **stejný formát rámce, bez CSMA/CD** – komunikace jen plně duplexní
- pro páteřní sítě (dosud velmi drahé)
- opět výměnné moduly pro média – XFP



XFP

Média pro 10G Ethernet

- **10GBASE-T**

- UTP kat. 6 (50 m) nebo 6a (100 m), zatím vzácné

- **10GBASE-SR**

- vícevidové vlákno, dosah podle vlákna 25 až 300 m

- **10GBASE-LR**

- jednovidové vlákno, 10 km

- **10GBASE-ER**

- jednovidové vlákno, 40 km

Stogigabitový Ethernet

- standard IEEE 802.3ba přijat v červnu 2010
- 18 standardizovaných variant + firemní
- rychlosti 40 a 100 Gb/s
- zachovává formát rámce
- na trhu pro high-end zařízení
- používá se ve vysoce zatížených částech infrastruktury (páteřní sítě, peeringová centra)

Terabitový Ethernet

- název používán pro rychlosti nad 100 Gb/s
- 200 Gb/s, 400 Gb/s IEEE P802.3bs (2017)
- 800 Gb/s IEEE P802.3df (2024)
- chystá se 1,6 Tb/s

vytvořeno s podporou
projektu ESF



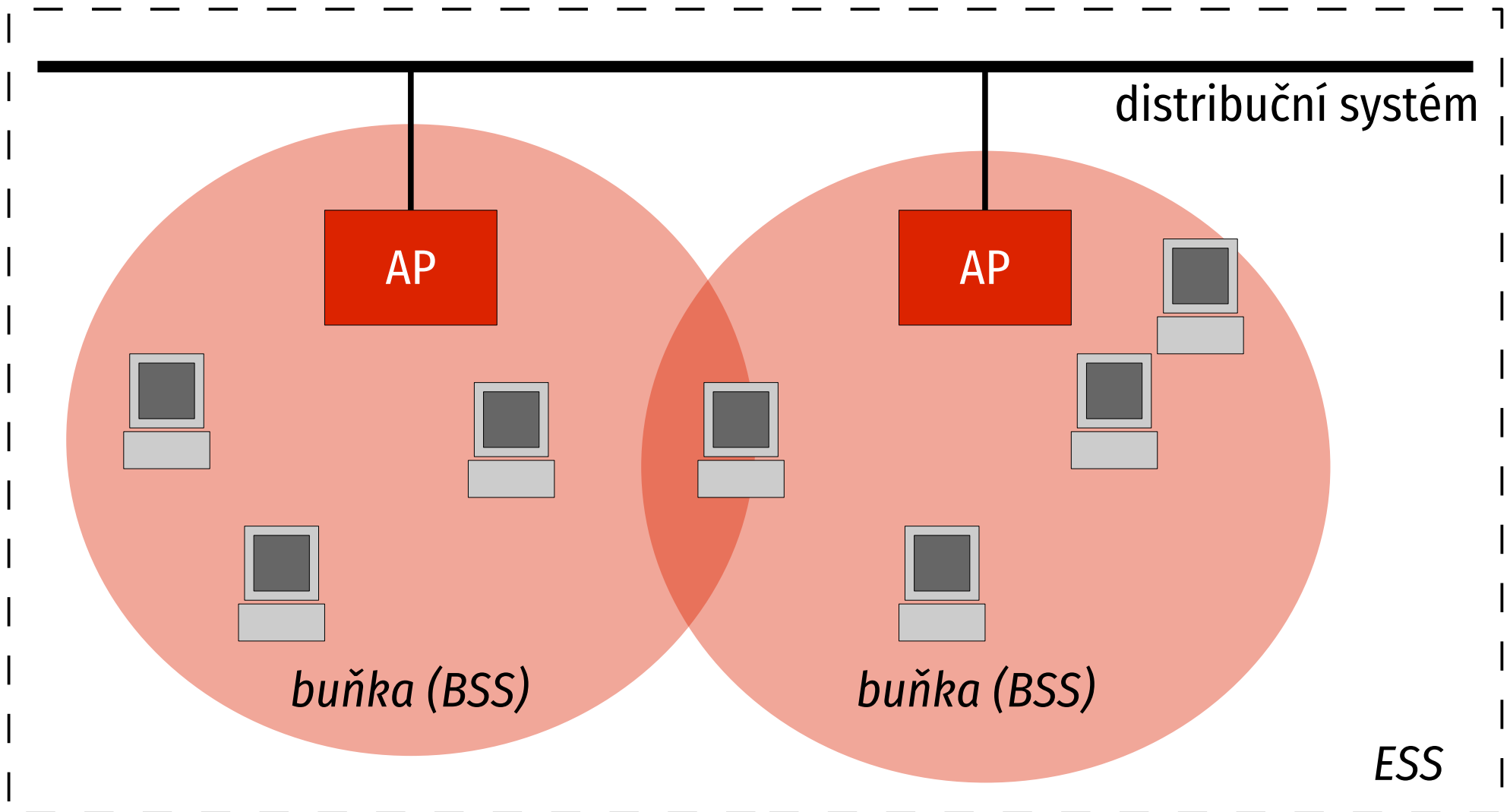
Bezdrátové sítě

IEEE 802.11

Vlastnosti IEEE 802.11

- velmi rychle se rozvíjejí
- **přednosti:**
 - pokrytí plochy, podpora mobility
 - umožňují propojení budov bez optických vláken
- **zápory:**
 - pomalejší
 - větší chybovost

Architektura sítě IEEE 802.11



Buňka (BSS)

- **Basic Service Set**
- skupina stanic komunikujících navzájem
- **nezávislá (ad hoc)**
 - stanice komunikují přímo, problém se vzájemnou slyšitelností
- **infrastrukturní**
 - řízena základnovou stanicí (Access Point, AP)
 - veškerý provoz prochází AP
 - umožňuje lepší služby

Činnost AP

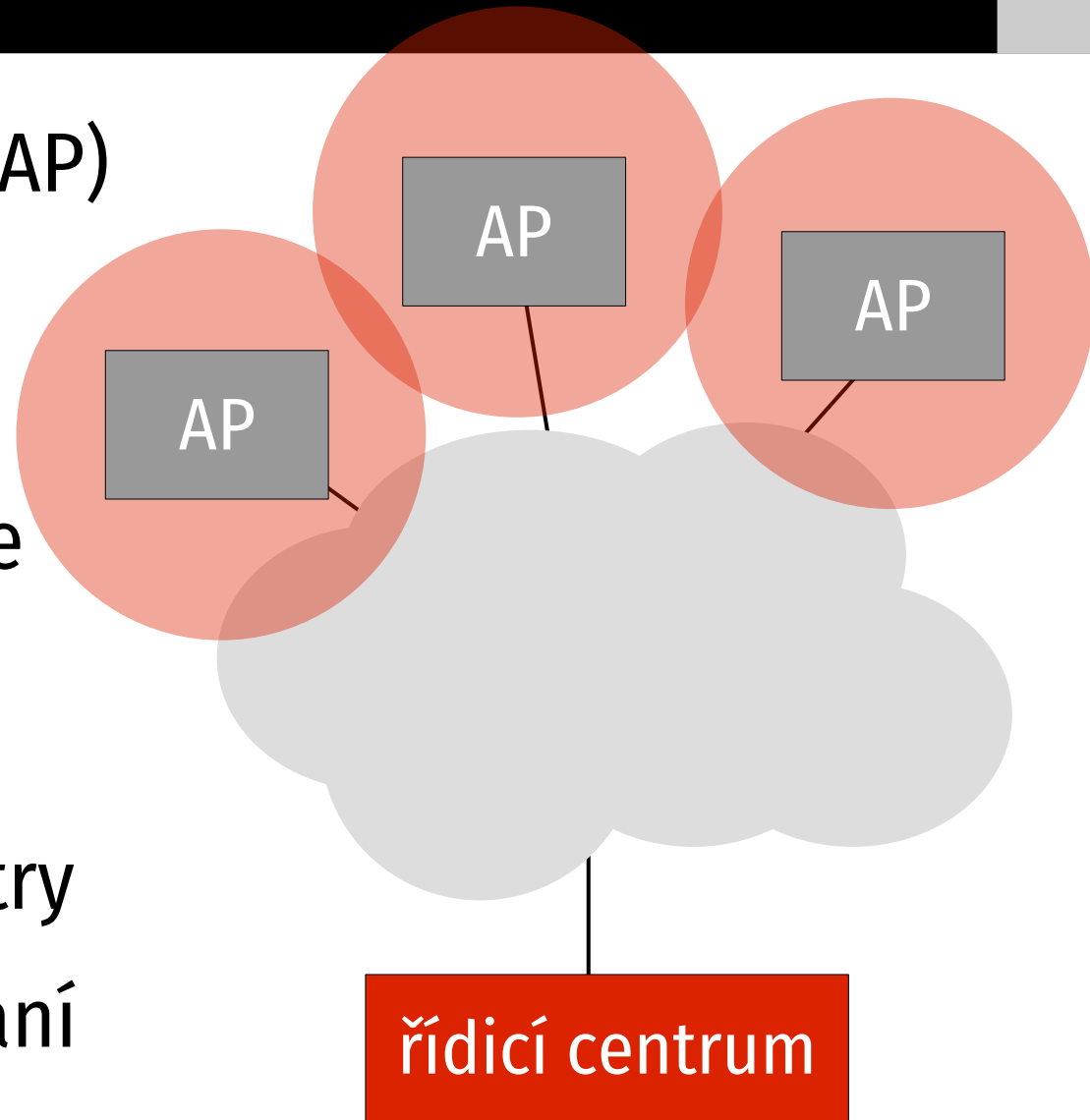
- řídí buňku
- veškeré přenosy procházejí přes AP
- ukládá rámce pro spící stanice (úspora energie)
- pravidelně vysílá Beacon Frame
 - synchronizace času
 - vyzývá nové stanice ke vstupu do buňky
 - systémové parametry
 - pravidelně 10 až 100× za sekundu

ESS

- **Extended Service Set**
- skupina spolupracujících buněk
- propojeny distribučním systémem (lokální sítě)
 - **portál** – zařízení propojující IEEE 802.11 síť s jinou sítí (typicky Ethernetem), obvykle integrován v AP
- vyžaduje komunikaci mezi AP
 - Inter-Access Point Protocol (IAPP)
 - standard IEEE 802.11F, přijat 2003, stažen 2006
 - firemní protokoly

Centrální řízení

- pro velké sítě (desítky AP)
- funkce AP omezeny na provoz buňky
- vše složitější rozhoduje centrum
- umožňuje nastavovat a koordinovat parametry
- obvykle webové rozhraní
- firemní řešení



Kuriozita

- Znáte ji?



Hedy Lamarr (1912–2000)

- rakouská herečka, první nahá scéna v historii filmu (Machatého Extase, 1932)
- vynalezla přeskokování frekvencí (US patent)
 - rychlé střídání frekvencí
 - ochrana před rušením
 - použito v IEEE 802.11 (v první generaci)



Fyzická vrstva

- **infračervené světlo**

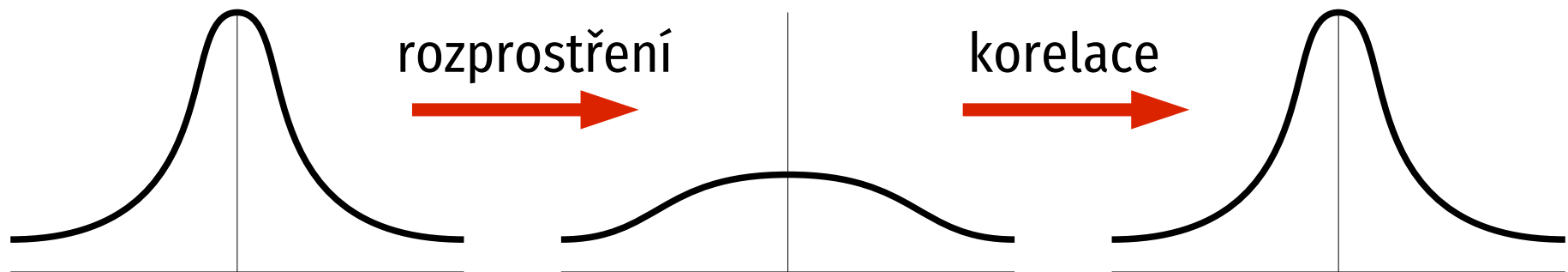
- definováno ve standardu, nikdy se nevyrábělo
- problém: vyžaduje přímou viditelnost

- **mikrovlny**

- bezlicenční pásma 2,4 a 5 GHz
- nižší frekvence má lepší prostupnost, ale menší šířku pásma a více konfliktů
- různé metody vysílání

802.11b

- první masově rozšířená varianta
- v pásmu 2,4 GHz
- Direct Sequence Spread-Spectrum (DSSS) – menší amplituda, ale širší pásmo
- max. 11 Mb/s



Problémy 802.11b

- reálná max. rychlost sotva poloviční (velká režie)
- pásmo 2,4 GHz je přetíženo, problémy s rušením
- v dostupném pásmu je 11 kanálů (13 v Evropě), ale měly by být alespoň o 5 od sebe, aby se nerušily – reálně použitelné jsou kanály 1, 6 a 11 (případně 1, 5, 9, 13)

802.11a

- starší než 802.11b, ale rozšířil se později
- pásmo 5 GHz (podstatně širší, ale vyšší útlum)
- Orthogonal Frequency Division Multiplexing (OFDM)
 - rozkládá signál do desítek nezávislých frekvencí; tento princip používá i ADSL
- různé modulace + samoopravné kódy
- 8 rychlostí, max. 54 Mb/s

802.11g

- snaha o vyšší rychlost při zachování zpětné kompatibility s 802.11b
- pásmo 2,4 GHz
- Orthogonal Frequency Division Multiplexing
- rychlosti až 54 Mb/s
- podporuje i režimy 802.11b a režim ochrany (řídící informace se vysílají tak, aby je zachytila i 802.11b zařízení) – pomalejší

802.11h

- v Evropě kladeny technické požadavky na zařízení v bezlicenčním pásmu 5 GHz
 - DFS – dynamická volba kmitočtu
 - TPC – automatická regulace výkonu
- 802.11a je nesplňuje – lze nasadit jen uvnitř budov
- 802.11h doplňuje potřebné vlastnosti, v podstatě evropská verze 802.11a
- novější (2004), málo rozšířená

802.11n

- přijato na podzim 2009
- cíl: čistá přenosová rychlost alespoň 100 Mb/s
- pásmo 2,4 i 5 GHz
- zařízení jsou běžně dostupná na trhu
 - cena se příliš neliší od a/b/g

802.11n – vyšší výkon

- Multiple-Input Multiple-Output (MIMO) – více antén pro vysílání a příjem (min. 2×2)
- minimalizace režijních přenosů
 - agregace rámců
 - blokové potvrzování
- 3 režimy činnosti
 - legacy – zpětně kompatibilní (a/b/g)
 - mixed (a/b/g/n)
 - greenfield (pouze n)

Další vývoj (1)

■ 802.11ac

- přijato v lednu 2014
- MIMO (až 8 antén)
- víceuživatelské MIMO – stanice na různých kanálech
- rychlost linky až 867 Mb/s, celková několik Gb/s

■ 802.11ad (WiGig)

- přijato 2012
- tři frekvenční pásma: 2,4 GHz, 5 GHz a 60 GHz
- až 7 Gb/s

Další vývoj (2)

■ Wi-Fi 6 aneb 802.11ax

- přijato 2021, navazuje na 802.11ac
- nový systém označování
- pásma 2,4 a 5 GHz, verze 6E navíc 6 GHz
- MIMO (až 8x8)
- víceuživatelské MIMO – stanice na různých kanálech
- celková rychlost až 9,6 Gb/s

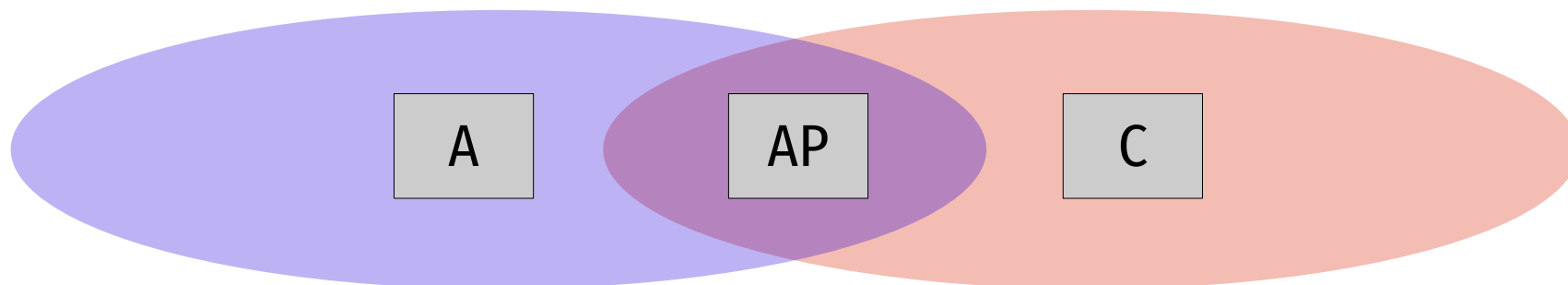
Mikrovlnné problémy

- **nekvalitní médium**

- rušení, útlum (vzdálenost, překážky)
- důsledek: **potvrzování**, přenos rámce a jeho potvrzení tvoří atomickou operaci

- **skrytý uzel**

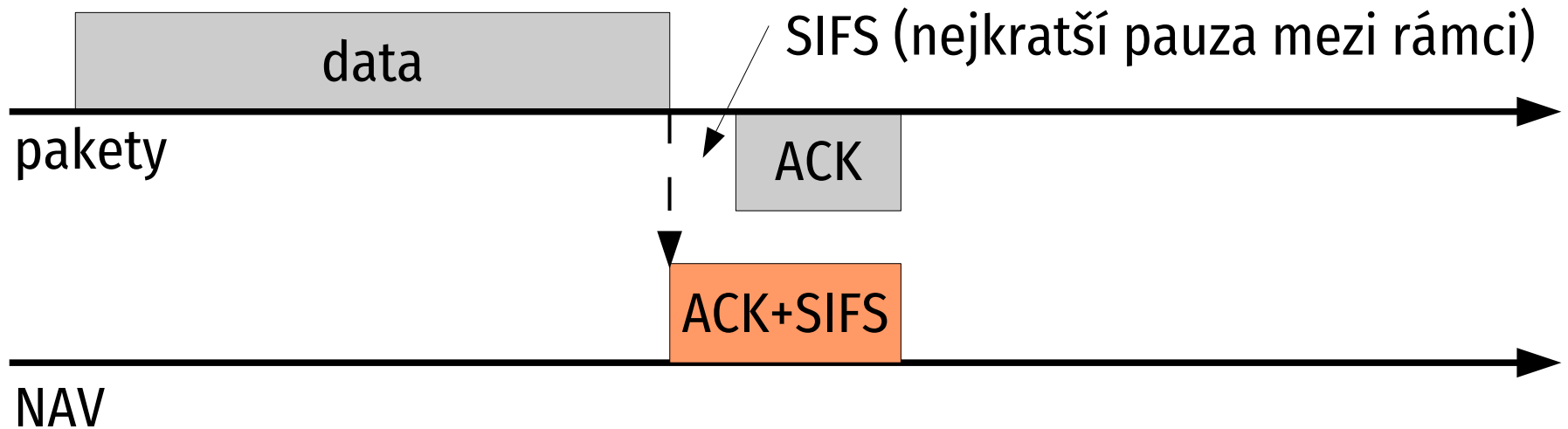
- A a C se přímo neslyší, jejich signály se ale u AP ruší



Virtuální naslouchání

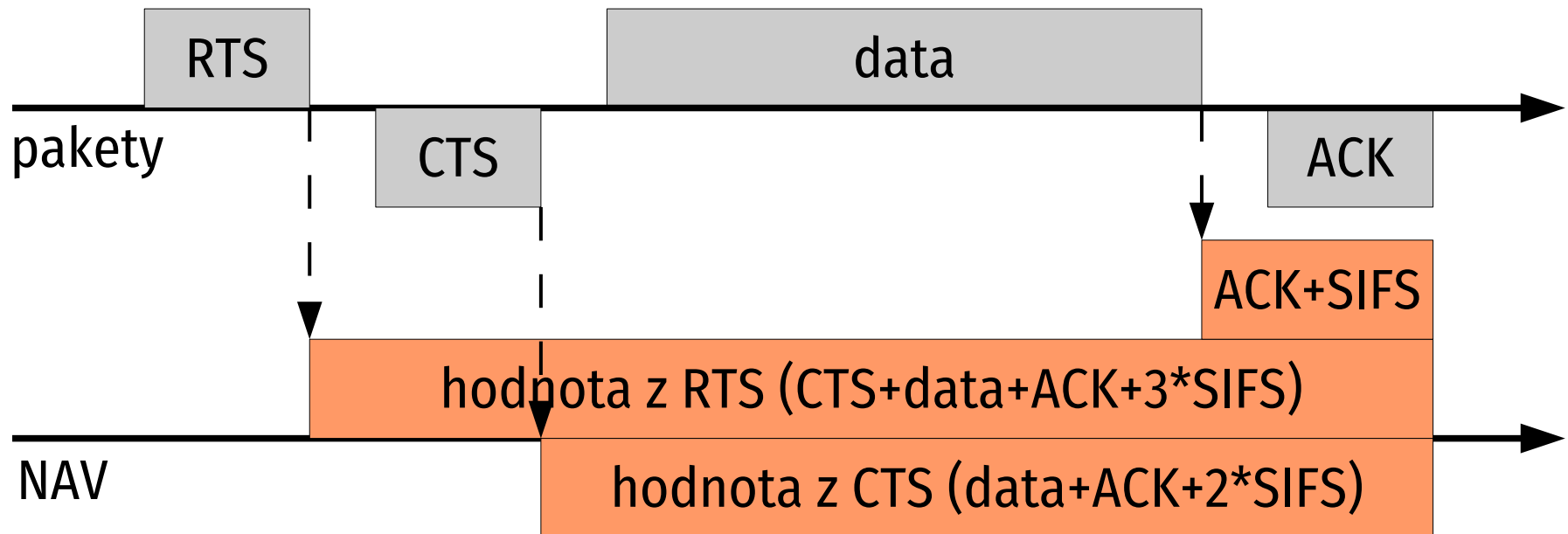
- řeší problém skrytého uzlu
- každá stanice si vede **Network Allocation Vector (NAV)** – čas, po který je médium rezervováno
- je-li NAV nenulový, médium je považováno za obsazené, i když žádný signál nepřichází
- hodnota NAV se přebírá z přenášených rámců

Základní výměna



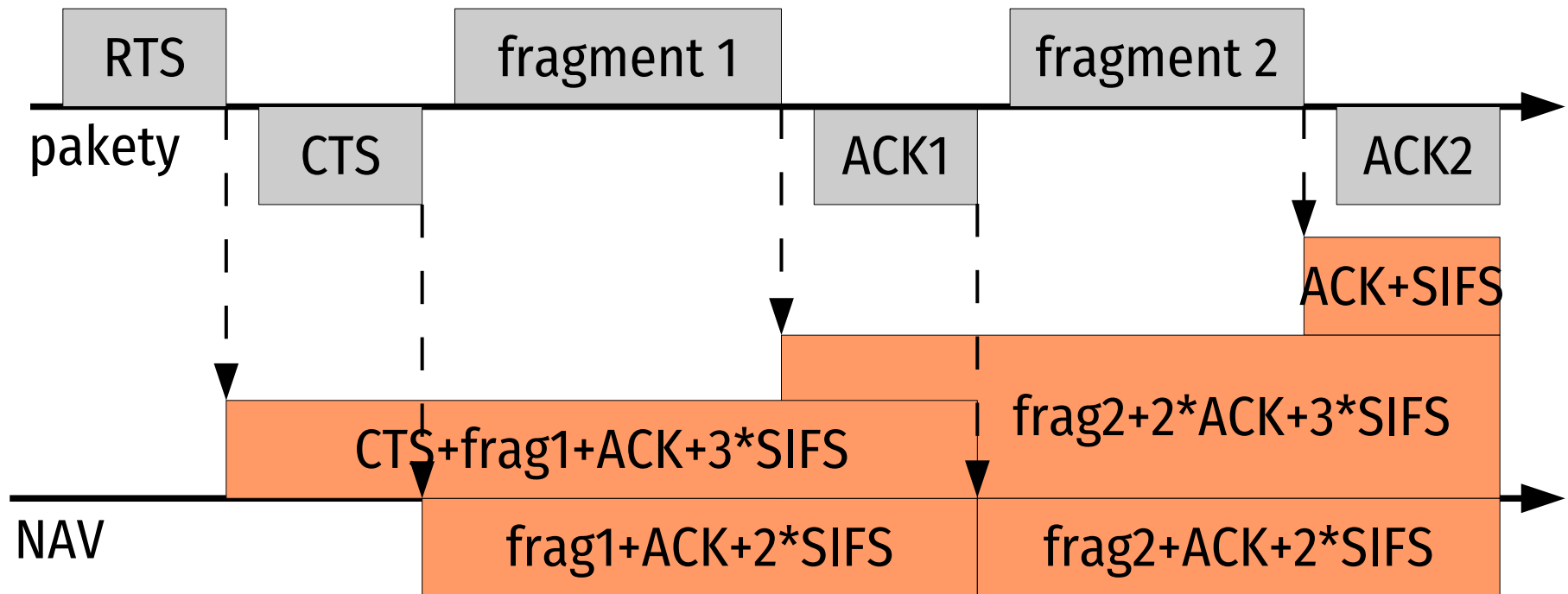
- pro krátké rámce
- vysílající pošle rovnou data, příjemce potvrdí
- NAV si odvozuje každý sám ze známých délek

RTS/CTS výměna



- vysílající avizuje přenos (Request to Send), příjemce potvrdí připravenost (Clear to Send)
- ostatní si nastaví NAV z hodnoty RTS či CTS

Fragmentace



- dlouhé rámce lépe rozložit na několik menších (zvyšuje pravděpodobnost úspěšného doručení)
- NAV se průběžně aktualizuje

Přístup k médiu

- **Distributed Coordination Function (DCF)**
 - bez centrálního řízení, stanice soutěží o médium
 - algoritmus CSMA/CA
- **Point Coordination Function (PCF)**
 - přístupový bod řídí veškeré přenosy
 - málo implementováno
 - kombinuje se s DCF

Intervaly v IEEE 802.11

- **SIFS** – Short Interframe Space
 - mezi rámci tvořícími atomickou operaci
- **PIFS** – PCF Interframe Space
 - mezi rámci při centrálním řízení
- **DIFS** – DCF Interframe Space
 - mezi rámci při distribuovaném řízení
- **EIFS** – Extended Interframe Space
 - při přenosové chybě

CSMA/CA

■ Carrier Sense Multiple Access with Collision Avoidance

1. je-li médium volné po dobu DIFS, začne vysílat
pokud protějšek nepotvrdí příjem, zahájí exp. čekání
2. je-li obsazeno, počká na uvolnění a zahájí exp. čekání
3. exponenciální čekání: po uplynutí DIFS začíná soutěžní
okno – rozděleno na sloty; stanice náhodně vybere slot
a pokud nikdo nezačne dříve, zahájí vysílání (jinak
zpět 2); při neúspěchu zdvojnásobí počet slotů
4. omezený počet pokusů

Formát rámce

2	2	6	6	6	2	6	0–2312	4
řízení	trvání	adresa 1	adresa 2	adresa 3	poř.	adresa 4	data	CRC

- **řízení:** příznaky určující typ rámce (datový, řídicí, správní) a další parametry
- **trvání:** očekávaná doba přenosu následujícího rámce (nastavení NAV)
- **adresy:** odesílatel, příjemce a až dva AP (význam závisí na typu rámce)
- **pořadí:** umožňuje číslovat rámce
- **CRC:** kontrolní součet

Bezpečnost

- dva okruhy problémů:
 - využití sítě neoprávněnými stanicemi
 - odposlech dat
- vstup do buňky:
 - autentizace – ověření, zda smí být vpuštěna
 - asociace – technické začlenění do buňky

Autentizace

- **volný přístup**
 - implicitní nastavení nových AP
- **podle MAC adres**
 - obtížně se udržuje, snadno se falšuje
- **šifrování + heslo**
 - nejčastější, dostatečně bezpečné a jednoduché
- **IEEE 802.1X**
 - centrálně řízené, pro větší počty uživatelů

IEEE 802.1X

- obecné pro lokální sítě (i pro Ethernet)
- **autentizuje uživatele, nikoli hardware**
umožňuje vzájemnou autentizaci obou stran
- zpočátku provoz počítače blokován, umožněny jen pakety 802.1X, po úspěšné autentizaci se otevře
- na počítači nutný klient, tzv. suplikant; AP ověřuje proti autentizačnímu serveru protokolem RADIUS
- vychází z Extensible Authentication Protocol (EAP)

WEP

- **Wired Equivalent Privacy**
- součást původního 802.11, šifra RC4
- chrání data během bezdrátové přepravy (nikoli v distribučním systému)
 - utajení (aby data nemohl číst neoprávněný uživatel)
 - integrita (aby nemohla být změněna)
 - autentičnost (ověření pravosti zdroje)
- slabiny: nedostatky algoritmu, společné heslo
- **považován za nedostatečný**

IEEE 802.11i

- vylepšené zabezpečení, dva různé protokoly:
- **Temporal Integrity Key Protocol (TKIP)**
 - též WEP2, WPA
 - využívá čipy pro WEP, ale s individuálními a dočasnými klíči (každý rámec jiný) a delšími inicializačními vektory
- **Counter Mode with CBC-MAC Protocol (CCMP)**
 - silnější šifrovací algoritmy, vyžaduje jiný hardware
 - vychází z šifry Advanced Encryption Standard (AES)

Wi-Fi Alliance

- sdružení výrobců HW
- založeno s cílem zlepšit interoperabilitu jednotlivých výrobků
- **certifikát Wi-Fi** zaručuje splnění daných testů
- vydává vlastní specifikace
 - např. dlouhý vývoj 802.11i vedl k vydání **Wi-Fi Protected Access (WPA)**, což je TKIP z návrhu 802.11i



vytvořeno s podporou
projektu ESF





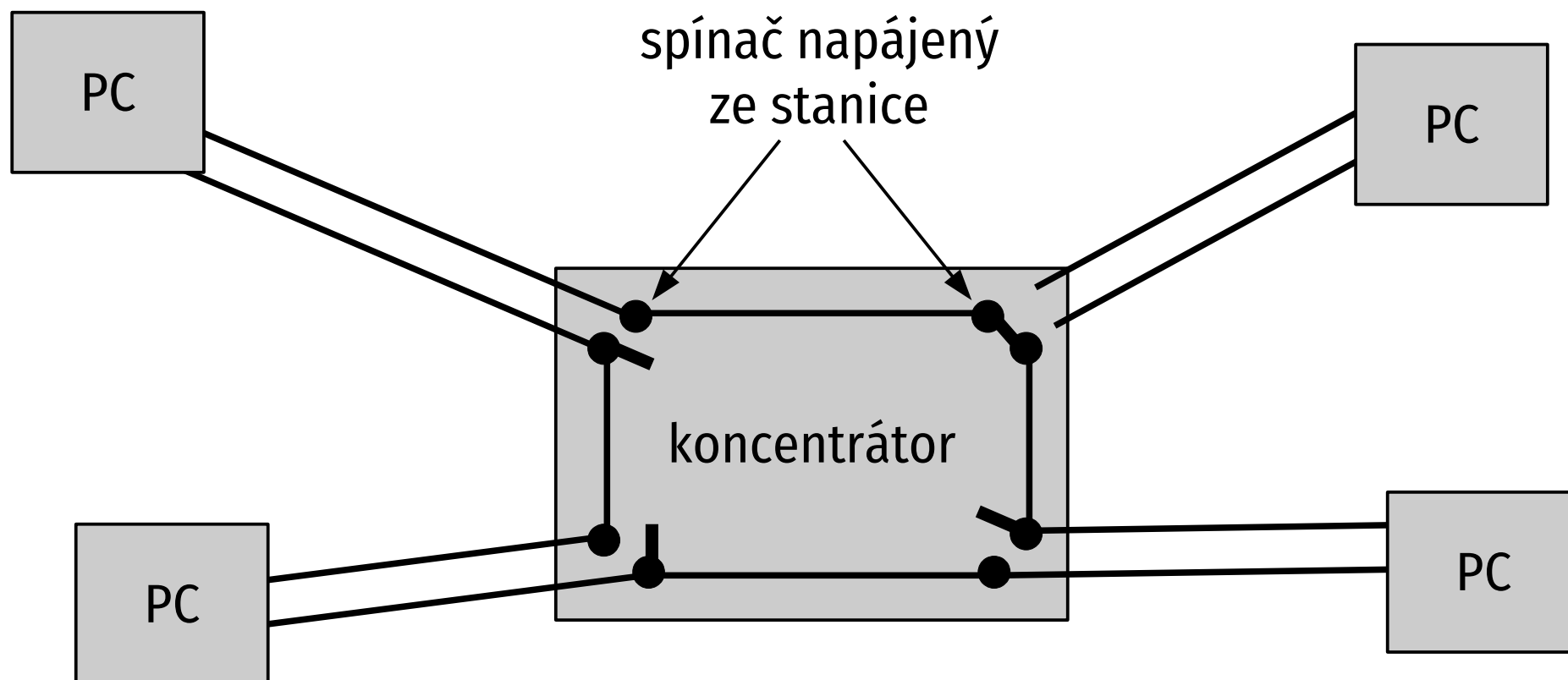
Alternativy Ethernetu

Token Ring

- IEEE 802.5
- vytvořilo IBM
- kruhová topologie, dvoubodové spoje na UTP
- rychlost 4, později 16 Mb/s
- přístup k médiu:
 - v kruhu obíhá token – oprávnění promluvit
 - stanice musí počkat, až dostane token; pak jej zadrží, odešle datový rámec a pošle token dál

Koncentrátor

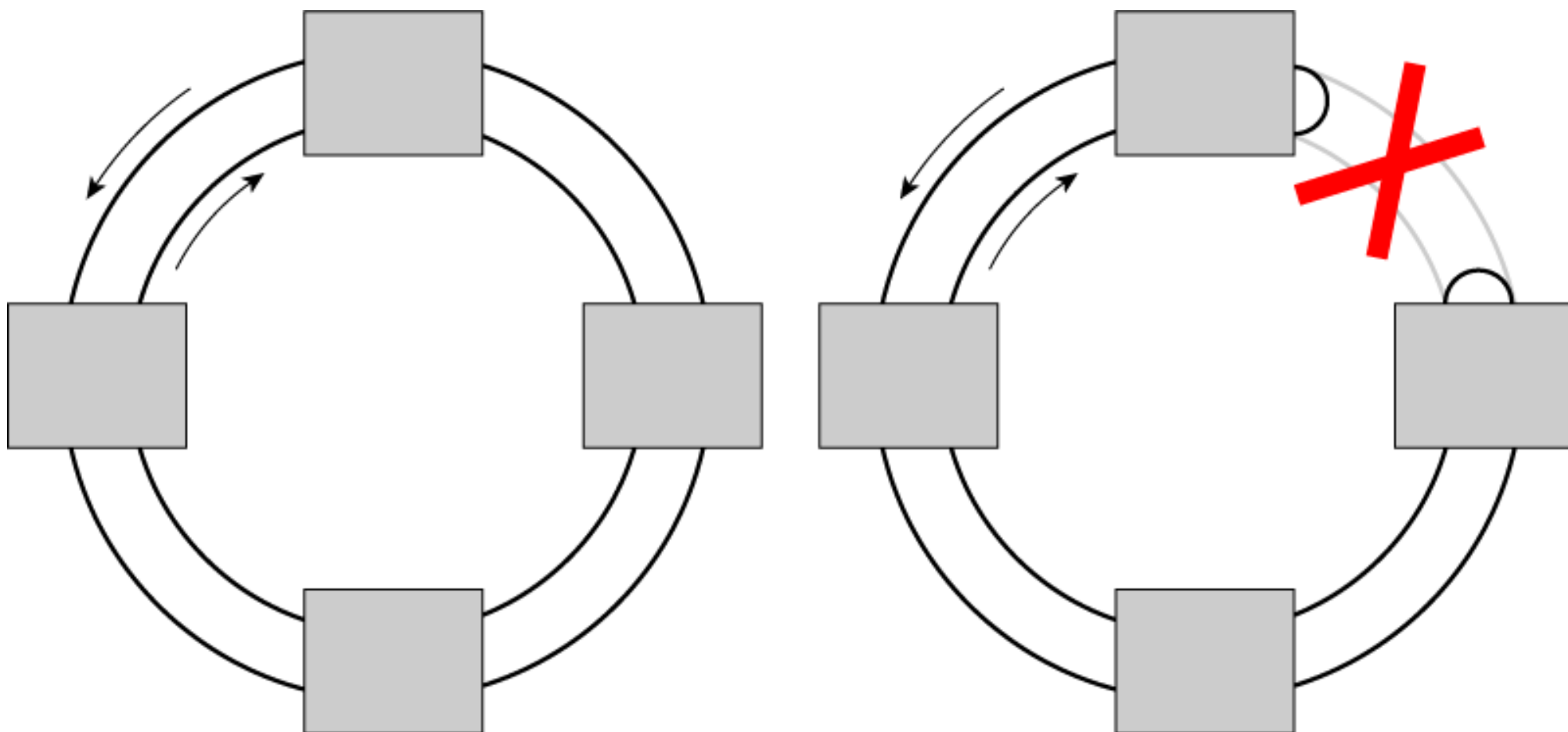
- řeší problém s přerušením kruhu
- de facto převede na hvězdu, logicky zůstává kruh



FDDI

- **Fibre Distributed Data Interface, ISO 9314**
- rychlost 100 Mb/s
- vícevidová vlákna, celkový dosah až 200 km
- dva protiběžné kruhy – primární a sekundární zálohuji se navzájem
- přístup k médiu opět řídí token, dílčí změny proti Token Ringu

Přerušení spoje



ATM

- **Asynchronous Transfer Mode**
- snaha o univerzální technologii – audio, video, data
- stromová topologie, dvoubodové spoje
- rychlosti 25, **155**, 622 Mb/s
- spojovaná služba (unikát)
- ATM přepínače (ATM switch) – à la ústředny

Buňky a okruhy

- data přepravována v **buňkách**
 - konstantní velikost – usnadňuje zpracování
 - velmi malé: 53 B, z toho 5 B hlavička (malá, identifikuje příslušnost k cestě a kanálu), 48 B data
- **okruhy**
 - **permanentní (PVC)** – stálý, nastaven správcem
 - **přepínaný (SVC)** – vytvářen na žádost aplikace, vyžaduje signalizaci pro domluvu zúčastněných (UNI – User-Network Interface), těžké problémy s kompatibilitou

Quality of Service (QoS)

- aplikace může při navazování spojení požádat o určité parametry (kapacitu, zpoždění, rozptyl,...)
- pokud ATM vstava přijme, garantuje jejich dodržení
- různé **přenosové třídy**
 - **CBR** – konstantní přenosová rychlost
 - **VBR** – průměrná rychlost + omezený počet buněk ve shluku posílaných maximální rychlostí
 - **ABR** – proměnlivá rychlost, omezená ztrátovost

Proč ATM neuspělo

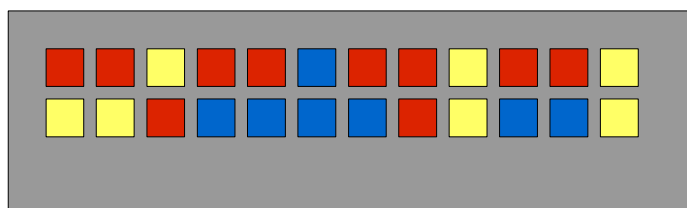
- ve 2. polovině 90. let hit vyspělých sítí
- radikálně odlišné
 - problematická spolupráce s jinými technologiemi
 - zcela nezvyklé pro autory SW
- pomalá standardizace, nekompatibility
- problémy s broadcastem (zoufalé broadcast servery)
- drahé
- nenabídlo gigabitové rychlosti

Virtuální lokální sítě (VLAN)

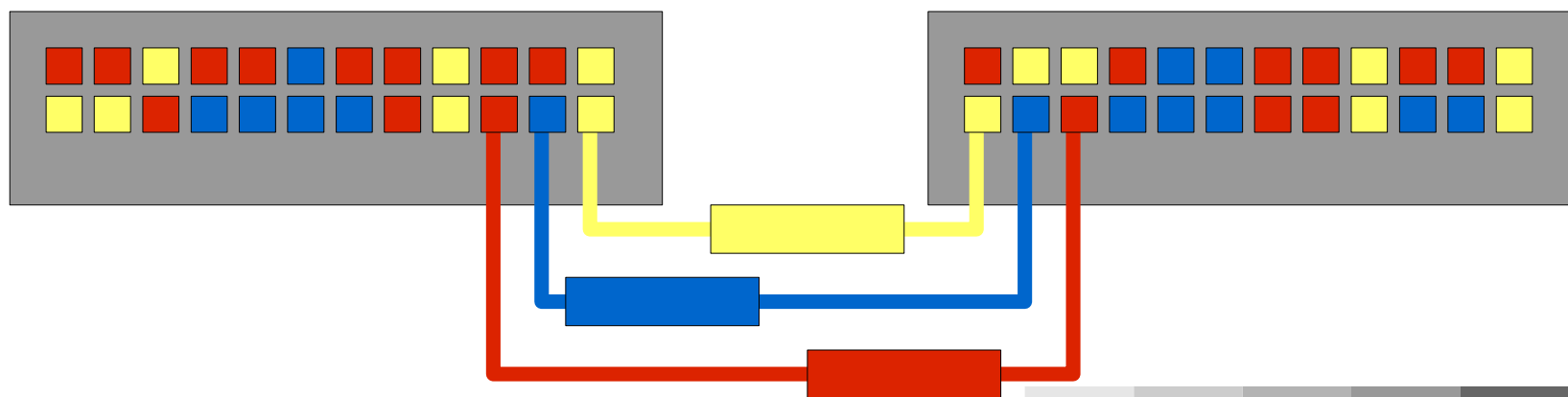
Co je VLAN

- část síťové infrastruktury (typicky ethernetové), která se chová jako samostatná LAN
- softwarově konfigurovatelná, může zasahovat do několika budov
- počítače komunikují přímo, distribuují se broadcast rámce apod.
- příklad: výdejní systém menzy – jedna izolovaná VLAN zasahující do několika lokalit

Původní řešení

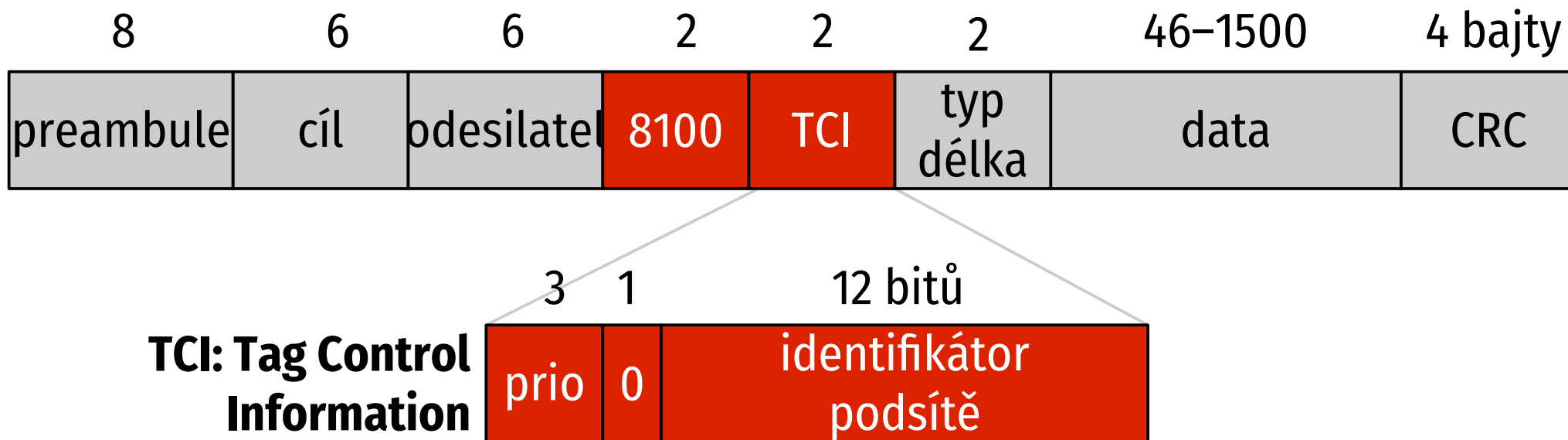


- rozdělení portů v přepínači
- **problém:** rozšíření do dalších přepínačů – každá podsíť vyžaduje jeden propojovací port



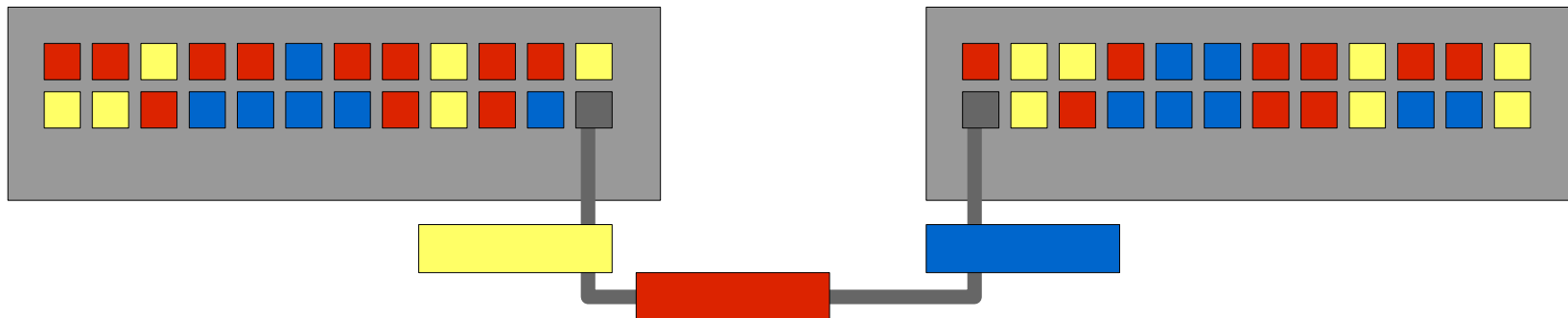
IEEE 802.1Q

- umožňuje několik podsítí na jednom portu
- rozšířen formát rámce: přibyla položka identifikující podsíť (max. délka se prodloužila o 4 B)



Použití IEEE 802.1Q

- porty dvou typů:
 - **značkové** – používají formát rámců podle 802.1Q, jednotlivé rámce označeny podle příslušnosti k VLAN; musí podporovat i protější zařízení (přepínač, server)
 - **neznačkové** – pevně přiřazeny do jedné VLAN
- jedním kabelem lze přenášet desítky VLAN



vytvořeno s podporou
projektu ESF





Internet



Standardizace Internetu (1)

- **RFC – Request for Comments**, základní dokumenty
- identifikovány čísla, po vydání se nemění – místo změny se nahradí jiným RFC
- přidělen stav
 - **proposed standard**: návrh (ustálené, bez implementace)
 - **Internet standard**: zralé, stabilní
 - **experimental**: zkoumá se
 - **informational**: čistě informační
 - **historic**: nahrazeno novějším

Standardizace Internetu (2)

- draft – pracovní dokument, platnost 1/2 roku
- **IETF – Internet Engineering Task Force**
 - velká komunita návrhářů, provozovatelů, výzkumníků...
 - účast dobrovolná
 - vyvíjí nové protokoly, služby,...
 - organizována do tématických pracovních skupin (working groups)
 - www.ietf.org

Internet Protocol (IP)

- RFC 791
- hlava rodiny TCP/IP
- drží Internet pohromadě – podpora jednotného IP umožňuje kterémukoli zařízení komunikovat s ostatními
- **bez spojení** (samostatné datagramy)
- **bez záruk** (best effort)

IP adresa

- každé rozhraní má svou adresu
- **32bitové číslo (4 bajty)**
- tečkovaný desítkový zápis 147.230.16.8
- celosvětově jednoznačné, distribuované přidělování
- Internet není síť počítačů, ale síť sítí – hierarchická struktura adresy:



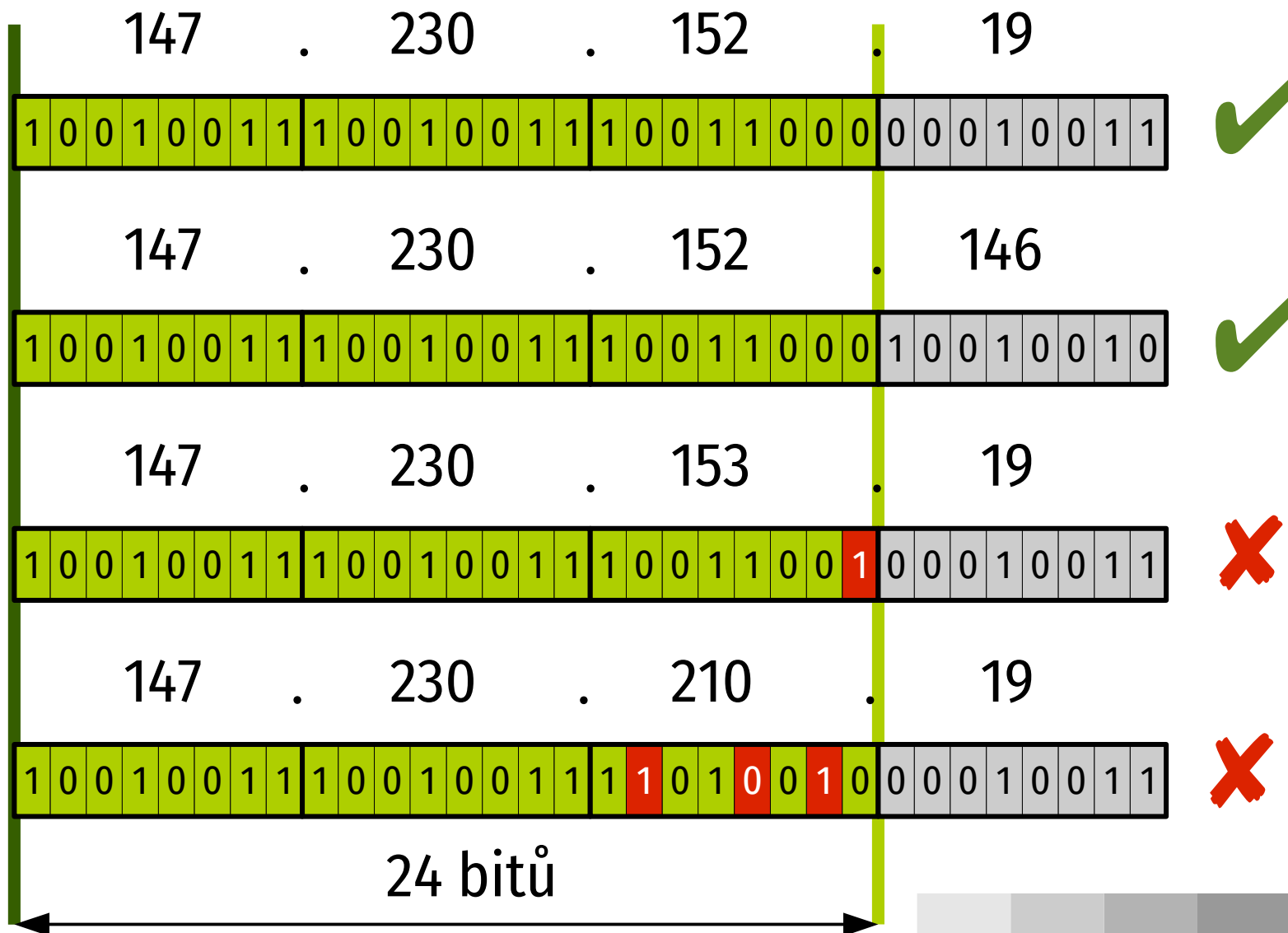
Podsítě

- počítače **přímo spojené ve 2. vrstvě** (Ethernetem) – počítače ve stejné podsíti spolu komunikují přímo
- **maska podsítě** určuje hranici mezi adresou podsítě a počítače
- obsahuje 1 v bitech adresy sítě a podsítě, 0 jinde
- 147.230.16.8 s maskou podsítě 255.255.255.0:
sít' 147.230, podsít' 16, počítač 8
prefix podsítě 147.230.16.0/24
- hranici **stanoví správce sítě**

Prefix

- **začátek IP adresy**
- délka může být různá, zápis s lomítkem – odděluje hodnotu adresy od specifikace významných bitů
 - **147.230.0.0/16** – kolik bitů od začátku adresy platí
 - **147.230.0.0/255.255.0.0** – maska, 11...1 na místě významných bitů, 00...0 na místě nevýznamných
 - část adresy, jež není součástí prefixu, bývá vynulována
- používají se při přidělování adres, směrování,...

Příslušnost k 147.230.152.0/24



Classless Internet Domain Routing

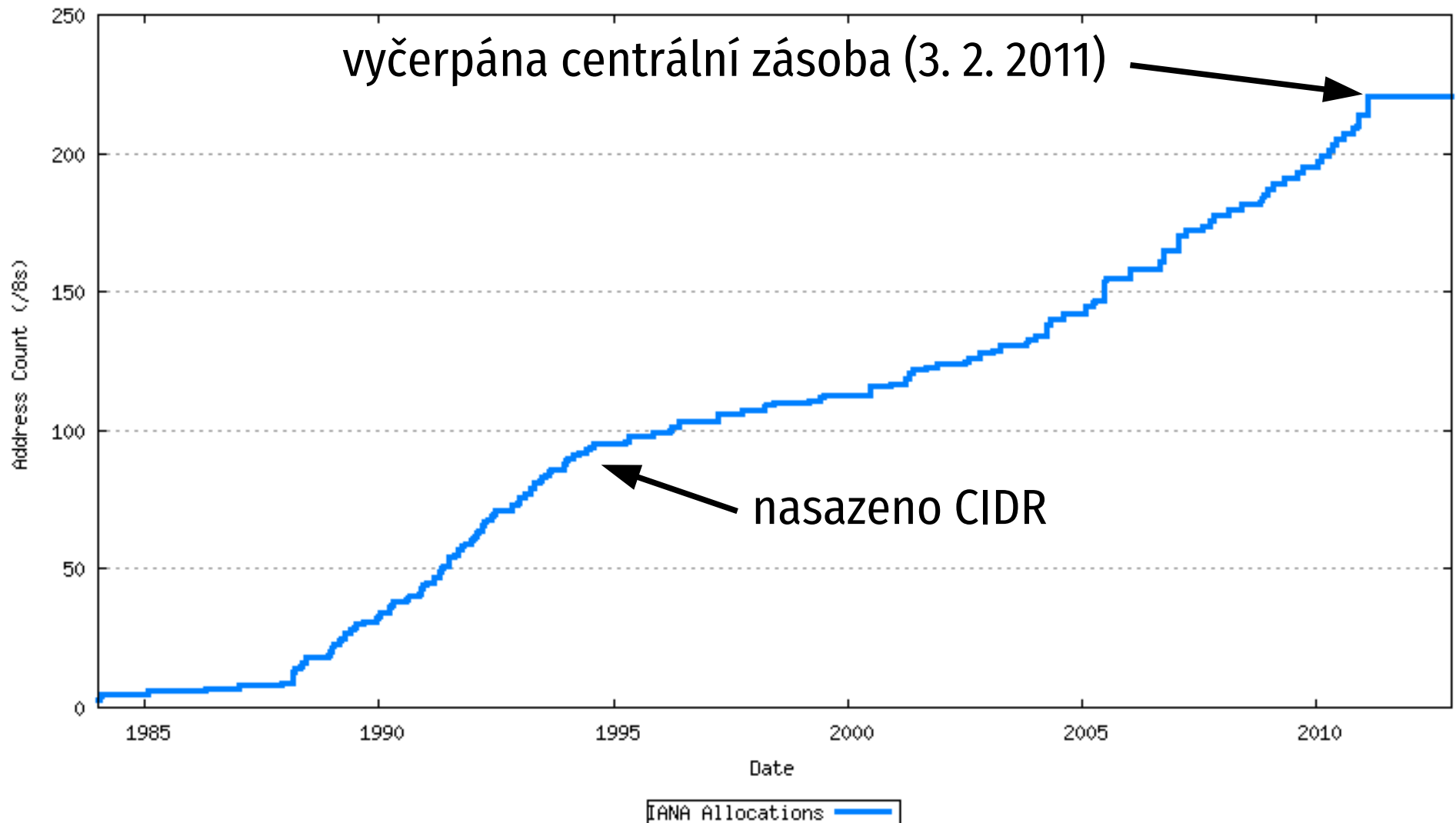
- původně: 3 délky adresy sítě – třídy A/8, B/16, C/24
- neosvědčilo se – málo adres třídy B, velké směrovací tabulky, plýtvání adresami; vzniklo **CIDR**
- síť dostane jen tolik prostoru, kolik opravdu potřebuje
- agregace prefixů
 - ISP dostane prefix, např. 147.230.0.0/16
 - jeho části (např. 147.230.1.0/24) přiděluje zákazníkům
 - mimo síť ISP lze celý jeho prostor shrnout pod jediný prefix 147.230.0.0/16

Přidělování adres

- **IANA (Internet Assigned Numbers Authority)**
 - centrální autorita
- **RIR (Regional Internet Registry)**
 - **RIPE NCC** (Evropa a Blízký východ), **ARIN** (Severní Amerika), **LACNIC** (Latinská Amerika), **APNIC** (Asie a Pacifik), **AFRINIC** (Afrika)
- **LIR (Local Internet Registry)**
 - poskytovatel Internetu
- zákazník

Spotřeba IP adres

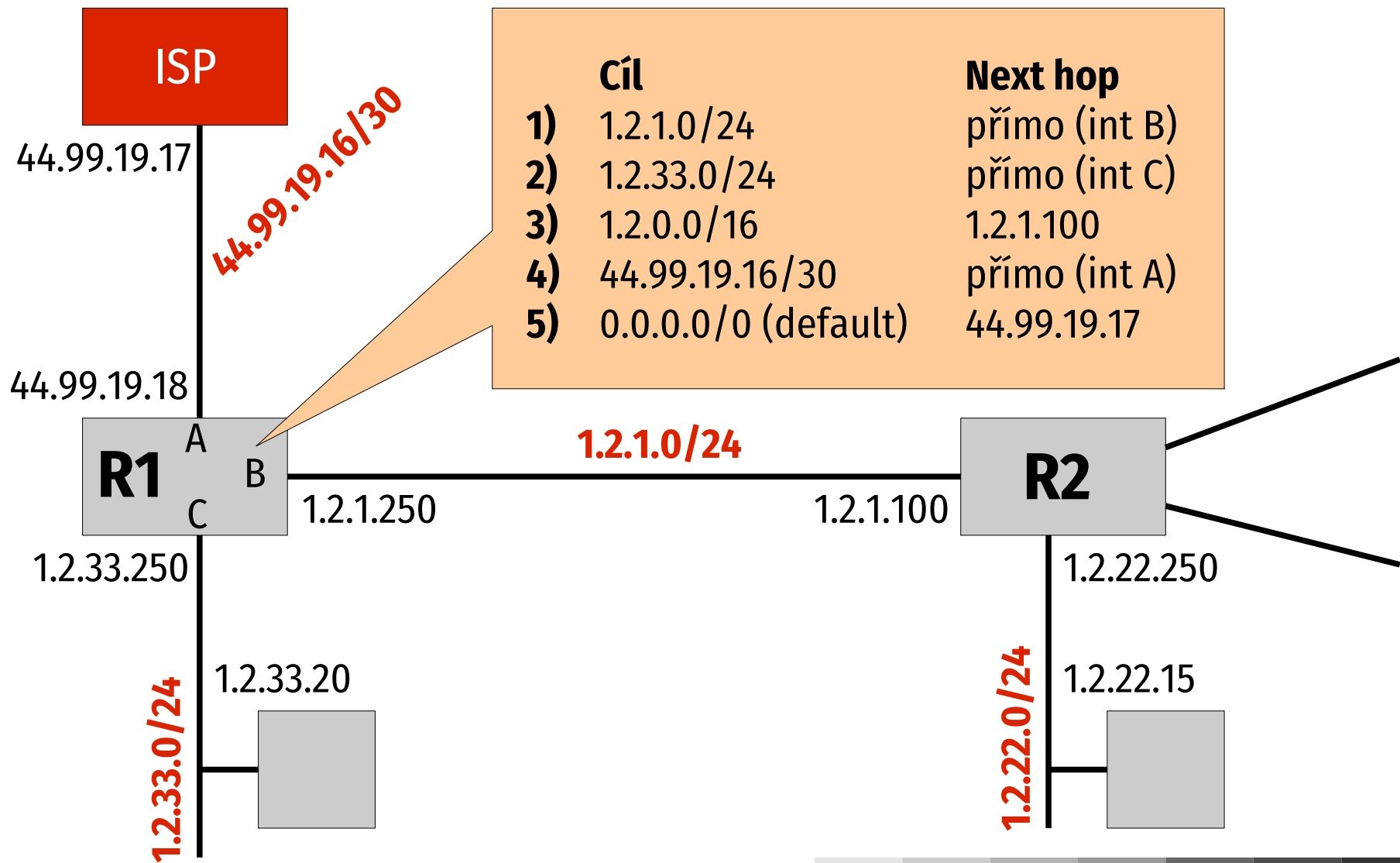
Time Series of IANA Allocations



Základní směrování

- **směrovací tabulka** – základní datová struktura
 - **cíl** – prefix adresy
 - **next hop** – komu předat pakety pro tento cíl (soused)
- **směrovací rozhodnutí**
 - podle adresy příjemce z IP datagramu
 - vybere všechny záznamy ze směrovací tabulky, kde **cíl odpovídá adrese příjemce**
 - z nich použije záznam s **nejdelším cílovým prefixem** (nejkonkrétnější)

Příklad směrovací tabulky



Příklady rozhodnutí R1

- cíl: **1.2.33.20**
 - použitelné záznamy 2, 3, 5
 - nejkonkrétnější je 2 – **doručí přímo rozhraním C**
- cíl: **1.2.22.15**
 - použitelné záznamy 3, 5
 - nejkonkrétnější je 3 – **předá na 1.2.1.100 (R2)**
- cíl: **147.230.16.8**
 - použitelné jen 5 – **předá na 44.99.19.17**

Terminologie

- směruje každé zařízení zapojené do Internetu (včetně koncových)
- **směrovač (router)** – propojuje několik IP (pod)sítí a předává mezi nimi datagramy
- **L3 přepínač (L3 switch)** – marketingový pojem, původně jednoduchý a rychlý směrovač s omezenými funkcemi, dnes totéž co směrovač
- **L2/L3 přepínač** – ethernetový přepínač i IP směrovač v jednom zařízení, závisí na konfiguraci

IP datagram (1)

verze	délka hlavičky	TOS	celková délka [B]	
identifikátor			přízn.	posun fragmentu
TTL		protokol	CRC hlavičky	
odesílatel (IP adresa)				
adresát (IP adresa)				
volby (nepovinné, proměnlivé složení)				
data				

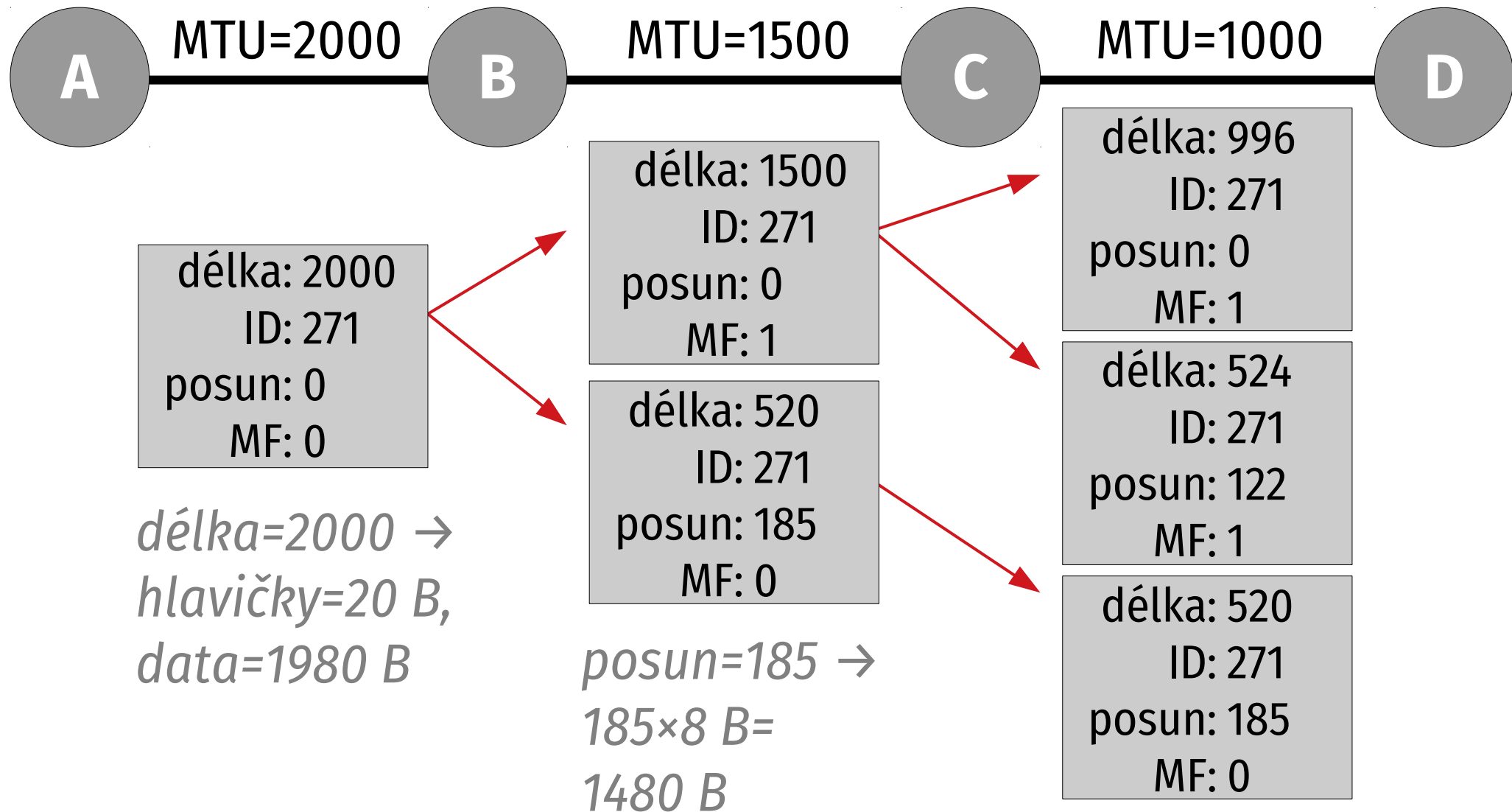
IP datagram (2)

- **verze:** v současnosti 4
- **délka hlavičky:** ve 32bitových slovech (max. 60 B)
- **TOS:** Type of Service, požadavky na přepravu
- **celková délka:** max. 65 535 B
- **TTL:** Time to Live, každý směrovač zmenší alespoň o 1, při vynulování zahodí – ochrana proti zacyklení
- **protokol:** kterému protokolu 4. vrstvy patří data
- **CRC:** nezahrnuje data

Fragmentace (1)

- maximální velikost paketu (**MTU, Maximum Transmission Unit**) se liší pro různé fyzické sítě
- je-li datagram $>$ MTU, bude rozdělen na fragmenty:
 - všechny mají stejný **identifikátor**
 - **posun fragmentu** udává, na které pozici původního datagramu začínají data tohoto fragmentu (děleno 8)
 - v **příznacích** mají všechny fragmenty kromě posledního nastaven „More Fragments“
 - je aktualizována celková délka

Příklad fragmentace



Fragmentace (2)

- fragmenty jsou samostatnými datagramy
 - přepravovány nezávisle
 - mohou být dále fragmentovány
- skládá až příjemce datagramu
- mezi příznaky je i „Don't fragment“, který zakazuje datagram fragmentovat
- **MTU cesty** – odesílatel se snaží najít co největší velikost, která nezpůsobí fragmentaci; doporučeno, fragmentace snižuje efektivitu

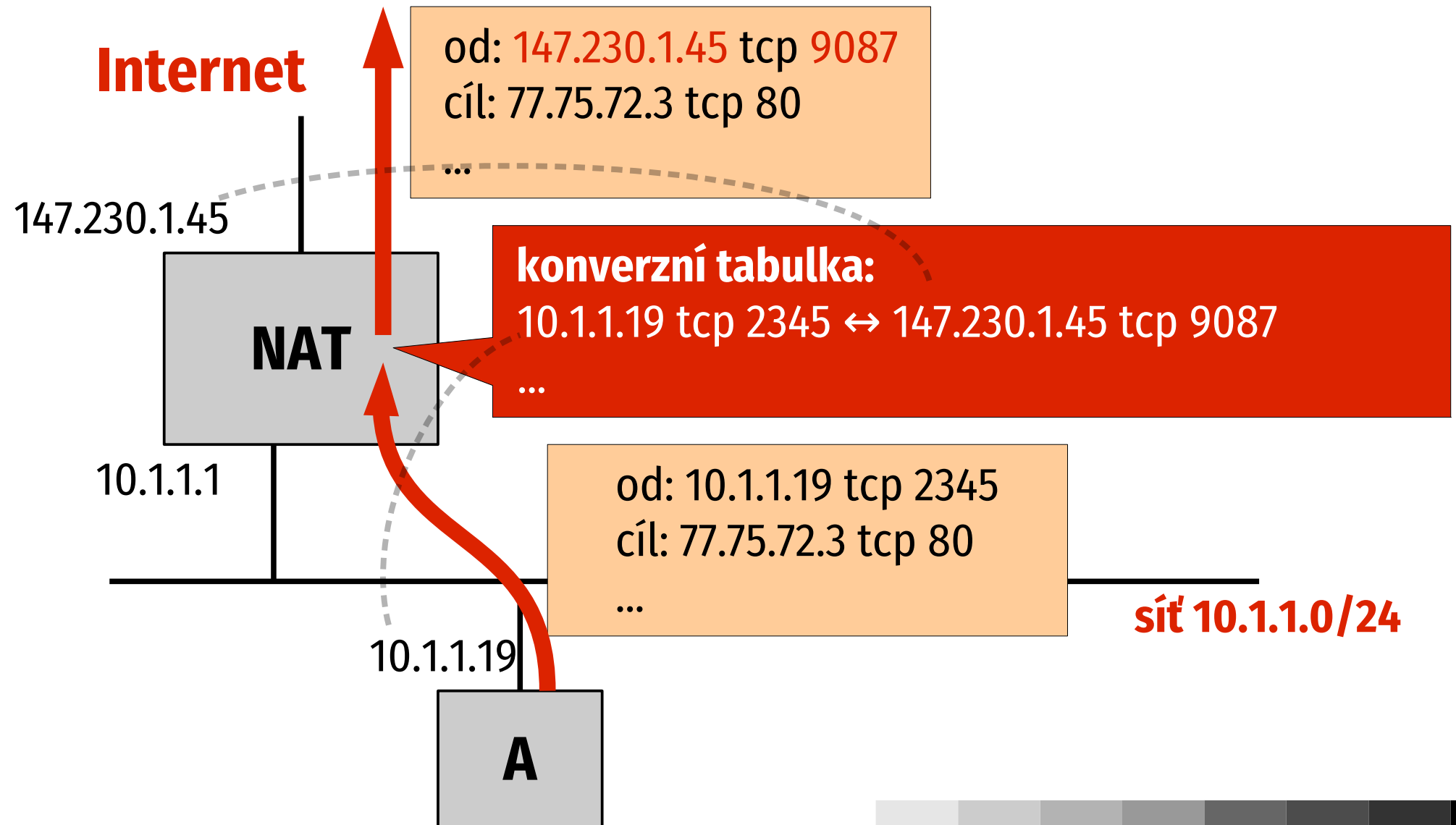
Neveřejné adresy

- RFC 1918 definovalo adresy pro **soukromé sítě**
 - 10.0.0.0/8
 - 172.16.0.0/16
 - 192.168.0.0/16
- nejsou směrovány v Internetu, nesmí překročit lokální síť
- dnes využívány pro rozšíření adresního prostoru v kombinaci s NAT

NAT (1)

- **Network Address Translation, RFC 3022**
- mezi dvěma částmi sítě
- **mění IP adresy a TCP/UDP porty v procházejících IP datagramech**
- typicky: lokální síť s neveřejnými adresami připojená NATem do Internetu – celá síť je adresována jednou veřejnou IP adresou, NAT „zastupuje“ místní stroje
- běžně implementováno např. v ADSL modemech

NAT (2)



NAT (3)

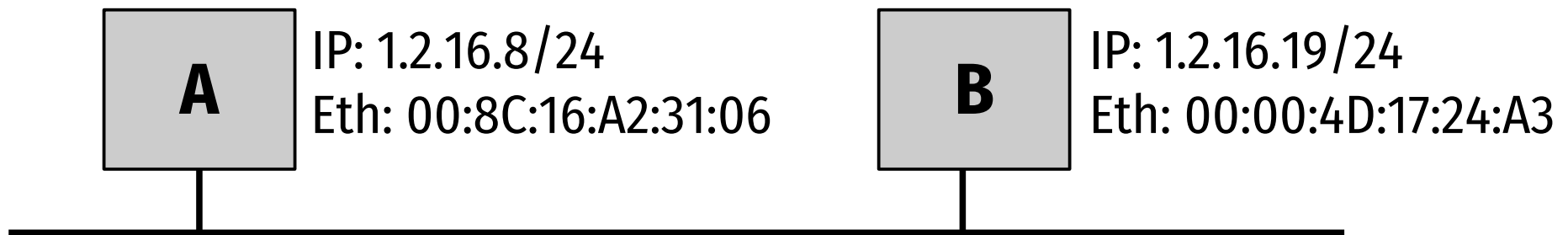
- záznam v konverzní tabulce se vytváří, když počítač „zevnitř“ odesílá paket „ven“
- **problémy NATu:**
 - komunikaci nutno navazovat zevnitř – dokud není záznam v tabulce, jsou vnitřní počítače nedosažitelné (nemají veřejné adresy)
 - narušuje přímou komunikaci (videokonference) – nutno přes prostředníka s veřejnou adresou
 - omezení dostupnosti vnitřní sítě má pozitivní dopady na bezpečnost

ICMP

- **Internet Control Message Protocol, RFC 792**
- servisní hlášení IP (součást 3. vrstvy)
 - zprávy o chybách (nedosažitelný cíl, vypršení TTL, zakázaná fragmentace, chybný datagram,...)
 - opravy směrování
 - test dosažitelnosti (ping)
 - informační zprávy (aktuální čas, maska podsítě,...)
- ICMP útoky (zahlcení) – ICMP někdy blokováno

ARP

- **Address Resolution Protocol, RFC 826**
- jak z IP adresy zjistit linkovou (MAC)



- **A→všem:** Kdo má IP 1.2.16.19? Já jsem 1.2.16.8, Ethernet 00:8C:16:A2:31:06.
- **všichni:** zapíší do ARP cache adresy A
- **B→A:** Já jsem 1.2.16.19, Ethernet 00:00:4D:17:24:A3.

RARP

- **Reverse Address Resolution Protocol**
- umožňuje stanici zjistit vlastní IP adresu
- RARP server má tabulku s MAC adresami a odpovídajícími IP
- **A→všem:** Kdo jsem? Mám Eth 00:8C:16:A2:31:06.
- **RARP server→A:** Tvoje IP je 1.2.16.19.
- stanice ale potřebuje více informací, RARP nestačí
- vývoj: RARP→BOOTP→DHCP

DHCP

- **Dynamic Host Configuration Protocol, RFC 2131**
- poskytuje vše pro automatickou konfiguraci sítě:
 - IP adresu
 - masku podsítě
 - implicitní cestu (default route)
 - adresu lokálního DNS serveru
 - případné další parametry...
- základem DHCP server(y)

DHCP transakce

- **A→všem:** Kdo jsem? Mám Eth 00:8C:16:A2:31:06. (Discovery)
- **DHCP server→A:** Mohu nabídnout 1.2.16.8. (Offer)
- **A→DHCP server:** Prosím 1.2.16.8. (Request)
- **DHCP server→A:** Je tvá. (Acknowledge)
- adresa je „pronajata“ na omezenou dobu, poté stanice žádá o prodloužení u stejného serveru

vytvořeno s podporou
projektu ESF



Směrovací algoritmy

Směrovací algoritmy

- směrování je základní funkcí síťové vrstvy
- jak vznikne a je udržována směrovací tabulka?
- **neadaptivní (statické)** – nepřizpůsobuje se situaci, případné změny se provádějí ručně
- **adaptivní (dynamické)** – reaguje na změny v síti
 - **globální (centralizované)** – řídí centrum
 - **lokální (izolované)** – každý sám za sebe
 - **distribuované** – spolupracují sousedé


Statické směrování

- typické pro koncová zařízení

- **DHCP:**

- IP adresa: 147.230.1.2
- maska podsítě: 255.255.255.0 (24 bitů)
- výchozí brána: 147.230.1.250

- **směrovací tabulka:**

- 
- 147.230.1.0/24 → přímo
 - 0.0.0.0/0 → 147.230.1.250

Centralizované směrování (1)

- v síti je **Routing Control Center (RCC)**
 - každý směrovač mu posílá zprávy o své situaci
 - RCC sbírá, vypočte optimální cesty a rozešle směrovačům jejich tabulky
- **výhody:**
 - globální informace – optimální řešení
 - ulehčí směrovačům

Centralizované směrování (2)

- **nevýhody:**

- špatně škáluje – u velké sítě jsou linky poblíž RCC přetíženy směrovacími informacemi
- hrozí nekonzistence – blízké směrovače dostanou tabulky dříve
- pomalé
- při výpadku centra se přestane aktualizovat

Izolované směrování

- neposílají se žádné informace o stavu sítě, každý se rozhoduje sám za sebe
- příklady:
 - horký brambor – pošle do linky s nejkratší frontou (de facto náhodné)
 - roztékání – pošle všude kromě příchozí
 - zpětné učení – učí se z procházejících paketů

Roztékání

- záplavový algoritmus, flooding
- paket pošle do všech linek kromě té, z níž přišel
- obrovská režie, nutno řešit cykly
- robustní – vždy najde cestu (pokud existuje), dokonce nejlepší cestu (zkouší všechny)
- vhodné pro
 - distribuci informace do celé sítě
 - situace, kde robustnost je klíčová

Zpětné učení

- do paketu se zapisuje vzdálenost, kterou urazil
- směrovač se dozví, že příchozí linkou vede cesta k odesilateli nanejvýš dané délky
- problémy:
 - jak začít?
 - jak reagovat na zhoršení?
 - jak agregovat?

Distribuované směrování

- směrovací informace si vyměňují sousedé či malé skupiny směrovačů
- poprvé použito v ARPANETu
- **Autonomní systém (AS)** – část Internetu se společnou směrovací politikou, typicky ISP + zákazníci
- **Interior Gateway Protocol (IGP)** – směrování uvnitř AS, důraz na rychlost, např. RIP, OSPF
- **Exterior Gateway Protocol (EGP)** – směrování mezi AS, důraz na stabilitu, BGP

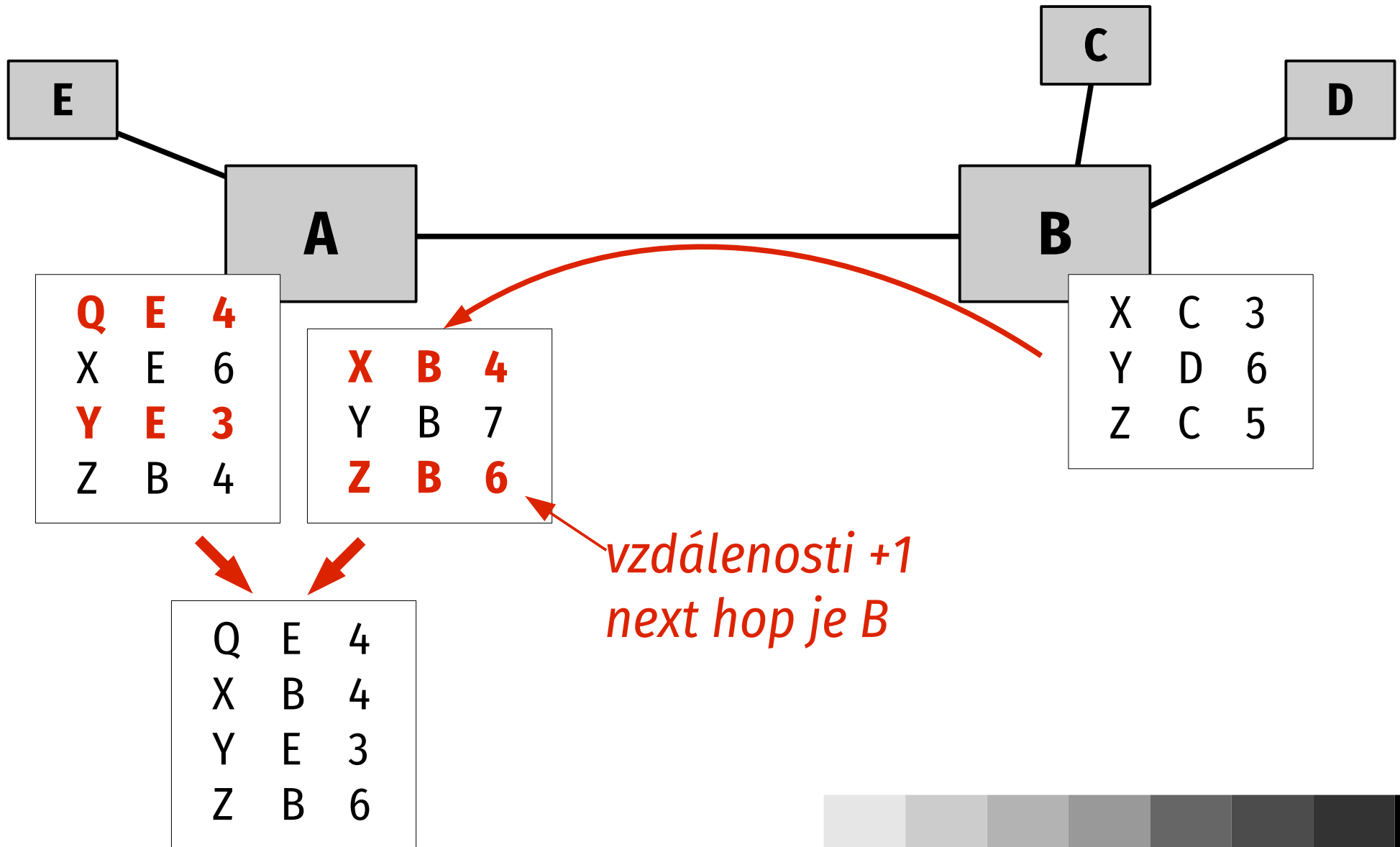
RIP

- **Routing Information Protocol, RFC 1058**
- nejčastější IGP (jednoduchý a dostupný)
- založen na vektoru vzdáleností, ve směrovací tabulce má: cíl, kudy k němu a vzdálenost
- vzdálenost měří ve „skocích“ (hop) – přenos paketu mezi 2 sousedními směrovači má délku 1
- maximální vzdálenost je 15
- jen pro menší sítě

Algoritmus RIP

- každých 30 s pošle směrovací tabulku sousedům
- soused přičte ke vzdálenostem 1 a porovná se svou tabulkou, **změní svůj záznam pokud:**
 - cíl ještě neznal
 - znal k cíli delší cestu
 - cesta k cíli vede přes odesilatele tabulky (aktuálně používaná cesta se zhoršila)

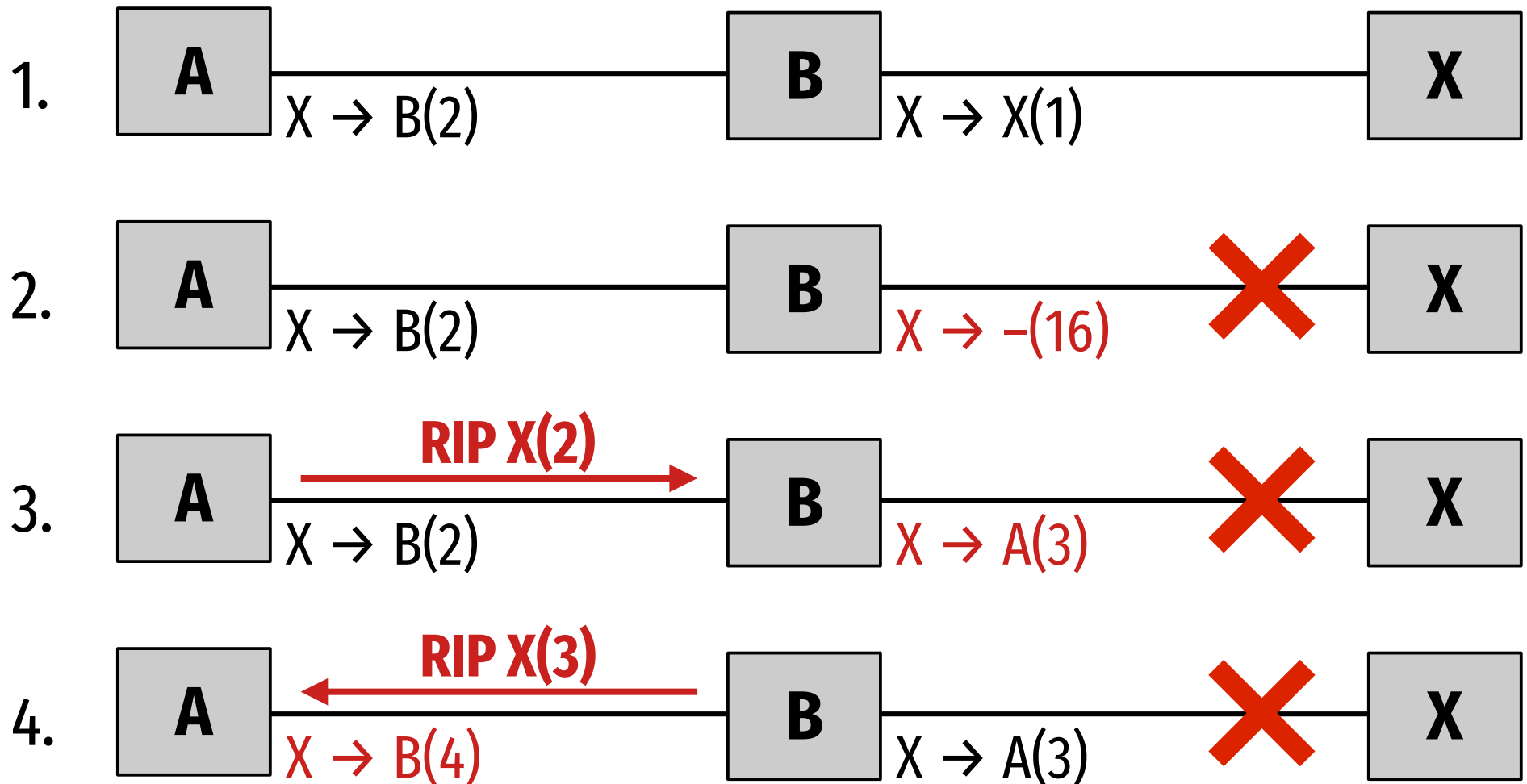
Příklad RIP



Problémy RIPu

- pomalá konvergence, každý krok 30 s
- malá maximální cena, nelze vyjádřit kvalitu linek
- mohou vznikat dočasné cykly:
 - B je spojeno s X, A směřuje X přes B (vzálenost 2)
 - spojení B–X padne, B změní vzdálenost do X na 16
 - A ohlásí: umím X se vzdáleností 2
 - B si aktualizuje cestu do X přes A (vzdálenost 3)
 - vznikne cyklus, postupně se bude zhoršovat, ale trvá několik minut

Vznik směrovacího cyklu



RIP verze 2

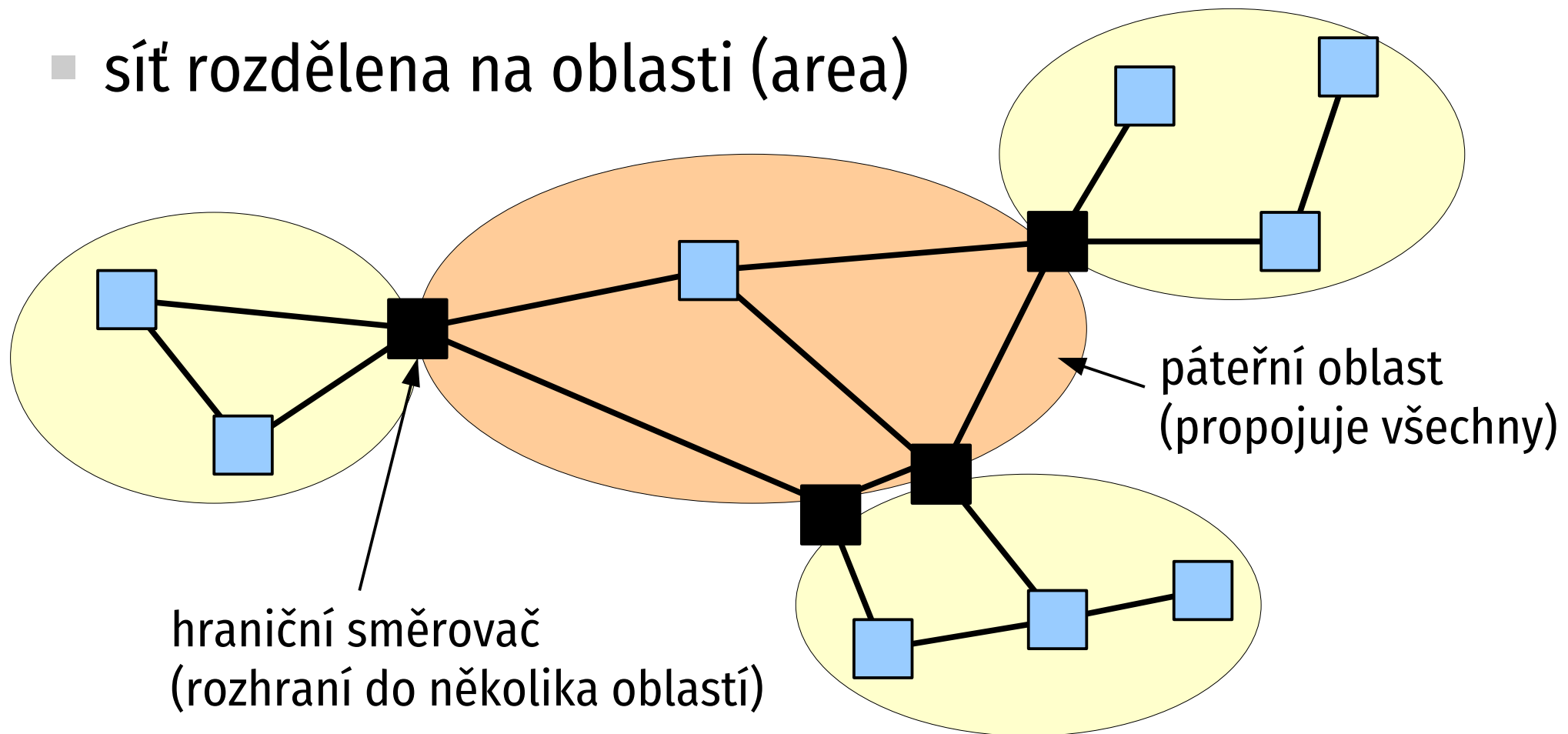
- RFC 2453
- proměnlivé délky prefixů (CIDR)
- **okamžité aktualizace (triggered update)**
 - změny hlásí hned, nečeká na pravidelný interval
- **rozdělený obzor (split horizon)**
 - sousedovi se neposílají cesty, které vedou přes něj
- **otrávené vracení (poisoned reverse)**
 - sousedovi se pošlou, ale nastaví se jim nekonečná vzdálenost

OSPF

- **Open Shortest Path First, RFC 2328**
- založeno na stavu linek – všechny směrovače si udržují totožnou mapu sítě
- každou změnu okamžitě hlásí sousedům
 - šíří se roztékáním – změna se předává všem ostatním
 - pozná opakovanou aktualizaci (cyklus), neposílá dál
- z mapy sítě vypočítá nejkratší cesty ke všem cílům
- linkám přiřazeny ceny (2 bajty)

OSPF oblasti

- **hierarchické směrování**
- síť rozdělena na oblasti (area)



OSPF oblasti

- **páteřní oblast** propojuje všechny ostatní
 - ostatní nejsou propojeny mezi sebou
 - cesta mezi oblastmi vždy prochází páteřní oblastí
- kompletní mapu synchronizuje jen v rámci oblasti
- **hraniční směrovač** předává informace z jiné oblasti v agregované podobě (cíle a vzdálenosti, ne celá topologie)

Koncová oblast

- **stub area**
- používá směrování implicitní cestou
- informace zvenčí se nepředávají
- ohlašuje se implicitní cesta
- typicky oblast s jediným hraničním směrovačem (zákazník připojený k poskytovateli Internetu)

vytvořeno s podporou
projektu ESF





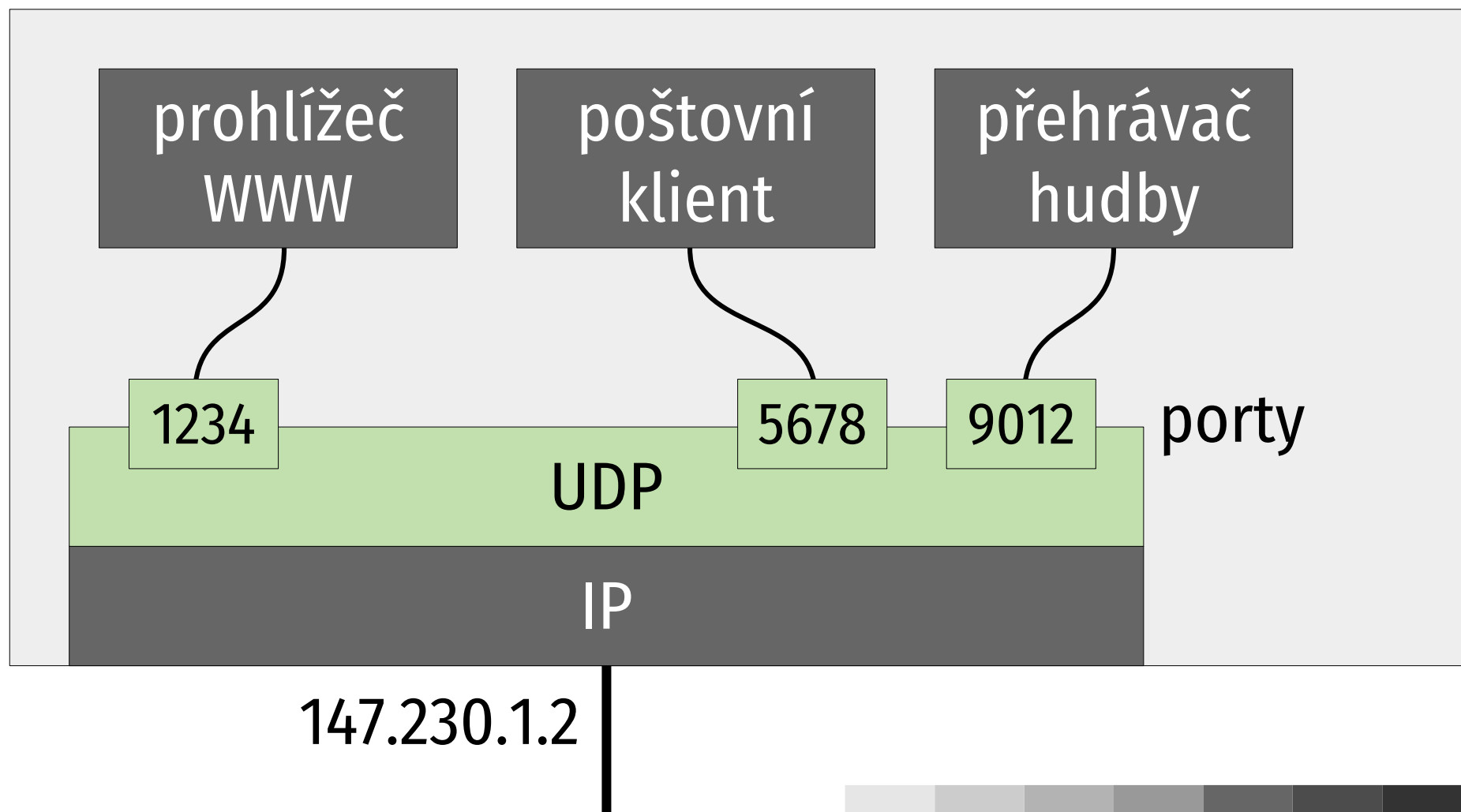
Transportní vrstva



UDP

- **User Datagram Protocol**, RFC 768
- jednoduchá nadstavba IP (adresování aplikací)
- datagramová služba bez záruk, řadě aplikací vyhovuje (DHCP, DNS, interaktivní,...)
- **port**
 - zjemňuje adresu na úroveň aplikace
 - 65 536 portů
 - komunikující aplikace se připojí k portu (služba OS)

Aplikace a porty



UDP hlavička

port odesílatele	port příjemce
délka	kontrolní součet

- **porty:** identifikují komunikující aplikace
- **délka:** délka UDP hlavičky + dat v B
- **kontrolní součet:** pokrývá pseudohlavičku (vybrané údaje z IP hlavičky) + UDP hlavičku + data

Porty

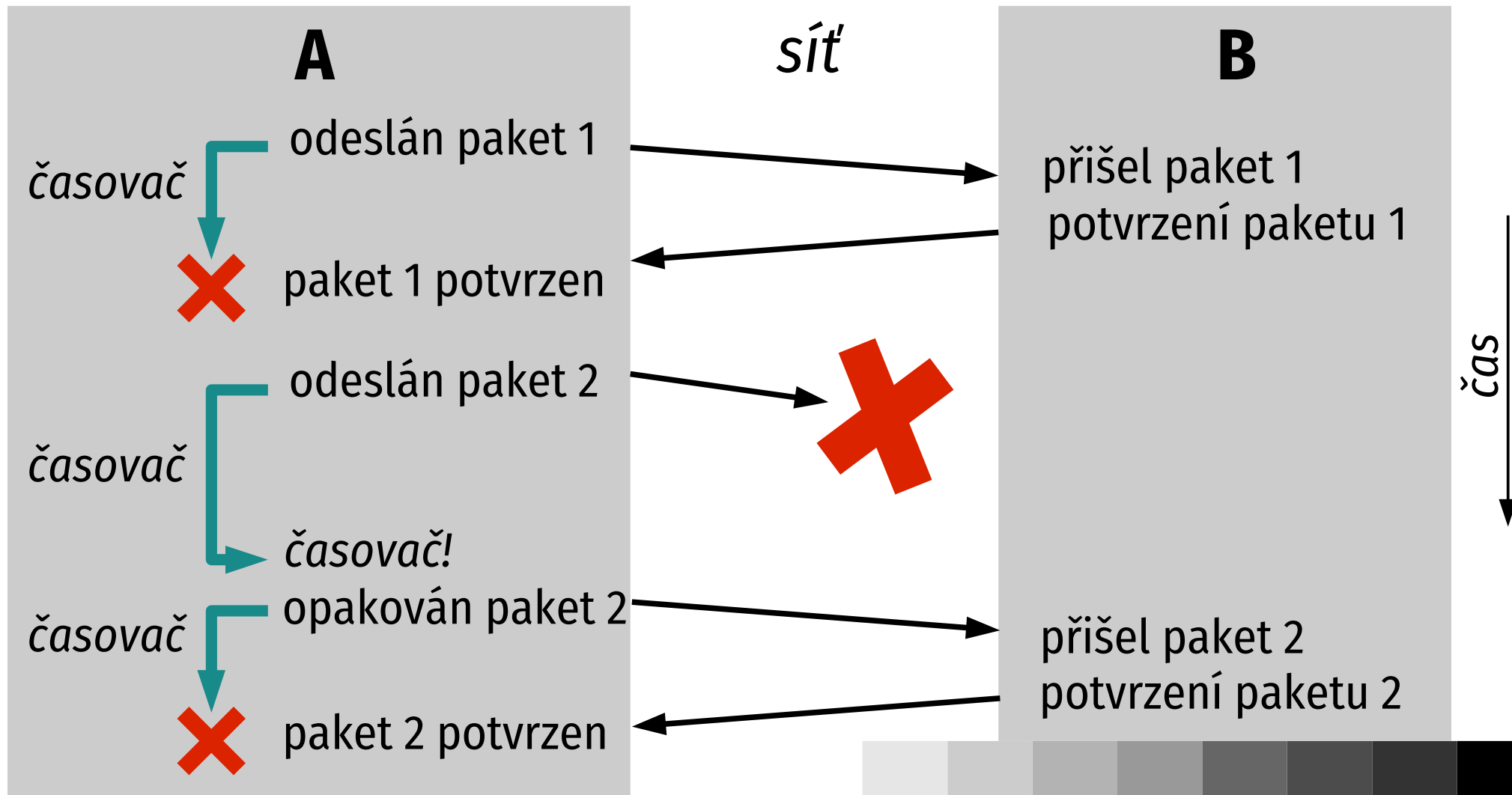
- k odeslání dat je třeba znát číslo portu dané aplikace
- **servery** používají standardní (well-known) porty
 - <http://www.iana.org/assignments/port-numbers>
 - nestandardní port serveru musí klientovi ohlásit uživatel
- **klienti** používají náhodná čísla portů
 - hodnoty > 1000

TCP

- **Transmission Control Protocol, RFC 793**
- spolehlivá přeprava, vyžaduje většina aplikací
- proud bitů bez struktury (bitová roura)
- spojovaná služba, virtuální okruhy
 - spojení udržováno na koncích, pod ním nespojované IP
- vyrovnávací paměti
 - rozděluje/seskupuje data pro maximální efektivitu
- plně duplexní spojení

Zajištění spolehlivosti (1)

- pozitivní potvrzování s opakováním



Zajištění spolehlivosti (2)

- **potvrzování** řeší ztráty paketů
- možnost přehození a duplikace – pořadová čísla
- TCP **čísluje bajty (oktety)**
- potvrzuje **nejdelší souvislý prefix** od začátku vysílání (posílá číslo bajtu, který očekává)
- jednoduché a jednoznačné
- ztráta potvrzení nemusí způsobit opakování
- nelze oznámit mezeru

Potvrzování paketů

výpadek



3x totéž – rovnou zopakuje

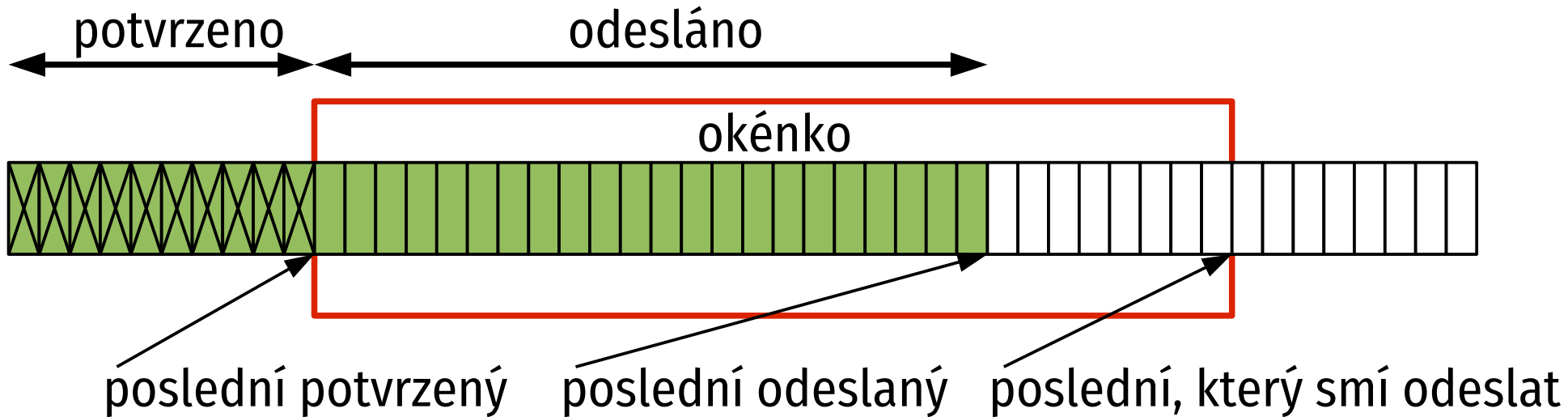
Časování potvrzení

- piggybacking – potvrzení se snaží přibalit k datům v protisměru
 - čeká 200 ms, jestli se nevyskytne vhodný paket
- problém: jak nastavit časovač pro opakování
 - příliš malý – bude se zbytečně opakovat
 - příliš velký – výpadek bude objeven pozdě
- **neexistuje univerzální hodnota, musí se přizpůsobovat chování sítě**

Nastavení časovače

- vychází z **průměrné doby odezvy** (RTT) a **průměrné odchylky** (MD)
- dorazí potvrzení se zpožděním M:
 - $\text{odchylka} = M - \text{RTT}$
 - $\text{RTT} = \text{RTT} + 0,125 \cdot \text{odchylka}$
 - $\text{MD} = \text{MD} + 0,25 \cdot (|\text{odchylka}| - \text{MD})$
 - $\text{časovač} = \text{RTT} + 4 \cdot \text{MD}$
- opakovaným paketům časovač zdvojnásobí
- pro opakované nepočítá

Okénko (sliding window)

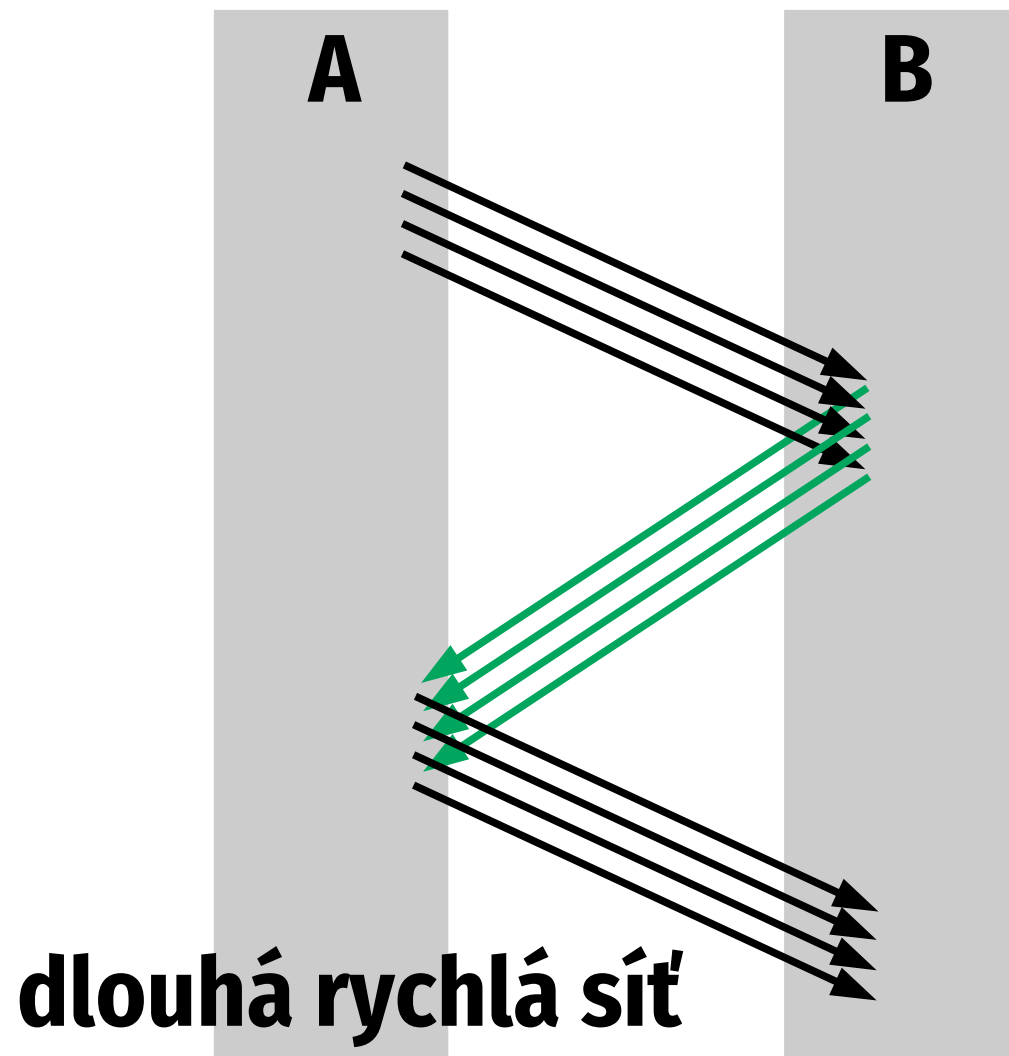
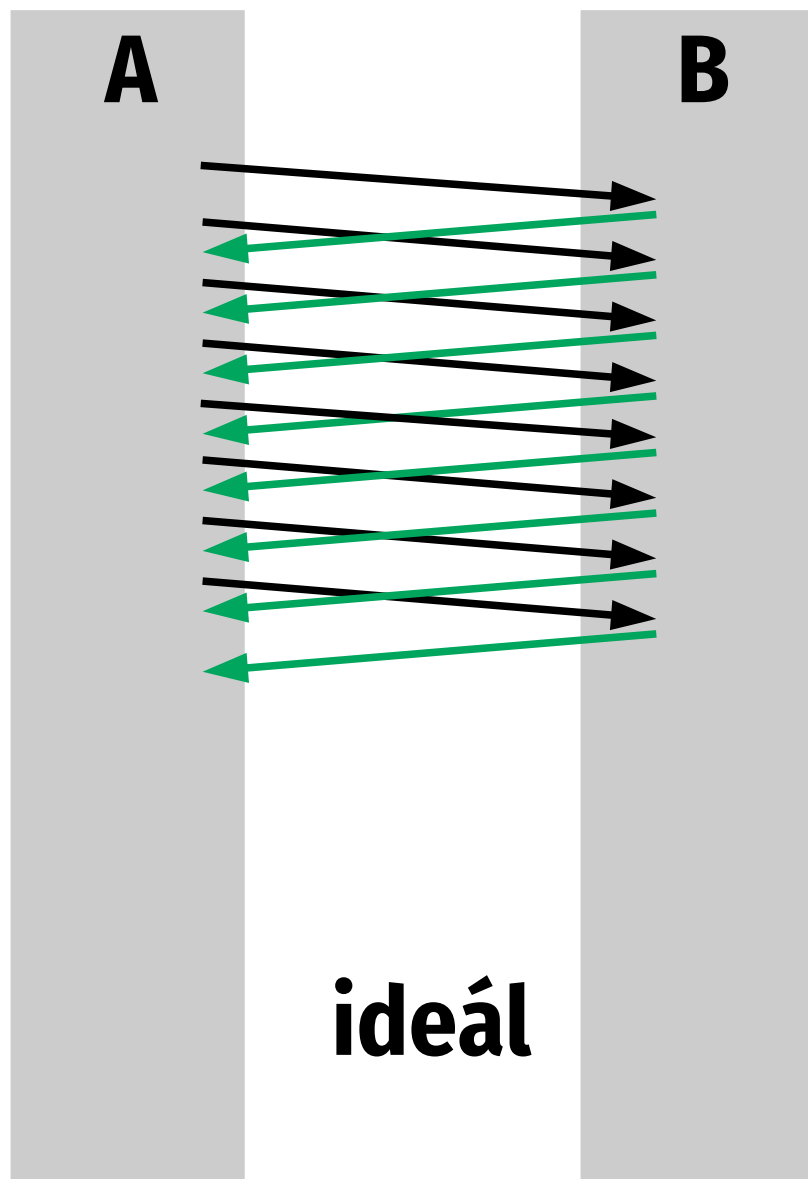


- **zvyšuje efektivitu** – nemusí se čekat na potvrzení

- **brání zahlcení pomalého příjemce**

- smí vysílat jen po horní hranici okénka, pak čeká
- tu určuje příjemce, nesmí couvnout
- prázdné okénko – musí čekat, až je příjemce otevře

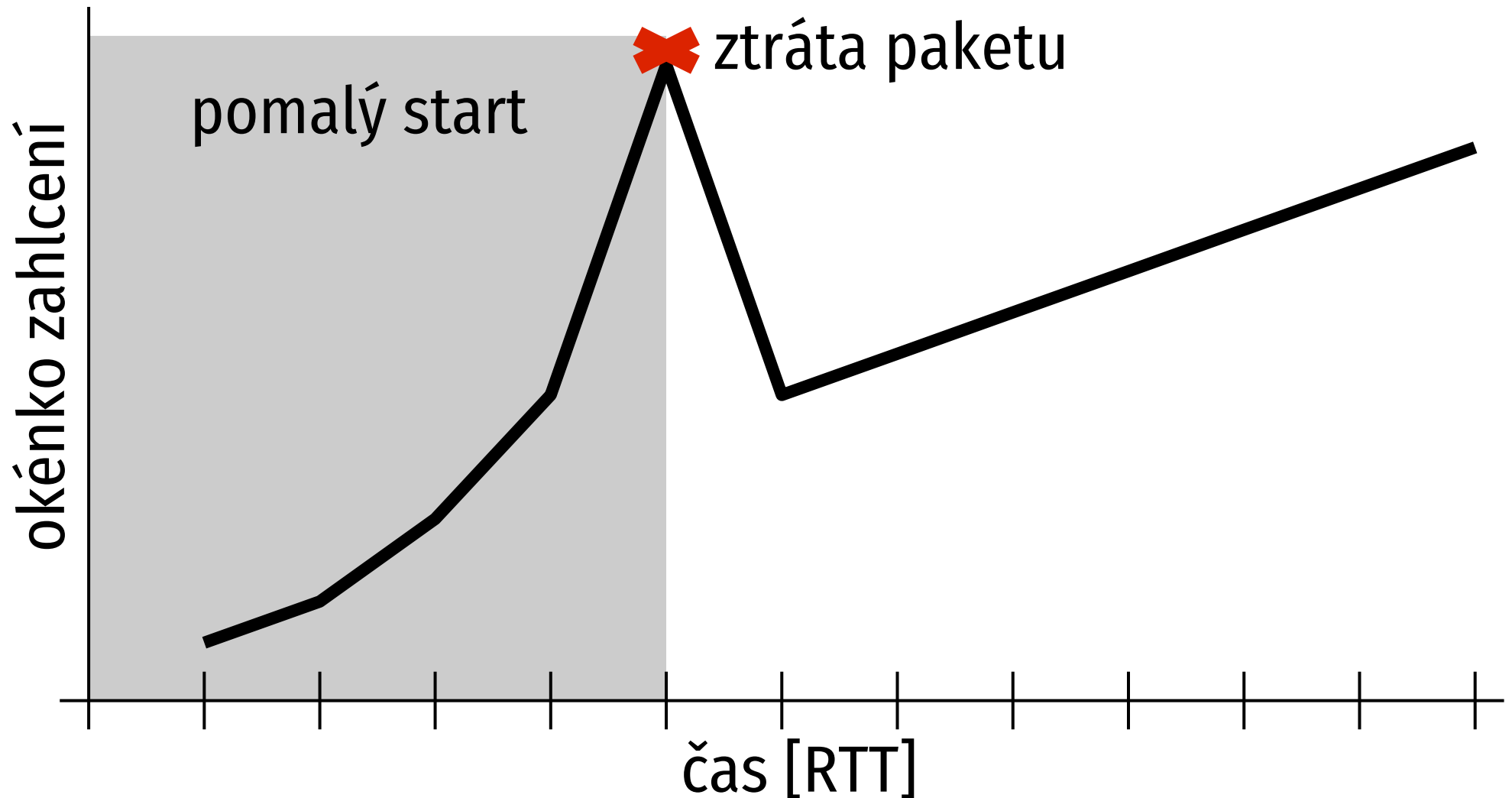
Fungování okénka



Ochrana proti zahlcení

- víceprvková a dost složitá, různé algoritmy
- základem **okénko zahlcení (congestion window)**
 - omezuje nepotvrzené pakety, které smí odeslat
- **pomalý start (slow start)**
 - začíná s velikostí 1 MSS (max. velikost TCP segmentu)
 - potvrzení paketu zvětší o 1 MSS
 - ztráta paketu = dosažení limitu → zmenší okénko na polovinu a zpomalí růst

Vývoj okénka zahlcení



Vysílání paketů

- obě okénka se kombinují
- může odeslat paket, pokud:
 - má od aplikace k dispozici data
 - umožňuje to plovoucí okénko (není na konci)
 - umožňuje to okénko proti zahlcení
- stanoví velikost paketu (shora omezeno MSS) a odešle
- MSS stanoví protějšek při navazování spojení

TCP segment

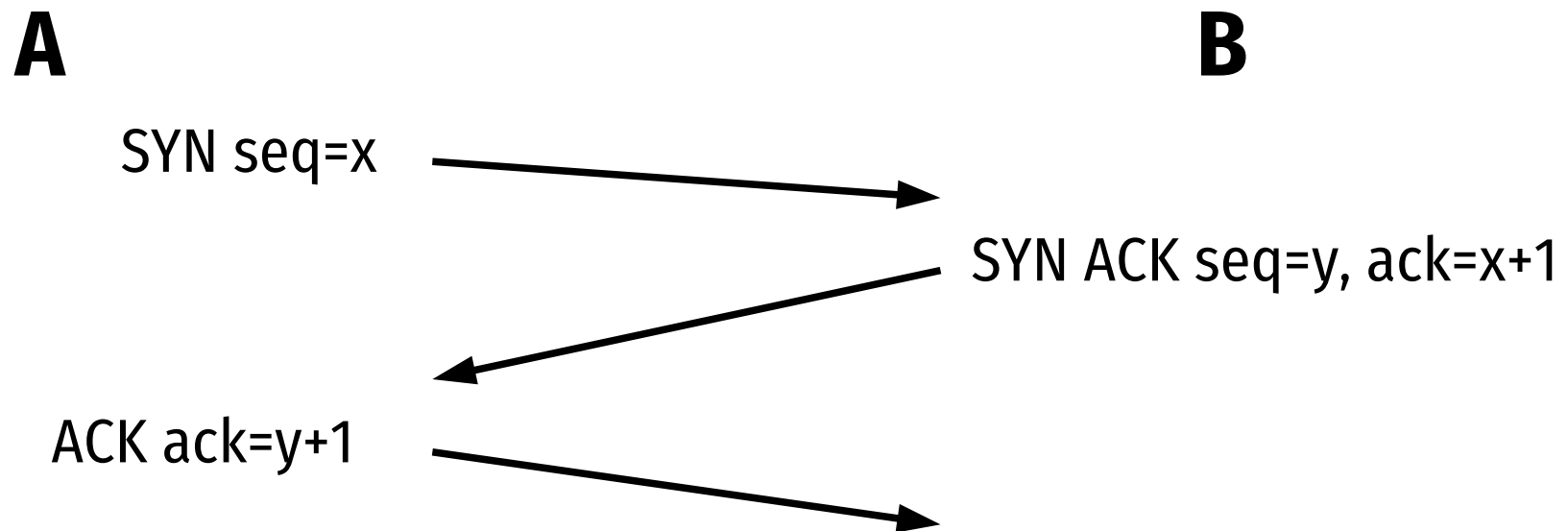
port odesilatele		port příjemce	
pořadové číslo číslo 1. bajtu			
potvrzení (pořadové číslo číslo očekávaného bajtu)			
délka hl.		příznaky	velikost okénka
kontrolní součet		konec urgentních dat	
volby (jsou-li)			
data (jsou-li)			

TCP hlavička

- **délka hlavičky:** ve 32b slovech
- **příznaky:**
 - **URG** – segment obsahuje urgentní data
 - **ACK** – obsahuje platné potvrzení
 - **PSH** – předat cílové aplikaci co nejrychleji (push)
 - **RST** – náhlé ukončení spojení (reset)
 - **SYN** – zahájení spojení (synchronizace pořadových čísel)
 - **FIN** – končím odesílání dat, polouzavření
- **kontrolní součet:** pseudohlavička + hlavička + data

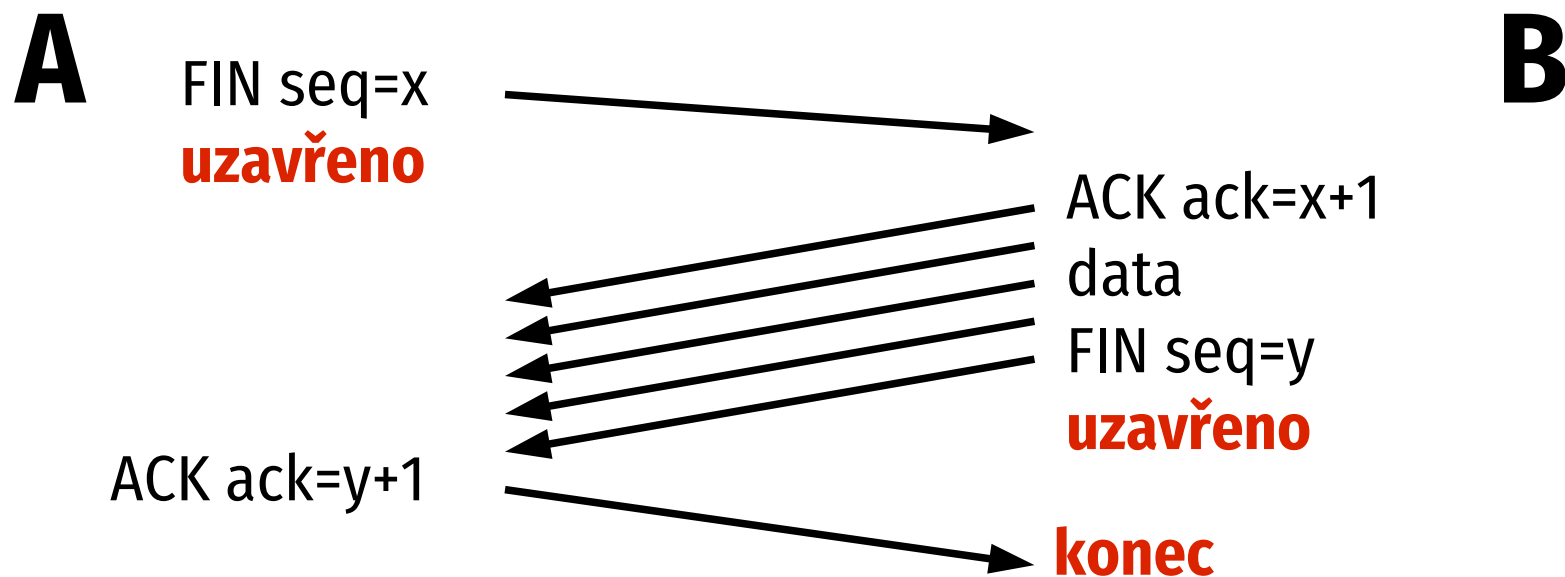
Navázání spojení

- three-way handshake
- **dohodnou si pořadová čísla a zahajovací okénka**



Ukončení spojení

- založeno na **polouzavření (half-close)**
- jedna strana ohlašuje, že ukončila vysílání, dále ale přijímá a potvrzuje data – protějšek může dokončit



vytvořeno s podporou
projektu ESF



Domain Name System (DNS)

Motivační citát

📌 Připnutý tweet



Paul Vixie @paulvixie · 17. 11. 2018

Odpověď uživatelům @XavierAshe a @Cloudflare

I have no idea how DNS works. Can you explain it to me please?

💬 23

↻ 249

❤️ 1 tis.



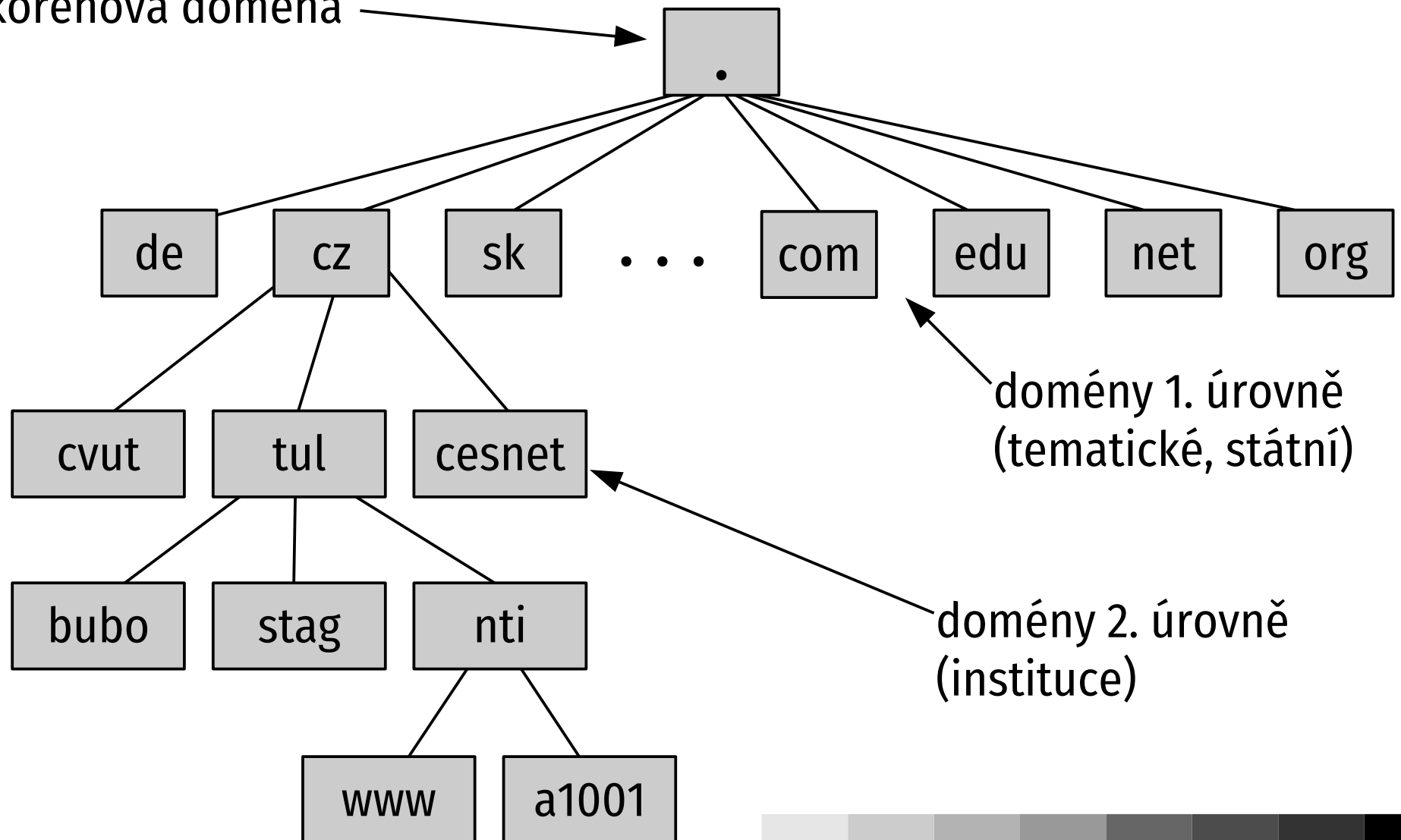
Paul Vixie, jeden z autorů DNS

Co je DNS

- RFC 1034, 1035
- řeší **vzájemné převody mezi jmény a IP adresami**
- rozšířeno na **distribuovanou** databázi informací
- jména nemají žádnou vazbu s topologií sítě
- **hierarchická struktura jmen** – složena z domén
- zápis:
 - od konkrétních k obecným, oddělovačem tečka
 - `www.tul.cz`

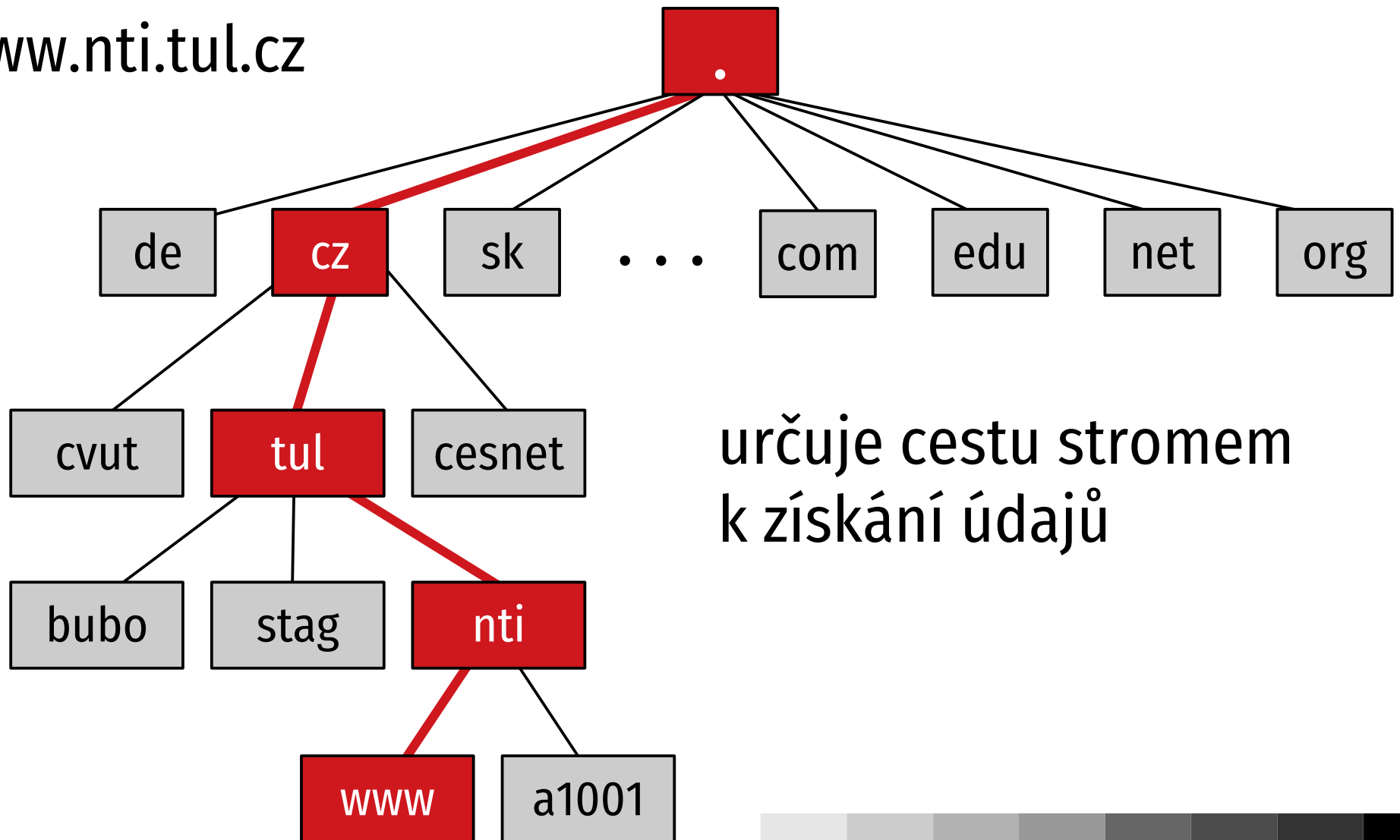
Doménový strom

kořenová doména



Doménové jméno

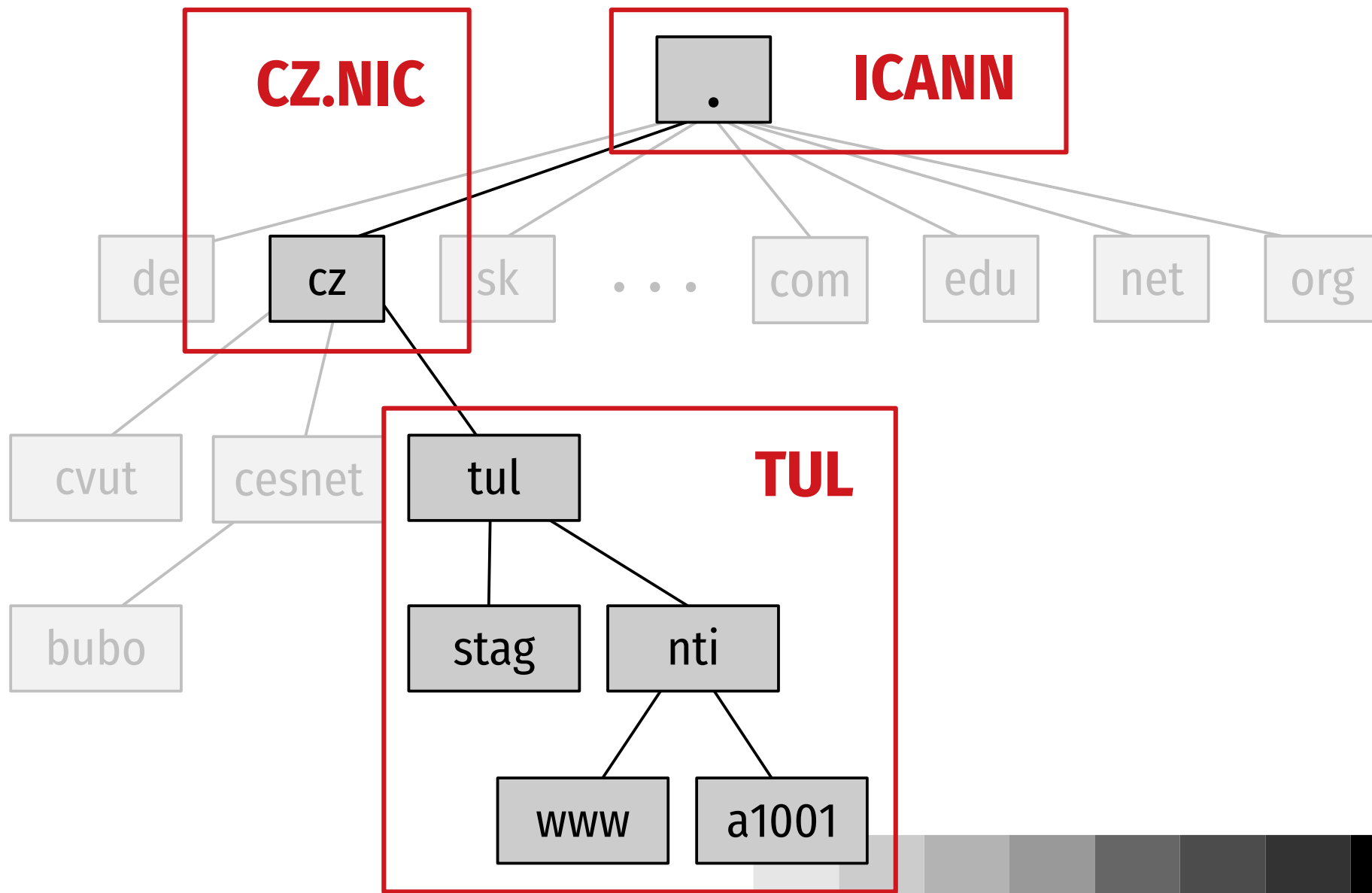
www.nti.tul.cz



Distribuovaná správa

- motivace: údaje vkládat co nejbližší místu, kde vznikají (nejlépe každý subjekt sám)
- každá doména má svého správce, ten určuje její obsah a pravidla v ní platná
- správce může poddomény svěřit jiným správcům
- **zóna** – souvislá část doménového stromu s jedním správcem

Zóny a správci



Doménová politika

- správce určuje pravidla pro danou doménu
- významné rozdíly pravidel domén 1. úrovně:
 - Musí mít subjekt vztah k doméně?
cz: Ne, doménu získá první zájemce.
 - Zavádí se tematické domény 2. úrovně?
cz: Ne.
 - Cena...

Problémy liberální politiky

- **doménové spekulantství**

- registrace atraktivních domén a snaha o jejich prodej bohatým zájemcům
- soudní spory o domény

- **registrace do nesystémových domén**

- akciové společnosti v doméně .as (Americká Samoa)
- televize v doméně .tv (Tuvalu)
- přesto je liberální politika nejúspěšnější

DNS servery

- správa domén distribuována, DNS servery spolupracují při řešení dotazů
- **typy serverů** (vztah ke konkrétní doméně):
 - **primární:** zde vznikají data pro danou doménu, autoritativní, právě jeden pro každou doménu
 - **sekundární:** automatická kopie primárního, autoritativní, alespoň jeden pro každou doménu
 - **pomocný (caching only):** neautoritativní, po určitou dobu uchovává předchozí odpovědi

Řešení dotazu

- **PC pošle místnímu serveru**
 - v PC tzv. koncový řešič (stub resolver), funkce OS
 - pouze předává dotazy místnímu serveru (získán z DHCP nebo nastaven staticky)
- **místní server pošle dotaz jednomu z kořenových**
 - jejich adresy zná ze své konfigurace
- **dále se postupuje dolů po jednotlivých patrech**
 - autoritativní server domény zná situaci v ní – ví, zda existuje poddoména a kdo jsou její autoritativní servery

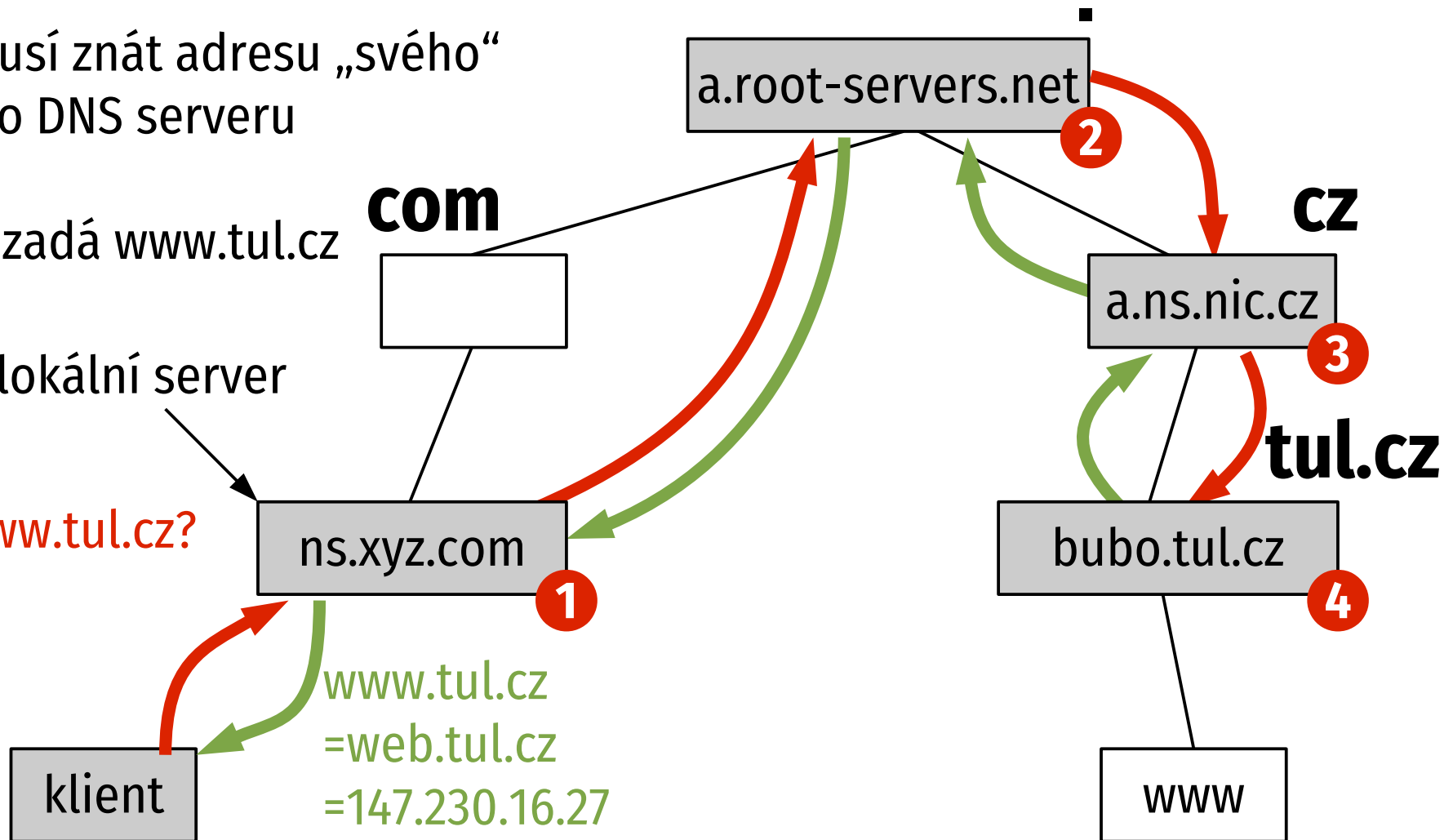
Idealizované vyřizování dotazu

klient musí znát adresu „svého“
lokálního DNS serveru

uživatel zadá `www.tul.cz`

lokální server

IP pro `www.tul.cz`?



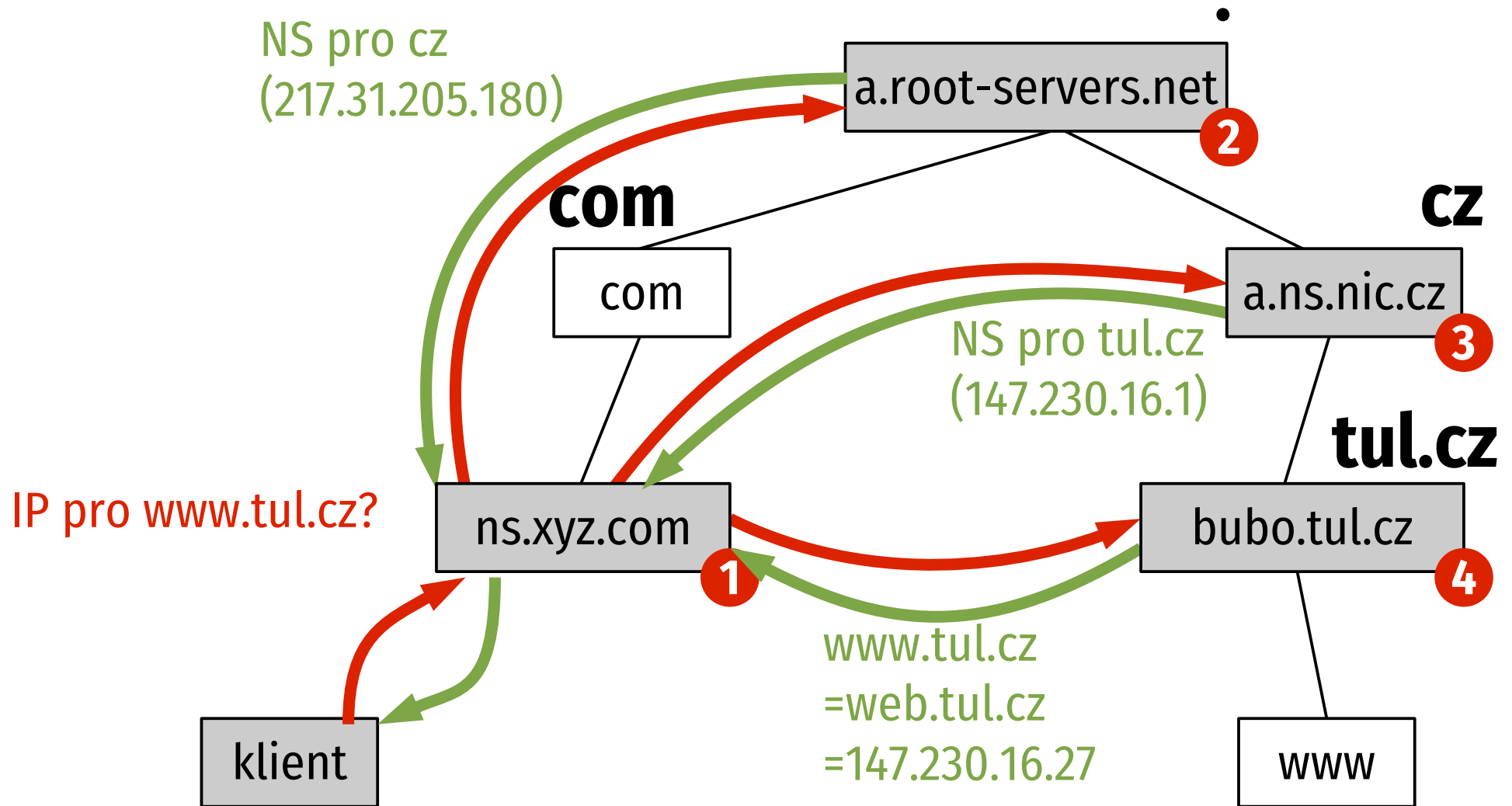
Kořenové servery

- mají klíčovou úlohu
 - řádově miliony dotazů za sekundu
- jejich adresy zná každý DNS server – cesta dotazu vzhůru je realizována jedním krokem
- 13 jmen/adres, většinou fyzicky realizovány skupinou serverů
- www.root-servers.org

Zpracování dotazu

- každý server po cestě může poskytnout neautoritativní odpověď z vyrovnávací paměti
- **rekurzivní zpracování**
 - server se chopí vyřízení a pošle až odpověď
 - typické pro lokální servery (plní si cache odpovědí)
- **nerekurzivní zpracování**
 - server jen pošle odkaz, kde se ptát dál
 - typické pro vrcholové servery (nestíhaly by rekurzivně)

Realistické vyřízení dotazu



stejné pořadí oslovených, mění se tazatelé

Zpětný dotaz

- **z IP adresy jméno**, např. pro informování uživatele (traceroute), zápis do logu apod.
- problém: obrácené pořadí významnosti
 - doménové jméno: obecné domény vzadu
 - IP adresa: obecný prefix vpředu
- řešení: **otočit pořadí bajtů a přidat in-addr.arpa**
 - umožňuje distribuovat správu reverzních domén
 - 147.230.16.8 → 8.16.230.147.in-addr.arpa
 - dále se vyřizuje obvykle

Data v DNS

- **zdrojové záznamy (resource records, RR)**
 - **jméno**
 - **třída** – teoreticky i pro jiné sítě, pro Internet třída = IN
 - **životnost** – jak dlouho smí být uložen ve vyrovnávací paměti
 - **typ** – jakou informaci obsahuje
 - **data** – interpretována podle typu
- může být více záznamů stejného typu pro stejné jméno, posílají se všechny

Nejčastější typy záznamů

- **A** adresa (AAAA pro IPv6)
- **CNAME** přezdívka (alias)
- **NS** autoritativní server pro doménu
- **MX** příjem pošty pro doménu
- **TXT** libovolný text
- **PTR** reverzní záznamy

Příklady

■ v tul.cz

	IN	NS	bubo.tul.cz.	;DNS server
	IN	MX	0 bubo.tul.cz.	;e-mail
fm	IN	NS	bubo.tul.cz.	;poddoména
web	IN	A	147.230.16.27	;IP adresa
www	IN	CNAME	web	;alias

■ v 230.147.in-addr.arpa

27.16	IN	PTR	web.tul.cz.	;jméno k adrese
-------	----	------------	-------------	-----------------

Domény s národními znaky (1)

- klasické DNS omezeno na (podmnožinu) ASCII: písmena anglické abecedy, číslice, pomlčky
- tlak (zejména od asijských zemí) na zavedení národních abeced
- **Internationalized Domain Names (IDN)**
 - RFC 5890, 5891, 3492
 - implementováno v klientech, servery beze změny
 - zakóduje se do ASCII a přidá předpona xn--

Domény s národními znaky (2)

- např. **blahopřání** převede na **xn--blahopn-mwa3iv2c**
- první zavedl Hong Kong (1999)
- od roku 2003 postupně zaváděno v Evropě
- **ČR** – CZ.NIC provedl (opakovaně) průzkum mezi uživateli, o zavedení IDN není zájem

Bezpečné DNS – DNSSEC

- DNS odpovědi lze podvrhnout, různé formy útoků
- **DNSSEC** umožňuje
 - **ověřit platnost odpovědi**
 - **ověřit neexistenci** daného záznamu
 - založeno na **elektronických podpisech**
 - **asymetrická kryptografie** – soukromé klíče mají správci domén, veřejné klíče pro ověření podpisů jsou v DNS
- definují RFC 4033, 4034, 4035

Principy DNSSEC

- každý záznam (resp. sada záznamů stejného typu pro stejné jméno) je podepsán – záznam **RRSIG**
- veřejné klíče k ověření uloženy přímo v DNS – záznam **DNSKEY**
- záznam **NSEC** ověřuje neexistenci, obsahuje:
 - existující typy záznamů pro své jméno
 - další jméno v doméně

Řetězec důvěry

- základní problém asymetrické kryptografie:
jak si ověřit, že veřejný klíč je pravý?
- obecný princip: **potvrdí ho někdo důvěryhodný**
- v DNSSEC: potvrdí nadřazená doména
 - obsahuje záznam **DS** s otiskem klíče domény pod sebou
 - záznam DS je podepsán jejím klíčem
 - otisk jejího klíče je o patro výš...
- veřejný klíč kořenové domény má každý klient

DNSSEC – ověření

- **kořenová doména:**
 - cz DS otisk klíče cz veřejný klíč kořenové domény klient má
RRSIG podpis klíčem kořenové domény
 - **doména cz:**
 - DNSKEY klíč cz
 - tul.cz DS otisk klíče tul.cz
RRSIG podpis klíčem cz
 - **doména tul.cz:**
 - DNSKEY klíč tul.cz
 - bubo A 147.230.16.1
RRSIG podpis klíčem tul.cz
- ← ověření
-

Nasazení DNSSEC

- prosazovalo se velmi dlouho
- první definice 1999
- 2005 radikálně změněno
- **1. 9. 2008 podepsána doména cz** (chybějící podpis kořenové domény řešen pomocí DLV)
- **1. 7. 2010 podepsána kořenová doména**
- v současnosti (začátek 2021) podepsáno přes 91 % domén 1. úrovně

Problémy DNSSEC

- podpisem velikost domény několikanásobně naroste (podepsaný .com má 10 GB)
- chybějí klienti s podporou DNSSEC
- záznamy NSEC umožňují vypsat kompletní obsah domény (řeší NSEC3)

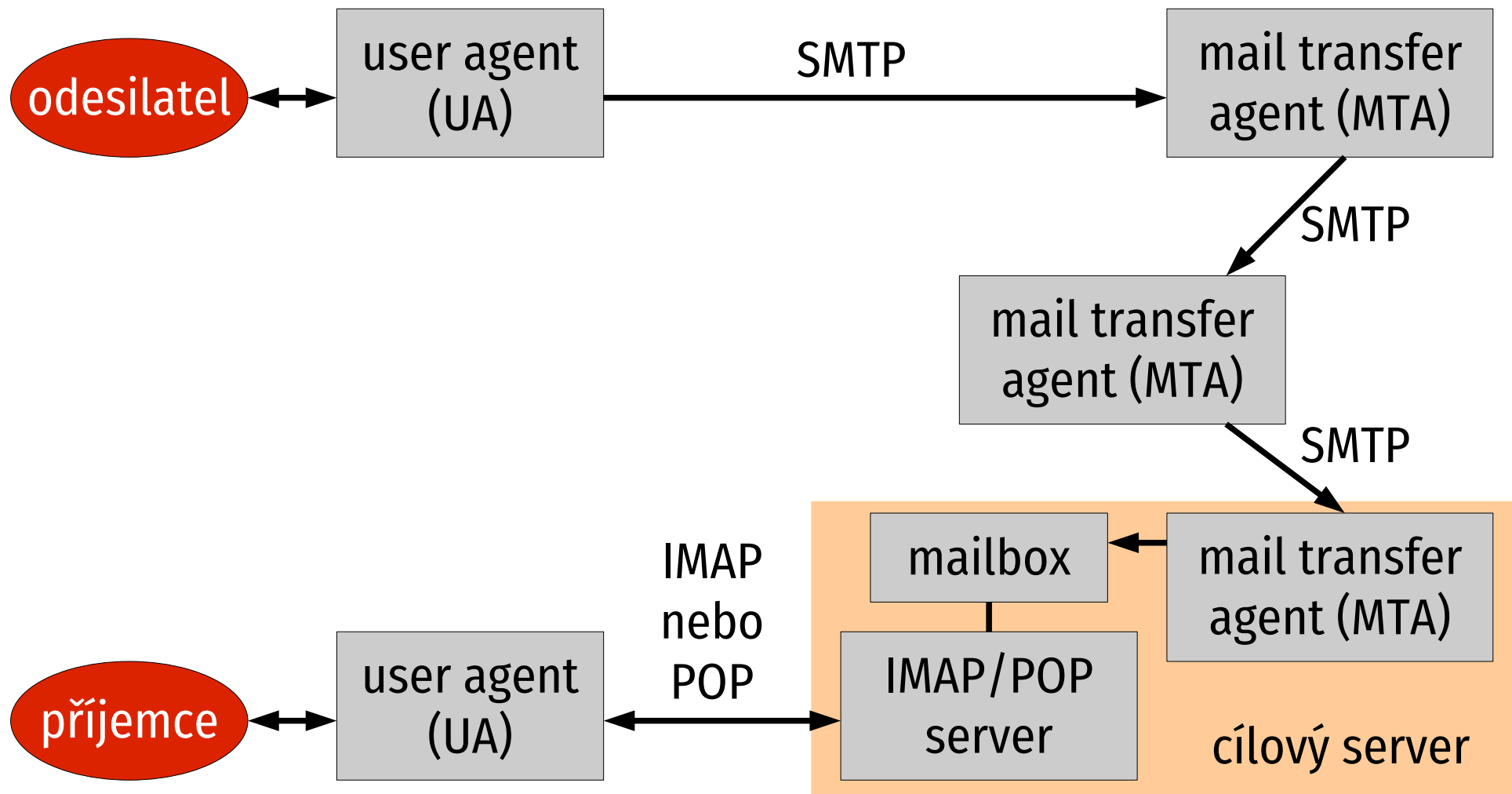
vytvořeno s podporou
projektu ESF



Aplikační protokoly

Elektronická pošta

Schéma elektronické pošty



Programy

- **User Agent (UA)**

- uživatelské rozhraní poštovního systému
- rozhodující pro uživatelský komfort
- MS Outlook, Mozilla Thunderbird,...

- **Mail Transfer Agent (MTA)**

- zajišťuje přepravu dopisů
- neviditelný z hlediska uživatele
- sendmail, Postfix, MS Exchange,...

SMTP

- **Simple Mail Transfer Protocol**, RFC 5321
- formát dopisu definuje RFC 5322:
 - **obálka**: přepravní informace, interní pro MTA, uživatel se o ní nedozví
 - **hlavičky**: kdo poslal, kudy prošlo,...; využívá UA, vychází z nich řada jeho funkcí (řazení dopisů, vyplňování adres při odpovědi,...)
 - **tělo**: vlastní nesená zpráva, pro uživatele

Příklad dopisu

Received: from bubo.tul.cz (147.230.16.1) by tyto.tul.cz (Mercury 1.44)
with ESMTP; 19 May 06 08:53:09 +0200

Received: from relay.xyz.cz (relay.xyz.cz [123.24.128.45]) by
bubo.tul.cz (Postfix) with ESMTP; Mon, 19 May 2006 08:53:09 +0200

Received: from xyz.cz (office.xyz.cz [123.24.132.67]) by relay.xyz.cz
(Postfix) with ESMTP; Mon, 19 May 2006 08:53:11 +0200

Date: Mon, 19 May 2006 08:53:09 +0200

From: "Vitezslav T. Se'm" <travis@xyz.cz>

To: Petr Adamec <Petr.Adamec@tul.cz>

Cc: Pavel.Satrapa@tul.cz

Subject: Spam pres buba?

← prázdný řádek odděluje hlavičky od těla
Zde je text tela dopisu.

Příklad SMTP komunikace

relay.xyz.cz (A)
předává dopis na
bubo.tul.cz (B)

A naváže TCP
spojení s B na
port 25, po něm
proběhne tento
dialog:

B: 220 bubo.tul.cz SMTP service ready

A: HELO relay.xyz.cz

B: 250 bubo.tul.cz says helo to relay.xyz.cz

A: MAIL FROM: <travis@xyz.cz>

B: 250 sender ok

A: RCPT TO: <petr.adamec@tul.cz>

B: 250 recipient OK

A: DATA

B: 354 Enter mail, end with "." on a line by itself

A: celý dopis – hlavičky a tělo

A: .

B: 250 message sent

A: QUIT

B: 221 relay.xyz.cz closing connection

E-mail a DNS

- používá DNS ke zjištění, kam posílat poštu
- MX záznamy (Mail eXchange)
MX prioritá jméno
- příklad: dopis pro **pavel.satrapa@tul.cz**
- vyhledá v DNS MX záznamy pro **tul.cz**:
0 **bubo.tul.cz**
50 **tul.cesnet.cz**
- pokusí se předat (po SMTP) na bubo.tul.cz
- neuspěje-li, zkusí server s horší prioritou

Vzdálený přístup ke schránce

- schránka musí být stále dostupná, je umístěna na počítači s cílovým MTA
- UA často na jiném počítači (přístup z domova)
- **Post Office Protocol (POP)**
 - umí stáhnout dopisy na počítač a vymazat ze schránky
 - jednoduchý, široce implementovaný
- **Interactive Mail Access Protocol (IMAP)**
 - vzdálená práce se schránkami, větší možnosti, složitější
 - ideální kombinovat se SSL

MIME

- **Multipurpose Internet Mail Extensions**, RFC 2045 a další
- dle RFC 822 smí tělo dopisu tvořit jen US ASCII
 - problém s národními znaky, přílohami,...
- MIME zakóduje složitý dopis do podoby podle RFC 822 – lze přepravovat stávajícími MTA
- implementuje klient (UA) – kóduje/dekóduje

MIME hlavičky

- **MIME-Version**
 - je použito MIME
 - identifikuje verzi, zatím stále 1.0
- **Content-Type**
 - jakého typu je obsah dopisu
- **Content-Transfer-Encoding**
 - jak je kódován
 - **Quoted-Printable** pro text s akcenty,
Base64 pro binární data

MIME typy (1)

- **typ/podtyp**
 - typ určuje základní charakter dat
 - podtyp identifikuje formát
- **text** – textová informace; text/plain, text/html
- **image** – obrázek; image/jpeg, image/gif
- **audio** – zvuk; audio/basic, audio/mpeg
- **video** – videosekvence; video/mpeg

MIME typy (2)

- **application** – data ke zpracování speciální aplikací; application/octet-stream, application/postscript
- **message** – obsahem je jiný dopis
- **multipart** – obsah má několik částí
 - multipart/mixed – prezentovat postupně (nejčastější)
 - multipart/parallel – prezentovat současně
 - multipart/alternative – různé varianty téhož obsahu
 - multipart/digest – každou částí je elektronický dopis
 - multipart/form-data – data z formuláře

Škodlivé dopisy (1)

- **spam** – nevyžádaná reklama
 - produkty i služby
 - oslovují koncové zákazníky i firmy
- **scam** – podvod
 - snaha vylákat peníze
 - typicky fiktivní velká cílová odměna (dědictví, výhra, dar) a vylákat z oběti „transakční poplatky“ po cestě k ní (právník, cestovné, administrativní poplatky, úplatky, ...)

Škodlivé dopisy (2)

- **ransom** – vydírání
 - někdy skutečné – zašifrování obsahu disku
 - často fiktivní – máme vaše intimní nahrávky, jste obviněn(a) z trestného činu ...
- **phishing** – vylákání důvěrných údajů
 - přihlašovací údaje, číslo platební karty, ...
 - předstírání provozní události (přeplnění poštovní schránky, aktualizace zabezpečení, ...)
 - falešná stránka, která napodobuje původní

Možnosti ochrany

- **systémové**

- greylisting
- detekce virů, spamů apod.

- **uživatelské**

- uživatel bývá nejslabším článkem
- nedůvěřujte automaticky příchozí poště
- pokud považujete za reálné, ověřte si jinou cestou (web, telefon), nepoužívejte odkazy z dopisu

Příznaky falešného dopisu

- skoro všechny výzvy typu „přihlaste se, abyste zabránili něčemu nepříjemnému“ jsou falešné
- nesmyslná adresa odesílatele (případně si zobrazte neformátovaný dopis a kontrolujte Received)
- falešné odkazy – vedou jinam, než se tváří
- špatná čeština, nevěrohodné formulace
- snaha vyvolat tlak, požadavek rychlé reakce



World-Wide Web



Základní prvky

- uspořádání klient–server
- **HyperText Transfer Protocol (HTTP)**
 - protokol pro komunikaci mezi klientem a serverem
- **HyperText Markup Language (HTML)**
 - jazyk pro definici obsahu stránky
 - XHTML – HTML přeformulováno do XML
 - vývoj koordinuje WWW konsorcium

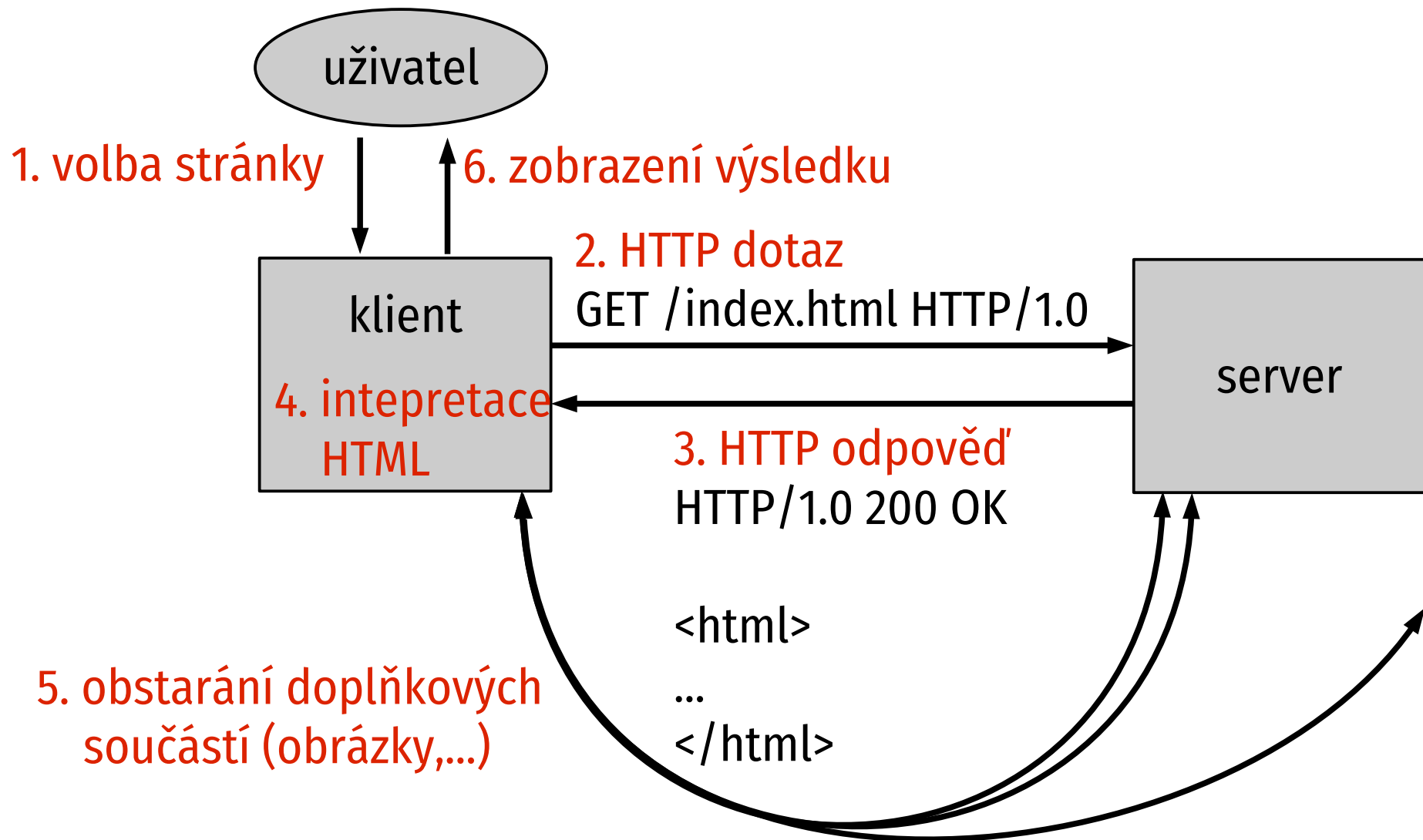
HTTP

- standardizace zpočátku chaotická (WWW konsorcium vs IETF, HTTP/1.0 nemá RFC)
- 2022 standardy zcela přepracovány
 - terminologie a sémantika – RFC 9110
 - HTTP/1.1 – RFC 9112
 - HTTP/2 – RFC 9113
 - HTTP/3 – RFC 9114

Účastníci HTTP provozu

- **prohlížeč** (uživatelský agent) – uživatelské rozhraní
- **server** – poskytuje obsah
 - často spojen s aplikací (e-shop, webmail,...)
- **prostředníci** – ne vždy, umožňují překonávat různá omezení
 - **cache** – ukládá obsah ze serverů
 - **proxy** – předává zprávy mezi prohlížečem a serverem

Komunikace klient-server



HTTP/1.1

- RFC 9112, TCP port 80
- **bezstavový protokol**
 - zodpovězením dotazu transakce pro server končí, neudrží stavové informace o klientech
 - další dotaz nedává do souvislosti s předchozími
 - stav si uchovává klient
 - výhody: robustní, snadnější implementace
 - nevýhody: větší režie, některé služby vyžadují stavové informace (nákupní košík) – klient musí předat serveru

HTTP zprávy

- formátem připomínají elektronický dopis

- **dotaz:**
metoda lokátor verze
hlavičky (doplňují)

- **odpověď:**
verze kód popis
hlavičky

tělo

prázdný
řádek

```
GET / HTTP/1.1  
Host: www.tul.cz
```

```
HTTP/1.1 200 OK  
Content-Type: text/html  
Content-Length: 6708
```

```
<html>...</html>
```

Uniform Resource Locator

- univerzální adresa
- struktura: ***schéma:specifická část***
- typicky:
http://www.kdesi.cz/doc/help.html

schéma (protokol) server cesta
- elektronická pošta:
mailto:Pavel.Satrapa@tul.cz

HTTPS

- HTTP + TLS (dříve SSL)
- TCP port 443
- **Transport Layer Security (TLS)**
 - RFC 8446
 - použitelné pro libovolný aplikační protokol
 - šifruje kompletní komunikaci (dotazy i odpovědi)
 - ověřuje autentičnost serveru (certifikát)
 - doporučováno pro veškerý webový obsah



HTTP/2

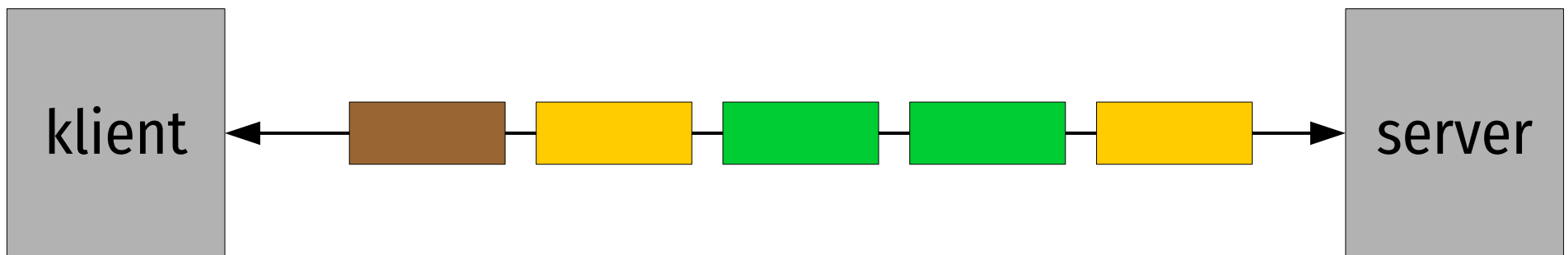
- RFC 9113, navazuje na SPDY
- **binární přenos dat**
 - přenášeno v tzv. rámcích
 - 10 typů – hlavičky, data, nastavení,...
- **proudy (stream)**
 - klient navazuje jedno TCP spojení
 - každý dotaz/odpověď v něm přenášeny samostatným proudem (jen číslo proudu v hlavičkách)
 - navzájem se nezdržují

Porovnání protokolů

HTTP/1.x – několik TCP spojení



HTTP/2 – jedno TCP spojení, několik proudů v něm



Další vlastnosti HTTP/2

- **hlavičky** nadále u každého požadavku a odpovědi, ale silně **komprimovány** (RFC 7541)
- **server push**
 - server může poslat data, o která nebyl žádán, např. odeslal HTML a rovnou začne posílat obrázky pro stránku
 - klient může odmítnout
- předpokládá se použití s TLS
 - není povinné, klienti často podporují jen HTTP/2 + TLS
- aktivace: hlavička Upgrade

QUIC (1)

- původně: Quick UDP Internet Connection
- protokol transportní vrstvy
- vyvinul Google, standard: RFC 9000
- **UDP**, port 443
- QUIC spojení určeno identifikátorem – přežije i změnu portu klienta (občas způsobí NAT)
- vše šifrováno

QUIC (2)

- vhodný pro web – přenos více malých souborů
- uvnitř spojení **nezávislé proudy** (à la HTTP/2)
- každý proud má své potvrzování a opakování – zajišťuje spolehlivý přenos
- rychlejší navázání spojení (odpadá TCP handshake)
- pokud v HTTP/2 čeká TCP na opakování (ztráta paketu), brzdí všechny proudy; v QUIC zpoždění jednoho proudu neovlivňuje ostatní

HTTP/3

- RFC 9114
- podobné HTTP/2, ale využívá QUIC → jednodušší
- jedno QUIC spojení, v něm nezávislé proudy pro jednotlivé dotazy a odpovědi na ně
- komprimuje hlavičky (QPACK, RFC 9204)
- umožňuje server push

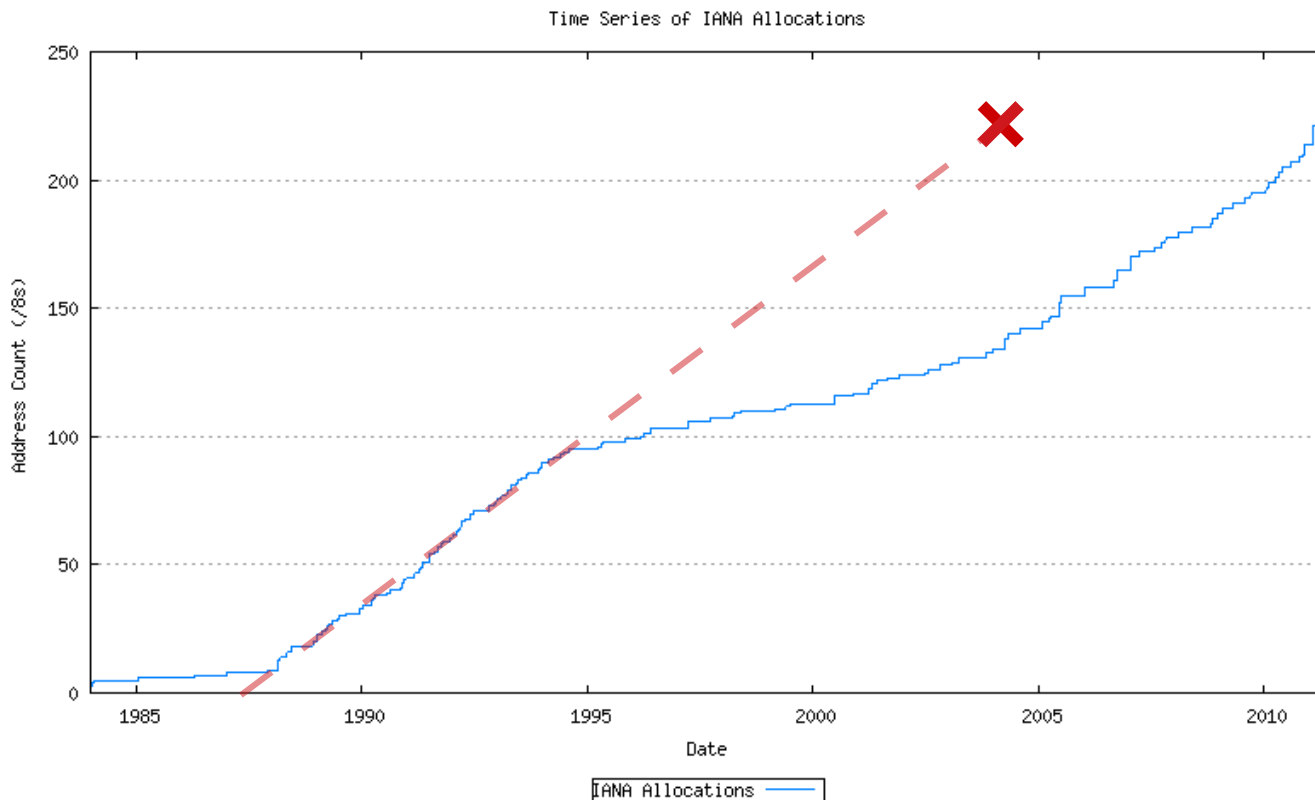
vytvořeno s podporou
projektu ESF



IP verze 6

Motivace

- počátek 90. let – zjevný nedostatek IPv4 adres
- opět aktuální



ipv4.potaroo.net

Vyčerpání adres

- IANA: únor 2011
- RIR
 - APNIC: duben 2011
 - RIPE NCC: září 2012
 - LACNIC: červen 2014
 - ARIN: září 2015
 - AFRINIC: duben 2017

Vlastnosti IPv6

- rozhodnuto zahájit vývoj nového protokolu, cíle:
 - dostatek adres (pokud možno navždy)
 - hierarchické směrování a adresace
 - zvýšení bezpečnosti (šifrování a autentizace přímo v IP)
 - služby se zajištěnou kvalitou
 - vysokorychlostní směrování
 - podpora mobilních zařízení
 - automatická konfigurace

IPv6 datagram

verze	třída provozu	značka toku		
délka dat		další hlavička	max. skoků	
adresa odesilatele				
cílová adresa				

Položky hlavičky

- RFC 8200
- **verze:** identifikuje verzi protokolu
- **třída provozu:** pro služby s definovanou kvalitou
- **značka toku:** identifikuje tok (proud souvisejících datagramů) pro vysokorychlostní směrování
- **délka dat:** počet bajtů za hlavičkou
- **další hlavička:** řetězení hlaviček (viz dále)
- **max. skoků:** analogie TTL, omezuje dosah

IPv4 datagram

verze	délka hlavičky	TOS	celková délka [B]	
identifikátor			přízn.	posun fragmentu
TTL	protokol		CRC hlavičky	
odesílatel (IP adresa)				
adresát (IP adresa)				
volby (nepovinné, proměnlivé složení)				
data				

Řetězení hlaviček

- délka hlavičky je konstantní (40 B) – urychluje zpracování
- případné **volitelné hlavičky** se připojují za ni
- položka **další hlavička** určuje typ hlavičky, která následuje, nebo protokol vyšší vrstvy
- každá rozšiřující hlavička obsahuje položku další hlavička – co je za ní
- pořadí hlaviček urychluje zpracování

Příklad řetězení

základní hlavička

další = 44 (Fragmentace)

hlavička Fragmentace

další = 60 (Volby pro cíl)

hlavička Volby pro cíl

další = 6 (TCP)

TCP data

Problémy řetězení hlaviček

- **zneužitelné**
 - dlouhé řetězce hlaviček zatěžují
 - RFC 7112: všechny hlavičky v prvním fragmentu
- zvyšují pravděpodobnost, že **datagram nedorazí**
 - firewally a různé nestandardní prvky
 - výsledky měření v RFC 7872 velmi depresivní – ztrátovost v řádu desítek procent

Adresy v IPv6

- délka 128 bitů (16 bajtů)
- zápis v šestnáctkové soustavě, čtveřice číslic odděleny dvojtečkou
- **2001:0718:1c01:0005:020b:dbff:fea1:d52c**
- úvodní nuly ve čtveřici lze vynechat
- jednu skupinu nulových čtveřic lze vynechat a nahradit dvěma dvojtečkami (např. smyčka je ::1)
- prefixy v obvyklém tvaru 2001:718::/32

Typy adres

- 3 typy adres:
- **individuální (unicast)**
 - určují jedno rozhraní
- **skupinové (multicast)**
 - určují skupinu rozhraní, data se doručují všem
- **výběrové (anycast)**
 - určují skupinu rozhraní, data se doručují nejbližšímu členovi

Globální individuální adresy



- první tři bity 001 (binárně)
- na začátku je **globální směrovací prefix**, politiku určují RIR (doporučeno: 48 b)
- identifikátor **podsítě** (zbytek do 64 b)
- identifikátor **rozhraní** (64 b)

Identifikátor rozhraní

- původně: vycházel z MAC adresy
 - modifikované EUI-64
 - problém: uživatele lze sledovat
- **krátkodobé náhodné adresy** (RFC 4941)
 - problém pro správce sítí
- **stabilní náhodné adresy** (RFC 7217)
 - hash z několika údajů (včetně prefixu)
 - stabilní, ale v různých sítích jiný – doporučeno

Objevování sousedů

- **Neighbor Discovery, ND**
- nahrazuje ARP + další možnosti
- **hledání linkové adresy:**
 - pošle **výzvu sousedovi** na skupinovou adresu s prefixem ff02:0:0:0:0:1:ff00::/104, k němuž připojí posledních 24 b hledané adresy (adresa pro vyzývaný uzel)
 - oslovený pošle **ohlášení souseda**
 - vyzývatel si zapíše do **cache sousedů** (a udržuje si zde informaci o jeho dosažitelnosti)

Automatická konfigurace

- **stavová (DHCPv6)**
 - podobně jako v IPv4 (pošle dotaz, server odpoví)
- **bezstavová (SLAAC)**
 - vše si obstará sám
 - výchoziskem **ohlášení směrovače** obsahující prefixy adres a jeho ochotu být implicitním směrovačem
 - počítač přidá své rozhraní k prefixu, ověří (objevováním sousedů) zda je volná a příp. začne používat
 - udržuje si tabulku implicitních směrovačů a střídá je

Směrovací protokoly

- nic speciálního, adaptace existujících protokolů
- **RIPng**
 - RIPv2 upravený pro IPv6 adresy
- **OSPFv3**
 - univerzální pro IPv4 i IPv6
- **BGP4+**
 - jediný používaný externí směrovací protokol (mezi autonomními systémy)

DNS

- záznamy **AAAA** pro IPv6 adresy
 - pc AAAA 2001:718:1c01:5:20b:dbff:fea1:d52c
- **reverzní:**
 - šestnáctkový zápis adresy včetně nul se obrátí
 - každá číslice se stává doménou
 - přípona **ip6.arpa**
 - c.2.5.d.1.a.e.f.f.f.b.d.b.0.2.0.5.0.0.0.1.0.c.1.8.1.7.0.1.0.0.2.
ip6.arpa

IPsec

- bezpečnostní mechanismy, dvě rozšiřující hlavičky:
- **Authentication Header (AH)**
 - ověření odesílatele
 - ochrana před změnou obsahu a opakováním
- **Encapsulating Security Payload (ESP)**
 - navíc šifrování obsahu – zašifruje vše za sebou
 - povinná a preferovaná
- databáze bezpečnostní politiky určuje pravidla pro zpracování datagramů

Mobilita

- mobilní počítač má domácí síť (zde je veden v DNS)
- po dobu nepřítomnosti jej zastupuje **domácí agent**
- pošle-li někdo datagram adresovaný cestujícímu počítači, domácí agent jej předá ESP tunelem
- mobilní počítač provede **optimalizaci cesty** – ohlásí partnerovi, že jeho aktuální adresa je jiná
- po optimalizaci budou data přenášena přímo

Přechodové mechanismy

- jak přejít od IPv4 k IPv6
- problém: IPv6 není zpětně kompatibilní
- **dual-stack** – podporují se oba protokoly, dnes nejčastější
- **tunelování** – oba konce hovoří stejným protokolem, síť mezi nimi ne
- **překlad** – datagramy se překládají z jednoho do druhého a naopak

Tunelování

- jeden protokol zabalen do druhého, přenesen „cizí“ sítí a na druhém konci vybalen
- statické tunely (tunel servery apod.)
- **6rd** – automatické, z jedné IPv4 adresy se vytvoří prefix pro adresování celé IPv6 sítě, RFC 5969
- **DS-Lite** – páteřní síť poskytovatele jen IPv6, IPv4 (s neveřejnými adresami) se zákazníkům doručuje tunely na centrální IPv4 NAT, RFC 6333

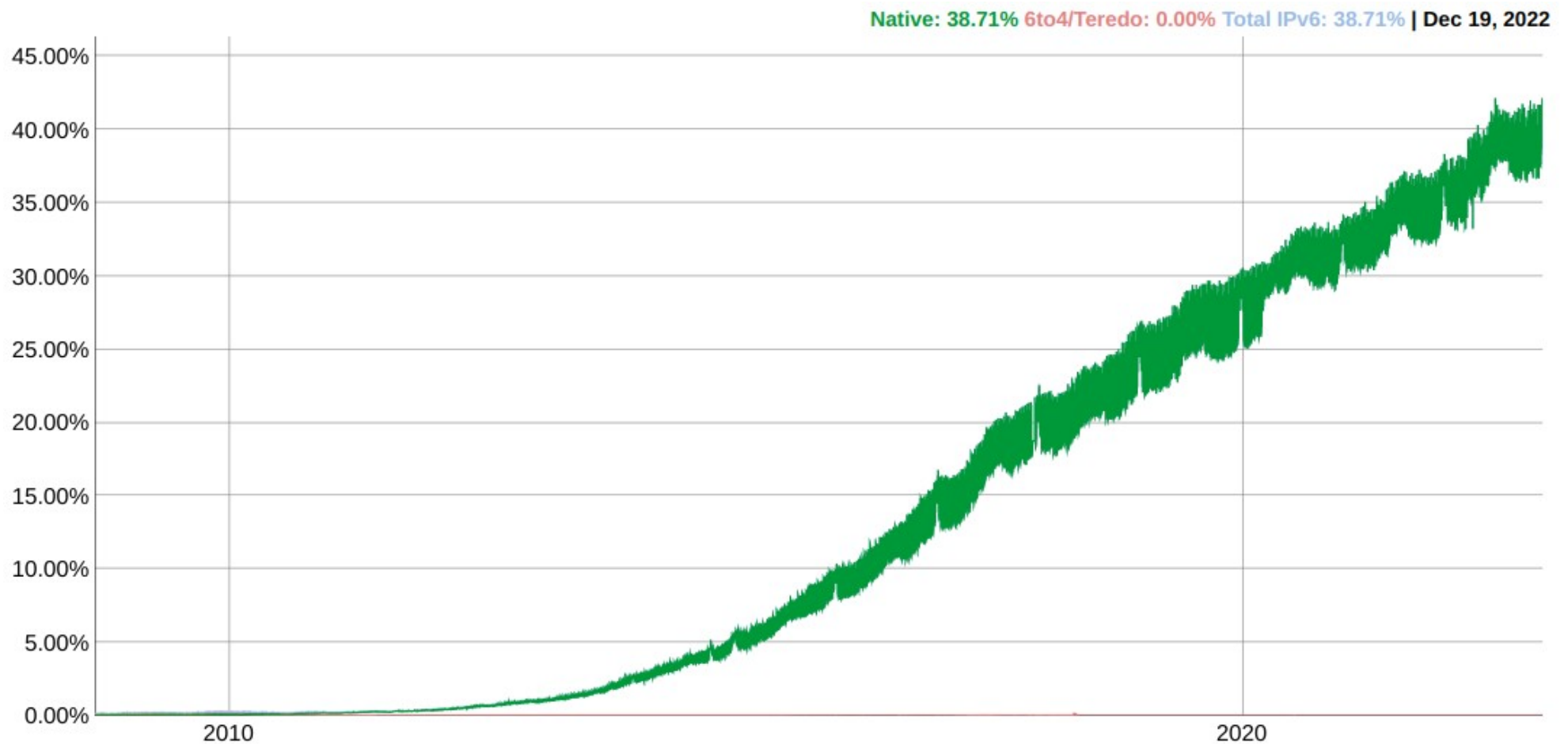
Překlad

- **SIIT** – pravidla, jak překládat kterou položku, neřeší adresy, využíváno ostatními, RFC 6145
- **NAT64 + DNS64** – překlad adres podobný IPv4 NATu, jednosměrné (přístup z koncové IPv6 sítě do IPv4 Internetu), RFC 6146 a 6147
- **464XLAT** – dvojitý překlad, páteřní síť poskytovatele jen IPv6, IPv4 se u zákazníka přeloží na IPv6 a na centrálním zařízení zpět do IPv4, používá T-Mobile v USA (70 mil. zákazníků), RFC 6877

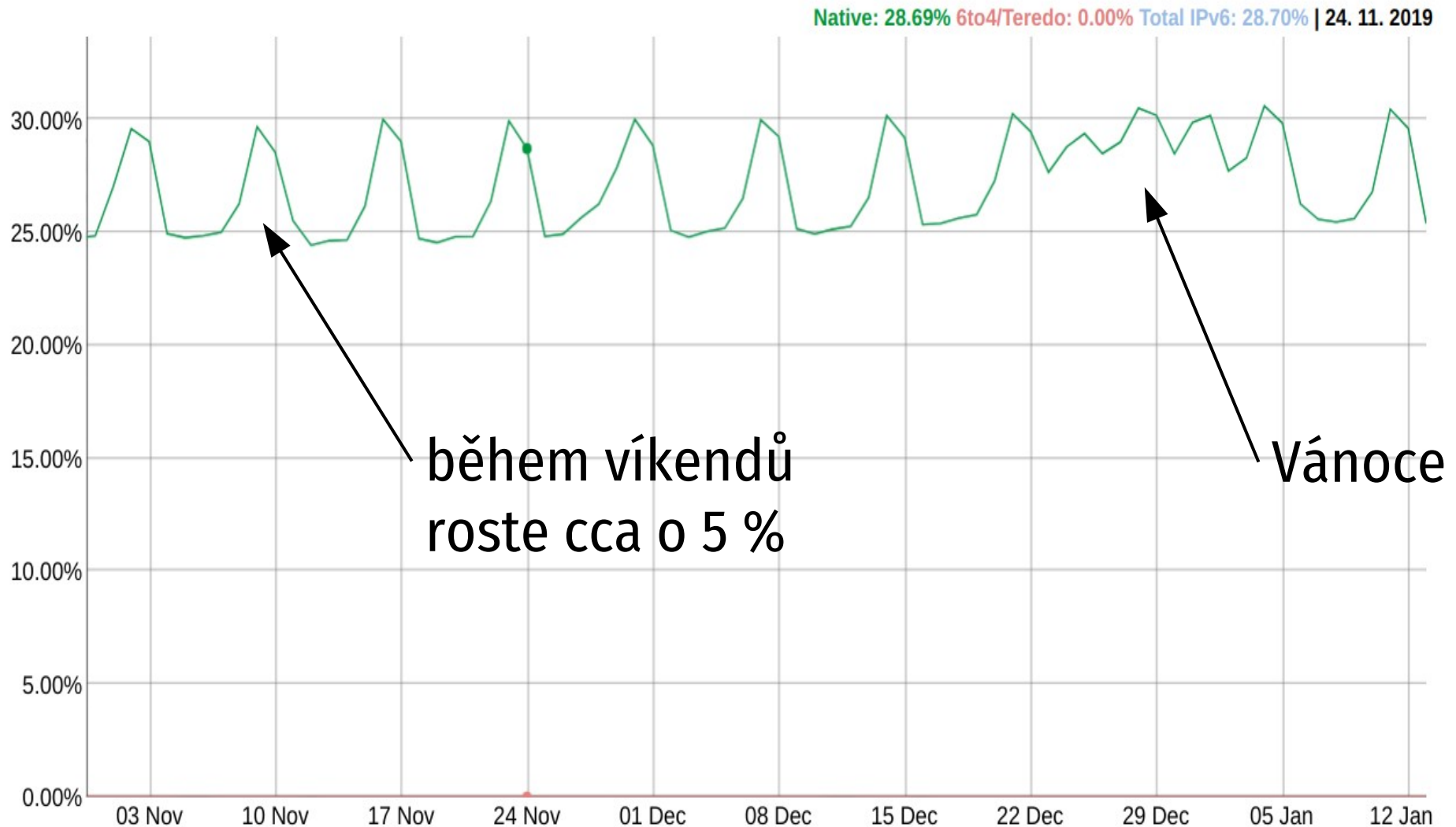
IPv6 v praxi

- Internet měl už dávno používat IPv6
- podporováno všemi současnými platformami
- dlouho se motalo v kruhu
 - proč bychom zpřístupňovali služby, když nejsou uživatelé
 - proč bychom doručovali uživatelům, když nejsou služby
- obavy z technických problémů
- World IPv6 Launch – 8. 6. 2011, nasadili velcí hráči (Google, Facebook, Akamai,...)

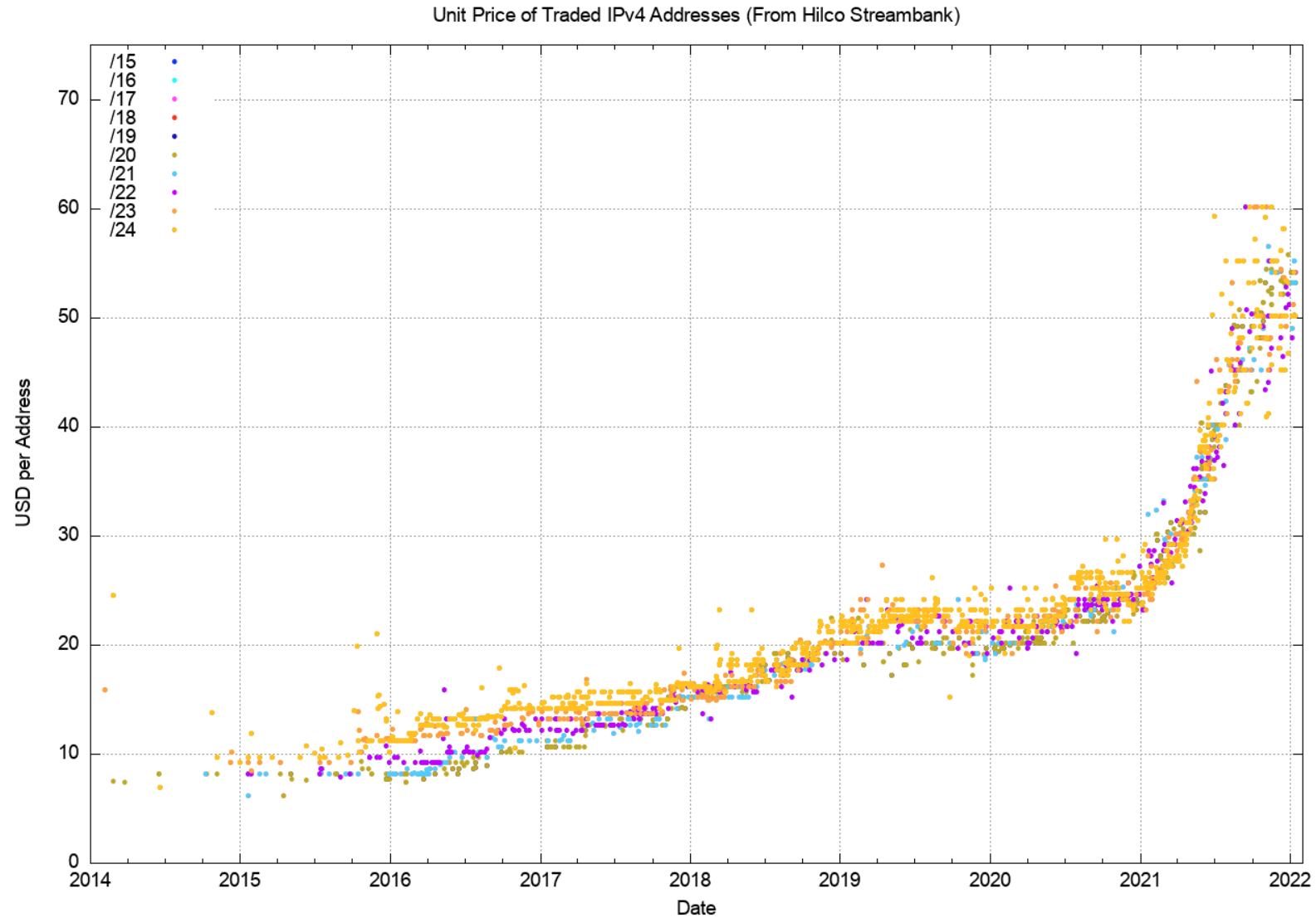
Statistika Google



Firmy jsou konzervativní

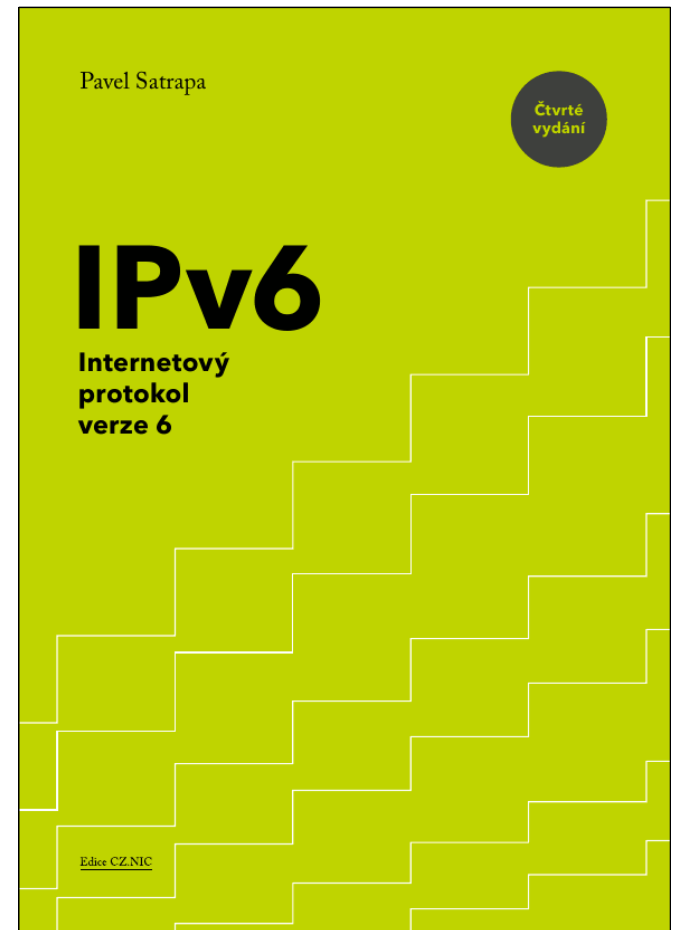


Cena IPv4 adresy



Podrobněji

P. Satrapa: IPv6
knihy.nic.cz



vytvořeno s podporou
projektu ESF

