

Datové sítě

Datové sítě

Autor: Jiří Peterka

zdroj: e-archiv

Vývoj datových sítí

V současné době probíhá **rozvoj datových sítí i na úkor rozvoje sítí původně určených pouze pro přenos hlasu**. Poptávka po službách přenosu dat rychle roste a trh s datovými službami není zatížen obrovskou setrvačností tradičního světa telekomunikací ani břemenem monopolních postavení.

Vše nasvědčuje tomu, že budeme svědky skutečné konvergence dvou dosud oddělených druhů sítí - hlasových a datových - do jedné univerzální sítě, schopné zajistit všechny požadované služby.

Jako "datová síť" (data network) se dnes chápe taková síť, která je určena pro přenos **digitálních dat**. Hlavní rozdíl mezi datovou sítí a sítí hlasovou je v tom, že **datová síť funguje na principu přepojování paketů (packet switching), zatímco síť hlasová funguje na principu přepojování okruhů (circuit switching)**.

Hlasové sítě původně fungovaly na analogovém principu, a to po mnoho desetiletí. Teprve v poslední době přešly tyto sítě na digitální způsob fungování, protože se to ukázalo jako výrazně výhodnější a efektivnější. **Tyto sítě dokáží vyhovět náročným požadavkům na kvalitu přenosových služeb, vyjádřenou například v celkovém přenosovém zpoždění či proměnlivosti tohoto zpoždění.**

Princip přepojování okruhů vyžaduje, aby se mezi komunikujícími stranami vždy nejprve vytvořilo spojení, v rámci kterého je také vyhrazena určitá přenosová kapacita. Tato vyhrazená kapacita pak až do následného zrušení spojení nemůže být přenechána nikomu jinému.

Datové sítě, fungující na principu přepojování okruhů, sice nejsou schopné garantovat kvalitu služeb, ale na druhé straně **efektivněji využívají dostupné zdroje a jejich služby proto mohou být výrazně levnější.**

Vývoj směřoval ke konvergenci

Datové sítě, se dlouhou dobu vyvíjely souběžně s hlasovými sítěmi. **Na počátku datové sítě byly ve skutečnosti realizovány jako nadstavba nad hlasovými sítěmi** (využívaly jejich přenosových schopností, například prostřednictvím modemů). **Rozvoj datových sítí probíhal výrazně rychleji, než rozvoj sítí hlasových.**

Datové sítě byly budovány v prostředí liberalizovaném, které je mnohem pružnější a schopné rychle reagovat jak na technologický vývoj, tak i na vývoj v poptávce.

V určitém okamžiku **rozvoje technologií pro přenos dat** se ukázalo, že dokážou zvládnout i **přenos hlasu (VOIP - Voice Over IP nebo VOFR - Voice over Frame Relay)**, Umožňují datovým sítím poskytovat stejné služby, které původně nabízely pouze sítě hlasové,

Výsledkem je "**konvergence**" sítí. Lze jej chápat jako **splývání dosud samostatných hlasových a datových sítí** a ústící v existenci jednotných **univerzálních sítí**.

Univerzální síť a kvalita přenosových služeb

Univerzální síť mají svou podstatou a mechanismem fungování nižších přenosových vrstev mnohem blíže k datovým sítím. Budou fungovat na principu **přepojování paketů**, a nikoli na principu přepojování okruhů. Současně však tyto univerzální sítě musí určitým způsobem vycházet vstříc požadavkům hlasových přenosů, které jsou dosti citlivé na přenosové zpoždění a na jeho rozptyl (a stejnou citlivost začínají vykazovat i některé kategorie "datových" aplikací, například různé multimediální přenosy).

Univerzální síť se snaží vycházet vstříc těmto specifickým potřebám zaváděním **podpory pro garanci přenosových služeb** (v této souvislosti se často používá i termín QoS, z anglického Quality of Service).

Způsob jakým se tak děje není dosud ustálen a nejspíše se bude ještě vyvíjet - jednou z možností je **přidělovat různým druhům přenášených dat různé priority**, díky kterým s nimi bude specifickým způsobem nakládáno při průchodu přes mezilehlé uzly (datové pakety s vyšší prioritou budou mít přednost oproti paketům s nižší prioritou). S podporou různých priorit přenášených dat sice počítají i dnes běžně používané protokoly (například protokol IP), ale tyto možnosti nejsou v praxi podporovány, resp. implementovány.

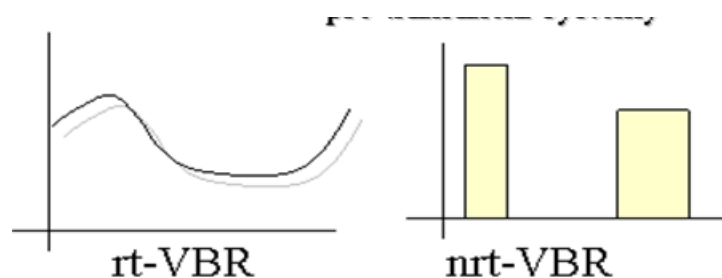
Jedním ze směrů je řešení s názvem **MPLS (MultiProtocol Label Switching)**. Viz samostatná část – MPLS.

Další možností jsou **různé rezervační metody**, které fungují na jiném principu: z celkové dostupné přenosové kapacity, která je mechanismem přepojování paketů využívána vždy celá (k přenosu těch paketů které jsou na řadě a mají být přeneseny), se "vyřízne" (vyčlení, rezervuje) určitá přenosová kapacita pro takové přenosy, které mají specifické nároky a požadavky. Takto vyčleněná přenosová kapacita pak může být využita i na původním principu přepojování okruhů, který je schopen garantovat požadované parametry přenosu.

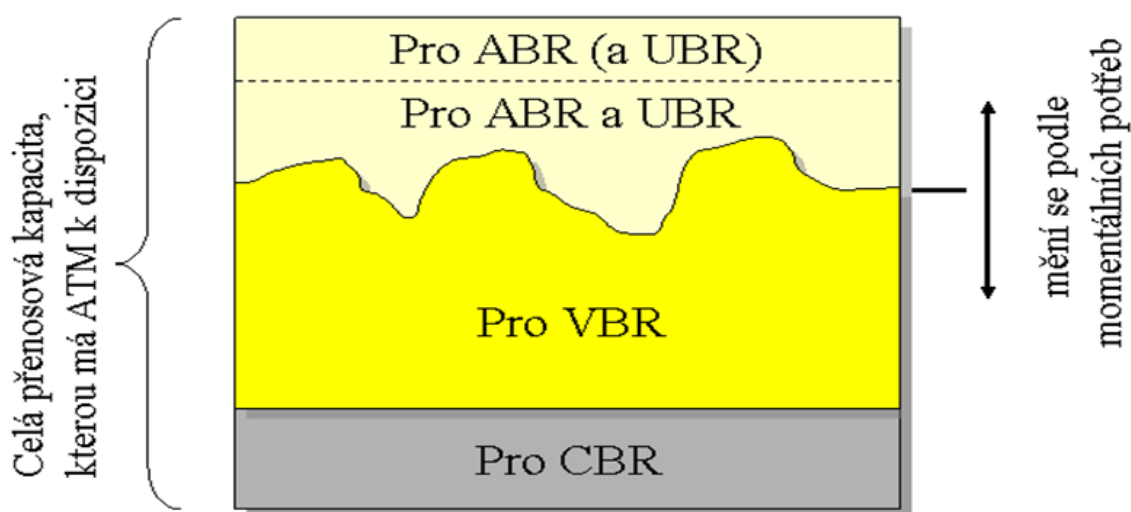
Služby datových sítí

Třídy služeb

- **CBR Constant Bit Rate** – garantuje objednanou přenosovou kapacitu. Jedná se o obodbu pronajaté linky. Vhodné pro nekomprimované video. Datové toky s konstatní zátěží.
- **VBR Variable Bit Rate** – garantuje maximální přenosovou kapacitu. Vhodné pro dávkové přenosy a komprimované video. Přenosy s nárazy datové zátěže. Dále se dělí dle obrázku



- **ABR Available Bit Rate** - garantuje minimální přenosovou kapacitu. Vhodné pro přenosy s garantovanou odezvou např. technologická zařízení. Přenosy s určitou dobou odezvy.
- **UBR Unspecified Bit Rate** – negarantuje nic. Využívá co je momentálně k dispozici. Tímto se blíží nejvíce službě „best effort“ tj. klasickému ethernetu.



	CBR	RT-VBR	NRT-VBR	ABR	UBR
Garance přenosové kapacity	Ano	Ano	Ano	Částečně	Ne
Vhodné pro real-time přenosy	Ano	Ano	Ne	Ne	Ne
Vhodné pro nárazový (bursty) provoz	Ne	Ne	Ano	Ano	Ano
Informuje o zahlcení	Ne	Ne	Ne	Ano	Ne

Terminologie datových sítí

Pojmy "veřejná datová síť" či "virtuální privátní síť", alias VPN.

Datovou sítí je každá síť sloužící k přenosu dat a fungující na principu přenosu paketů. Tedy například lokální síť (síť LAN), která propojuje počítače v určité lokalitě, například v počítačové učebně či kanceláři. Stejně tak je nutné považovat za datové sítě i sítě rozlehlé (síť WAN), které propojují různé lokality na větší vzdálenosti, například v různých zemích světa, či alespoň v různých městech. V praxi se pod pojmem "datová síť" nejčastěji rozumí síť propojující více různých lokalit a sloužící potřebám propojení lokálních sítí v těchto lokalitách.

Privátní je taková datová síť, kterou si určitý subjekt buduje, provozuje a také využívá sám. Typickým příkladem mohou být sítě, které si budují subjekty s pracovišti dislokovanými v různých lokalitách, za účelem propojení těchto lokalit (ve skutečnosti za účelem propojení lokálních sítí v těchto lokalitách).

Protipólem "privátní" datové sítě je **datová síť "veřejná"** - jak její přívlastek naznačuje, je tato síť otevřena nejširší veřejnosti, které nabízí své služby spočívající v přenosu dat. Uživatelem takovéto sítě se skutečně může stát kdokoli, kdo o to má zájem a je ochoten za to zaplatit, resp. přistoupit na podmínky toho, kdo takovouto síť provozuje. Provozovatelem přitom bývá takový subjekt, který svou datovou sám nepoužívá - vlastní ji a provozuje především proto, aby její služby mohl poskytovat na komerční bázi jiným subjektům.

Zřizování a provozování veřejných datových sítí ve většině zemí světa vyžaduje získání licence (licence na poskytování veřejných služeb přenosu dat), a v praxi pak velmi záleží na tom, jaké konkrétní možnosti a podmínky zde platí.

V ČR byl až do poloviny roku 1995 stav takový, že licenci na poskytování veřejných datových služeb vlastnil tehdejší Eurotel, a byla to licence exkluzivní - což znamenalo, že služby přenosu dat nemohl nabízet nikdo jiný (neboť na to nemohl získat licenci).

Ke změně došlo až v citované polovině roku 1995, kdy Eurotel přešel majoritně pod křídla SPT Telecom a musel si pořídit novou licenci. Ta již byla udělena jako neexkluzivní, a potřebné oprávnění k provozování datových služeb nejširší veřejnosti pak mohly získat i další subjekty. Od té doby se u nás datuje jak výrazný rozvoj veřejných datových sítí, tak například i rozvoj Internetu - dřívější exkluzivita Eurotelu totiž vylučovala existenci plně komerčních poskytovatelů připojení (providerů), neboť jejich služby (přístup k Internetu) byly chápány jako datové služby.

Poloveřejné, nebo poloprivátní?

Mezi čistě privátními datovými sítěmi a sítěmi plně veřejnými existují v praxi různé varianty. **Subjekty si mohou budovat, provozovat a také používat vlastní datové sítě, ale z různých důvodů je předimenzovávají a samy nevyužívají veškerou jejich kapacitu.**

Nevyužité kapacity privátních sítí mohou být nabízeny dalším subjektům, na takové bázi jakou si zúčastněné strany dohodnou - může jít o plně komerční (tedy: placenou) službu, nebo o určitou formu reciprocitu za jiné služby, podporu partnerských organizací apod.

Další možností pak jsou takové **sítě, které jsou budovány a provozovány v zásadě jako veřejné (tedy s tím, že jejich vlastník je sám nebude využívat) ale jejich služby nenabízí zcela veřejně, nýbrž pouze určitému specifickému okruhu uživatelů (například jen akademickým uživatelům)**. Důvody mohou být různé, jedním z velmi pádných může být i nemožnost získat potřebné oprávnění (licenci) pro skutečně veřejné poskytování datových služeb. V ČR to bylo aktuální do zmiňovaného přelomu roku 1995, do kdy bylo možné získat pouze licenci na neveřejné datové služby, poskytované pouze specificky vymezenému okruhu uživatelů.

Prostor pro outsourcing

Jednorázové vybudování i trvalé provozování datové sítě je něčím, co vyžaduje nemalé lidské zdroje a knowhow. Některé firemní subjekty takového zdroje nemusí mít, nebo se jim nemusí vyplatit si je pořídit. Pro ně je pak vhodným řešením outsourcing, neboli řešení založené na externí dodávce.

Outsourcing se v případě datových sítí může týkat jednorázového pořízení, kdy celou síť někdo "postaví na klíč". Stejně tak se ale může týkat i provozu datové sítě, přesněji průběžné správy a systémové péče o chod sítě, podpory uživatelů atd. Stále se však může jednat o ryze privátní datovou síť, protože jejím vlastníkem i jediným uživatelem je stále jeden původní subjekt.

Virtuální privátní síť

Část veřejné či "poloveřejné" datové sítě se vůči svým uživatelům chová jako síť privátní. Tj. Má samostatný adresový prostor (samostatné adresy, principiálně odlišné od adres jiných uživatelů téže fyzické sítě), a také možnost přímé komunikace pouze mezi uživateli. Virtuální privátní síť garantuje svým uživatelům určitou přenosovou kapacitu.

Je zajištěno zabezpečení přenášených dat - není problémem data při vstupu do sítě zakódovat, nechat je přenést zakódovaná, a při výstupu ze sítě je odkódovat.

Realizace datových sítí - vývoj

X.25: Pouze navenek, nikoli uvnitř

Protokoly X.25 se používaly pro potřeby veřejných datových sítí. Dlouhou dobu platilo, že co veřejná datová síť, to síť na bázi protokolů X.25 - natolik byly tyto protokoly v dané oblasti dominantní. Zajímavé ale je, že právě u veřejných datových sítí **byly protokoly X.25 nasazovány a využívány pouze na rozhraní mezi veřejnou datovou sítí a jejími uživateli - přístupová technologie pro potřeby přístupu koncových uživatelů (či: zákazníků) k datové síti**, zatímco uvnitř mohla datová síť fungovat jiným způsobem.

Důvodem pro zavádění takového iluze byla snaha o jednotnost: pokud jsou služby veřejných datových sítí nabízeny nejširší veřejnosti, je velmi žádoucí, aby technické podmínky pro připojení k takovéto síti a komunikaci s ní byly jednotné pro všechny potenciální zákazníky (a právě to realizovaly protokoly X.25). Fungování každé konkrétní sítě "uvnitř" pak může být odlišné, a je výlučně záležitostí jejího provozovatele.

Protokoly X.25 se s úspěchem používaly i pro realizaci privátních datových sítí - zde však i "uvnitř", a ne pouze na rozhraní mezi sítí a uživatelem. Vlastníci a provozovatelé privátních datových sítí neměli zapotřebí skrývat skutečný způsob fungování sítě, kterou měli "plně ve své moci". Přesto ale i oni velmi často volili právě protokoly X.25, a to zejména pro jejich celkovou robustnost i pro dostupnost produktů na bázi X.25.

Změnily se mnohé z původních předpokladů, ze kterých koncepce X.25 vycházela.

- spolehlivost přenosových cest se zlepšila (resp. jejich chybovost klesla), a tak výrazně poklesla i potřeba silných mechanismů pro zajištění spolehlivosti.
- výrazně vzrostla poptávka po rychlosti a na celkovou propustnost přenosových částí sítě.
- původní předpoklad, že spolehlivý přenos je jediný žádoucí, zatímco nespolehlivou přenosovou službu by nikdo nechtěl, neplatí. Multimediální aplikace dávají přednost rychlosti a pravidelnosti přísunu dat a naopak některé aplikace si spolehlivost raději zajistí samy, protože ta kterou by poskytovala přenosová část sítě pro ně není dostatečná.

Technologie X.25 dokázala zareagovat na tyto trendy například tím, že zvýšila svou maximální možnou přenosovou rychlost - původní verze protokolů X.25 z roku 1974 počítala jen s přenosovými rychlostmi do 64 kbps, a teprve novější verze standardu (z roku 1992) zvýšila rychlostní limit až na 2 Mbps.

Jiných svých vlastností se ale X.25 nedokázala zbavit, resp. překonat je a aktualizovat podle potřeby. Jde zejména o **zátěž mechanismů pro zajištění spolehlivosti, způsobující zbytečnou neefektivnost**.

Právě z tohoto důvodu je dnes X.25 považována za přežitou, i když stále ještě používanou technologii.

Další vývojovou etapou je Frame Relay

Cesta dalšího vývoje, hnaná především požadavkem na **co nejvyšší efektivnost přenosů**, se nejprve postarala o odstranění mechanismů pro zajištění spolehlivosti - **tím se z technologie X.25 stala technologie Frame Relay**.

Frame Relay je technologie, která na rozdíl od X.25 funguje již jen na linkové vrstvě, a je schopna vytvářet iluzi dvoubodového spoje mezi dvěma lokalitami. Snaží se také spojovat výhody mechanismů přepojování okruhů a přepojování paketů - lze se na ni dívat jako na funkční analogii vyhrazených pevných okruhů, ovšem realizovanou prostřednictvím sítí fungujících na principu přepojování paketů. Díky tomu mohou být sítě na bázi Frame Relay ekonomicky výhodnější, než klasické pronajaté okruhy.

Rámec FR

- proměnná délka rámce, **max. cca 8kB** (?)
- pro přenos uživatelských dat, **jediný typ rámce, nejsou sekvenční čísla** (není flow-control a error-control)

Struktura rámce

Flag | Address | Information | FCS | Flag

Pole adresy:

DLCI: Data Link Connection Identifier

- identifikátor virtuálního spojení (10 bitů) - 1024

DE: Discard Eligible

- určuje vhodnost rámce jako kandidáta na likvidaci (priority, congestion control)

FECN: Forward Explicit Notification Control – řízení toku
BECN: Backward Explicit Notification Control - řízení toku

C/R: bit command/response, uživatelsky závislé využití

Princip přepínání

- **virtuální okruhy identifikovány DLCI**, DLCI má vždy lokální význam
- frame handlery (switche) mají **přepínací tabulky** ve tvaru:

`< in-line, in-DLCI, out-line, out-DLCI >`

- **během přepínání se testuje FCS (kontrolní součet)**, při chybě se rámce zahazuje

DLCI 0 vyhrazen pro signalizaci, vyhrazený DLCI pro management

Parametry kontraktu o spojení mezi uživatelem a sítí:

- **Committed Information Rate (CIR)**, garantovaná minimální průchodnost sítě (**commitment** = [smluvní] závazek).
- Excess Information Rate (EIR),
- Committed Burst Size (Bc) - maximální objem dat, která je síť ochotna přenést během určitého časového intervalu (Tc)
- Excess Burst Rate (Be) - maximální objem dat, o který se smí překročit Bc během intervalu Tc, doručuje se s nižší pravděpodobností

Vazba na IP

- **Frame-relay map (tabulka na koncové uzlu pro získání DLCI z IP)**
- Inverse ARP (získání IP dotazem na druhý konec virtuálního okruhu)
- Seznam aktivních virtuálních okruhů zjistitelný přes LMI

Technologie Frame Relay dokáže garantovat určitou minimální propustnost pro jednotlivé virtuální přenosové okruhy které vytváří (podle toho, jakou hodnotu parametru CIR, Committed Information Rate si uživatel/zákazník sjedná). Vedle toho se ale Frame Relay snaží v praxi nabízet i vyšší přenosové kapacity, pokud je možné je poskytnout a jsou požadovány.

ATM

Další technologií, která se výrazně prosadila v oblasti datových sítí, je technologie ATM. Lze ji chápat také jako další **vývojovou variantu ve sledu protokolů X.25 a Frame Relay**, i když technologie ATM původně vznikla spíše jako řešení pro potřeby "světa spojů". Poměrně brzy se ale začala prosazovat i jako řešení použitelné i ve "světě počítačů", a to zejména kvůli své snaze **spojit výhody mechanismů přepojování paketů a přepojování okruhů**.

V tomto ohledu je tedy technologie ATM podobná technologii Frame Relay, i když přeci jen mezi nimi existuje výrazná odlišnost: **Frame Relay přenáší rámce proměnné velikosti (na úrovni linkové vrstvy)**. Naproti tomu **ATM přenáší bloky dat pevné velikosti, v zásadě také na úrovni linkové vrstvy**.

Bloky dat, které technologie **ATM přenáší, jsou opravdu velmi malé - mají jen 53 bytů, z nichž 5 bytů tvoří hlavičku a 48 bytů užitečný náklad**. Říká se jim "buňky" (cells), a hlavní předností jejich malé velikosti je jejich počet - sice "unesou" málo dat, ale na druhé straně může být takovýchto ATM buněk přenášeno opravdu hodně, a kdykoli je zapotřebí odněkud někam rychle přenést nějaká data, je statisticky větší šance najít volnou buňku do které bude možné data vložit a odeslat (s rostoucí velikostí buněk, resp. bloků tato pravděpodobnost klesá). Díky této své vlastnosti pak technologie ATM dokáže dobře vyhovět potřebám různých multimediálních přenosů včetně přenosů hlasových, citlivých na velikost přenosového zpoždění a jeho rozptýl.

Schopnost technologie ATM **vycházet vstříc různým požadavkům na kvalitu služeb** (QoS, Quality of Service) je její velkou předností. Na druhou stranu velkou nevýhodou technologie ATM je její celková komplikovanost a nepružnost, i úplně jiný "pohled na svět", než jaký je dnes obvyklý ve světě datových komunikací. Většina dnešních počítačových aplikací například dává přednost tzv. nespojovanému přenosu, při kterém není navazováno spojení. To ATM nepodporuje a pracuje pouze na tzv. spojovaném principu (vždy předpokládá, že mezi komunikujícími stranami je vytvořeno spojení, v rámci kterého jsou také dohodnuty požadované parametry komunikace). Další nevýhodou ATM je to, že nepodporuje tzv. všesměrové vysílání, neboli broadcast (čili vysílání jednoho uzlu současně ke všem ostatním uzlům).

Všechny tyto vlastnosti pak podstatně **komplikují provozování typických "počítačových" aplikací nad ATM sítěmi - příslušné "napasování" přenosových protokolů vyšších vrstev (zejména protokolu IP) nad ATM je hodně složité a ztrácí se při něm mnoho z celkové výkonnosti ATM**.

IP over everything

Je-li technologii ATM vytýkána její velká složitost a nepružnost, pak úplným protikladem k ní jsou protokoly z rodiny TCP/IP, konkrétně přenosový protokol IP.

Efektivita byla i původním záměrem autorů TCP/IP, který lze charakterizovat sloganem "IP nad vším" (IP over everything).

Protokol IP byl samozřejmě od začátku koncipován jako základní přenosový protokol pro datové sítě (v obecném slova smyslu, pro sítě určené k přenosu dat a fungující na principu přepojování paketů). Původně se používal především pro potřeby Internetu, ale s postupem času se začal prosazovat i do dalších sítí, včetně těch, které je dnes možné považovat za typické veřejné či privátní sítě. **Stal se také převažujícím protokolem, který svým uživatelům nabízí dnešní virtuální privátní sítě.**

Nad protokolem IP jsou dnes provozovány opravdu nejrůznější aplikace, včetně přenosů hlasu a nejrůznějších multimediálních aplikací. Zde se samozřejmě naráží na problém toho, že protokol IP (ani jiné protokoly z rodiny TCP/IP) nepodporují různé úrovně kvality služeb, a "měří všem stejně", na principu maximální snahy, ale nezaručeného výsledku (viz úvodní článek).

Absence podpory kvality služeb se v prostředí IP sítí řeší v zásadě třemi různými způsoby:

- zaváděním mechanismů pro podporu kvality služeb (viz úvodní článek)
- zvyšováním celkové dostupné přenosové kapacity, v očekávání že její dostatek bude statisticky minimalizovat situace, kdy se nebude dostávat zdrojů pro uspokojení všech souběžných požadavků
- zaváděním nových technik digitalizace a komprese, které snižují citlivost multimediálních aplikací (včetně přenosu hlasu) na kvalitě přenosových služeb.

Možností řešení linkové vrstvy je tzv. WAN Ethernet a nebo METRO Ethernet.

Všechny výše uvedená řešení datových sítí na linkové vrstvě navazují na řešení fyzické vrstvy. **Většinou se pro realizaci rozsáhlých sítí používají optická média.** Standardní přístup k tomuto médiu je uveden dále.

Řešení přístupu k fyzickému médiu pro datové sítě je například SONET nebo SDH.
SONET Synchronous optical network / SDH

Byl vytvořen **jako náhrada PDH** pro přenos velkého množství telefonních a datových přenosů, a aby byla **sjednocena technologie zařízení různých výrobců**. Synchronizace je pomocí atomových hodin.

Synchronous Digital Hierarchy (SDH) standard vytvořen [ITU \(G.707\)](#) a jeho rozšíření [G.708](#) byl vytvořen ze zkušeností SONETu. SONET se používá v [USA](#) a [Kanadě](#), SDH ve zbytku světa. SDH doplněná například o ATM se stává nejvýhodnější technologií přenosu dat všech druhů.

Dat.rychlosti:

SONET/SDH Designations and bandwidths

SONET Optical Carrier Level	SONET Frame Format	SDH level and Frame Format	Payload bandwidth ^[1] (kbit/s)	Line Rate (kbit/s)
OC-1	STS-1	STM-0	48 960	51 840
OC-3	STS-3	STM-1	150 336	155 520
OC-12	STS-12	STM-4	601 344	622 080
OC-24	STS-24	STM-8	1 202 688	1 244 160
OC-48	STS-48	STM-16	2 405 376	2 488 320
OC-96	STS-96	STM-32	4 810 752	4 976 640
OC-192	STS-192	STM-64	9 621 504	9 953 280
OC-768	STS-768	STM-256	38 486 016	39 813 120
OC-1536	STS-1536	STM-512	76 972 032	79 626 120
OC-3072	STS-3072	STM-1024	153 944 064	159 252 240

Základní jednotkou **SDH je STM-1 (Synchronous Transport Module-level 1)** vycházející z STS-3, pracující na trojnásobné rychlosti 155.52 kbit/s oproti STS-1.

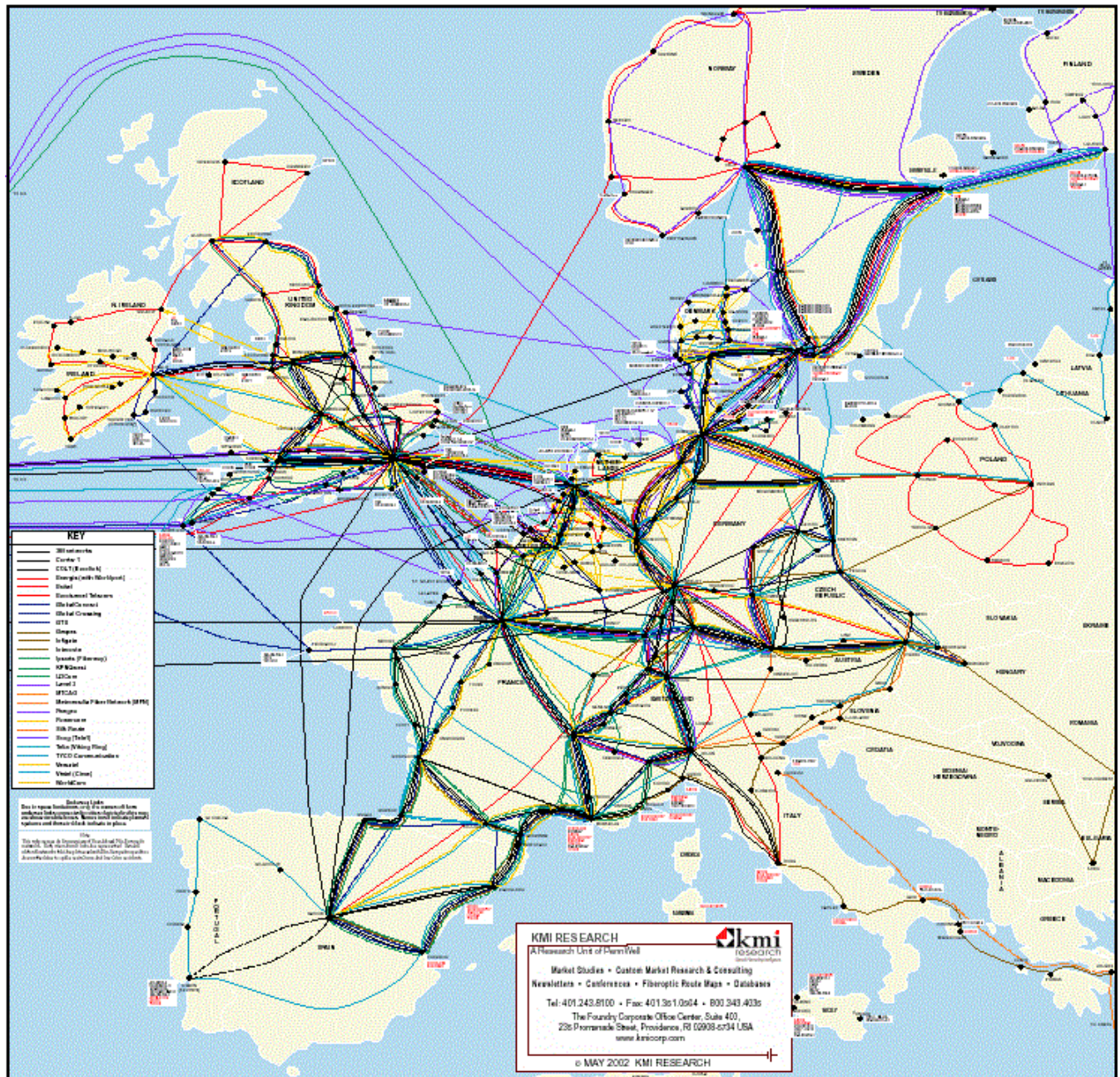
Poskytovatelé Internetového připojení

Domácnosti, firmy a další platí poplatky ISP za poskytování připojení k Internetu. Otázka zní, **komu platí tyto ISP za přístup k internetu? A komu platí tyto za přístup k Internetu?**

ISP se člení na tři úrovně (tiery): Tier 1, 2, 3.

Tier 1 ISP

Je jich celkem 15 (z toho 9 má HQ v USA). Jsou to společnosti, které mají ve správě hlavní síťové rozvodny Internetu a propojení mezi nimi. Jádrové rozvodny jsou propojené jak v rámci jedné společnosti, tak s rozvodnami několika ostatních Tier 1 ISP. Přesná světová mapa není k dispozici, ale takto vypadá rozložení hlavních datových rozvodů v Evropě:



Je vidět, jak se kabely sbíhají ve velkých městech, kde jsou rozvodny. Od Británie poté vede pás optických podmořských kabelů středem Atlantiku k pobřeží USA.

15 Tier 1 ISP tvoří tzv. **páteř internetu (Internet Backbone)**. Tier 1 ISP neplatí nikomu poplatky, naopak – každý, kdo potřebuje přístup do globálního Internetu, musí platit poplatky **Tier 1 ISP**. Na tuto páteřní síť se napojují buď Tier 2 ISP, nebo centra největších světových společností.

Tier 2 ISP

Neboli národní/regionální ISP – poskytují připojení v rámci svého státu (nebo jeho oblasti), a **platí za připojení k páteřní Tier 1 síti**. Tier 2 poskytovatelé mohou být navzájem propojeni – všechna data tak nemusí putovat přes páteřní síť, a tím se zamezí jejímu přetížení.

Velké korporace si opět mohou v rámci zvýšení spolehlivosti či rychlosti zařídit připojení přímo s Tier 2 rozvodnami, ale jejich hlavní účel je poskytnout přístup Tier 3 ISP:

Tier 3 ISP

Alias lokální poskytovatel připojení – obvykle pokrývají oblast jednoho města + jeho okolí. **Za přístup k Internetu samozřejmě platí poskytovatelům druhé úrovně.**

Od těchto ISP si domácnosti a běžné instituce pořizují přístup k Internetu

Vývoj datových sítí

Konvergence sítí

Autor: Jiří Peterka

zdroj: e-archiv

O co jde v rámci roamingu?

Původní návrhy, obsažené v Propojeném kontinentu, **chtěly řešit roaming tak, že ho fakticky zruší**. Tedy ve smyslu eliminace roamingových příplateků, resp. rozdílů v ceně: **využívání služeb v roamingu mělo stát stejně, jako využívání stejných služeb doma**, v domovské zemi příslušného zákazníka, resp. uživatele.

Tento záměr se pochopitelně **nemohl líbit operátorům**, kteří na roamingu vydělávají díky značně vysokým maržím – které by se zde vlastně úplně eliminovaly. Navíc museli dostat strach z toho, že by jim mohli rázem **začít konkurovat operátoři z dalších zemí, jejichž služby (a SIM karty) by si zákazníci kupovali právě kvůli tomu, aby je mohli využívat v jiné zemi (ze svého pohledu „doma“), v rámci roamingu, ale za podmínek a „domácích“ cen příslušného zahraničního operátora.**

Právě kvůli tomuto nebezpečí se pak **začaly složitě hledat různé pojistky**, charakteru „zastropování“ či „nastavení maxima“. Fakticky by se jednalo u určité FUP, nutící uživatele, aby princip „v roamingu jako doma“ (anglicky: RLAH, Roam like at home) nevyužívali „přespříliš“. Jenže nalezení takového pojistky se nepodařilo.

Nepodařilo se i kvůli nejasnostem kolem toho, jaké by vše mělo dopady na trhu a ekonomiku operátorů. To by vyžadovalo určitou analýzu – a tak vznikl další spor ohledně toho, kdy a jak takovou analýzu dělat. Zda nejprve zavést změny a pak analyzovat jejich dopady, nebo nejprve analyzovat a pak teprve něco měnit. Tak ostatně vyznělo u vyjádření českého účastníka příslušných jednání na půdě Rady EU.

Svým způsobem se tak **jednání ohledně roamingu**, ještě pod vedením italského předsednictví, **dostala do slepé uličky**. Nové lotyšské předsednictví ale hned na počátku roku přišlo s poměrně radikálním návrhem, od kterého si slibuje vyvést jednání ze slepé uličky. První verze tohoto návrhu se objevuje v [pracovním dokumentu](#) nového předsednictví ze 7.1.2015, a zástupci

jednotlivých členských zemí o něm poprvé jednali na [pracovním jednání](#) Rady 23. ledna. Následně byl návrh upřesněn v [novém dokumentu ze 27. ledna](#), který mají projednávat pracovní skupiny počátkem února.

Co je přístup k Internetu?

Kromě toho v [novém návrhu](#) lotyšského předsednictví přeci jen přibyla **určitá definice, a to „služby přístupu k Internetu“ (Internet access service)**. Schválně si ji **srovnáme s naší domácí definicí**, obsaženou v pravidlech řízení datového provozu od ČTÚ:

[návrh EU] Službou přístupu k internetu se rozumí veřejně dostupná služba elektronických komunikací, která poskytuje přístup k internetu, a tím i konektivitu mezi prakticky všemi koncovými body internetu, bez ohledu na použitou technologii sítě a použité koncové zařízení

[definice ČTÚ] Službou přístupu k síti internet se rozumí veřejně dostupná služba elektronických komunikací, která umožňuje **využívání obsahu, aplikací a služeb sítě** internet, a tím propojení prakticky všech koncových bodů připojených k síti internet (a to protokolem IPv4 a IPv6), bez ohledu na použitou technologii sítě.

Rozdíl je v tom, že naše definice hovoří (kromě propojení, resp. konektivity) také o možnosti využívání obsahu, aplikací a služeb, což nově navrhovaná unijní definice nedělá. Navíc naše definice explicitně zmiňuje IPv4 a IPv6 - ale obě dvě definice požadují obecnou nezávislost na zvoleném technickém řešení (technologii sítě).

Unijní definice navíc zmiňuje i nezávislost na použitém koncovém zařízení, což naše definice nedělá. To nejspíše souvisí s tím, že unijní definice hovoří jen o samotné konektivitě, kterou lze poskytnout jakémukoli koncovému zařízení – zatímco s možností využití veškerého obsahu, aplikací a služeb na všech koncových zařízeních už to tak jisté a jasné není.

Co zero rating?

V rámci svého nového návrhu pak lotyšské předsednictví otevírá dva nové (a i dle mého názoru velmi důležité) problémy.

První se týká toho, čemu se běžně říká **zero rating (ve smyslu: nezapočítávání)**, ale co **návrh pojmenovává jako „pozitivní cenovou diskriminaci“**. Fakticky jde o to, že **určitý druh datového provozu je vyjmut z FUP a není počítán do objemových limitů v rámci datových tarifů**. Příkladem mohou být datové tarify, které do FUP nezapočítávají například přístup na Facebook, nebo jiné konkrétní servery, služby atd.

Je ale takováto praktika správná, či alespoň přípustná a tolerovatelná? **Třeba v Nizozemí, kde na síťovou neutralitu hodně dbají, je zero rating zakázaný**. Nedávno za něj udělil vysoké pokuty národní regulátor i [ve Slovinsku](#) – ale ostatní členské země EU v tomto ohledu nejsou ještě „zcela rozhodnuté“. Výjimkou je přidružené Norsko, které se k zero ratingu **staví také jednoznačně negativně**. Naopak v ČR je zero rating celkem běžně používán (a stal se i důvodem určitých kontroverzí, [kritizovaných i zde na Lupě](#)).

Když nové lotyšské předsednictví „nadhodilo“ **možnost zákazu zero ratingu** (resp. pozitivní diskriminace), dočkalo se souhlasu od některých členských zemí, ale nesouhlasu od jiných. A ve svém [dokumentu z 20.1.2015](#) konstatovalo, že podle jeho názoru není reálné dosáhnout souhlasu se zákazem. Proto předsednictví navrhuje takový kompromis, který by umožnil

jednotlivých členským zemím, aby si to rozhodly samy, na své národní úrovni – bohužel s tím negativním dopadem, že výsledek nebude jednotný a v různých zemích to dopadne různě. Což opět jde proti původnímu principu jednotného telekomunikačního trhu, se stejnými podmínkami.

Co blokování z vlastní vůle?

Druhý problém se týká toho, **zda providerům má být umožněno blokovat či jinak omezovat určitý druh obsahu z vlastní vůle**. Přesněji: na základě samoregulačních mechanismů, které sledují „uznávaný veřejný zájem“.

Osobně si pod tím představuji třeba to, co naši mobilní operátoři dělají někdy od poloviny roku 2008 (viz tehdejší [kauza blokování](#), široce diskutovaná i zde na Lupě): **dodnes vlastně nevíme, co přesně blokují. Zda jen dětskou pornografii (a podle čeho ji hodnotí), nebo i další obsah, který hodnotí jako nelegální.**

I nynější lotyšské předsednictví, v rámci nadnesení tohoto problému, konstatuje že má významné právní aspekty. A vlastně i zde konstatuje, že to na nějaký konsensu s dohodu moc nevidí.

To když v [závěru svého návrhu](#) nové předsednictví konstatuje, že pokud by se tyto právní aspekty podařilo vyřešit, a členské země by podpořily zavedení samoregulačních mechanismů, pak by zvážilo zařazení příslušných textů do celého nového balíčku.

O čem je síťová neutralita?

Síťová neutralita byla původně ryze technickou záležitostí. Dnes se do ní zařazují i další, spíše již ne-technické aspekty, jako blokování či naopak upřednostňování některých služeb.

Dnes, v pondělí 18.5.2015, se v Praze koná další ročník [konference Law FIT 2015](#), o právu a IT. Letos má ve svém podtitulu otázku „Konec volného Internetu?“, která naznačuje i [zaměření](#) letošního ročníku: na problematiku síťové neutrality a volného a svobodného Internetu.

Sám mám na této konferenci jeden z příspěvků, právě na téma síťové neutrality – čeho se vlastně týká a co se v ní řeší. Jeho záměrem je představit co nejsrozumitelnější formou techničtější aspekty síťové neutrality lidem, kteří se věnují spíše netechnickým oborům. Tedy například právníkům.

Tento můj článek je vlastně jinou (časopiseckou) formou části mé prezentace, kterou si v původní podobě můžete prohlédnout [v mém archivu](#), či na [Slideshare](#) nebo [Scribd](#).

Síťová neutralita není nový problém

Problematika síťové neutrality rozhodně není nová. Její prvopočátky lze zasadit do pionýrských dob ještě před vznikem dnešního Internetu, kdy se teprve rodila koncepce protokolů TCP/IP – a jejich autoři jim vtiskly určité „neutrální chování“. K jeho podstatě se záhy dostaneme podrobněji, ale v prvním přiblížení jej lze popsat tak, že **protokoly TCP/IP (a zejména protokol IP) nedělají rozdíly mezi přenášenými daty a se všemi nakládají stejně.**

Dříve to nevadilo, a naopak to přinášelo velkou **výhodu v tom, že přenosové sítě mohly být jednodušší a levnější**. Díky tomu se také Internet snáze a rychleji rozrostl do své dnešní podoby a velikosti.

Jenže **dnes, kdy po Internetu chceme třeba telefonovat, sledovat živé video či přehrávat si všelijaké audio a videoklipy, je situace jiná**. Dnes může být takovéto neutrální chování naopak na závalu a způsobovat dobře známé problémy typu zadržávání videa, zkreslení zvuku až do nesrozumitelnosti atd.

Je proto zajímavou a důležitou otázkou, zda a **jak mohou, či přímo mají provozovatelé modifikovat neutrální chování svých sítí (těch „internetových“, na bázi protokolů TCP/IP), tak aby k problémům výše naznačeného charakteru nedocházelo vůbec, či docházelo co možná nejméně často**.

Vše je ale komplikováno tím, že provozovatelé sítí musí dbát i na řadu dalších „provozních“ aspektů, včetně dostupnosti pro všechny uživatele, spolehlivosti, kvality atd. Nehledě již na stále aktuálnější otázky bezpečnosti.

Sečteno a podtrženo: **dnešní „internetové“ sítě a s nimi související služby jsou složitým technickým systémem. „Vyladit“ jej tak, aby po technické stránce fungoval optimálně, je velmi netriviální záležitostí**.

Často je těžké zajistit už jenom to, aby celý systém vůbec fungoval a jeho služby byly dostupné. Nedávno se o tom přesvědčili i v Bruselu, když počátkem května Evropská komise [představovala svou novou strategii](#) jednotného digitálního trhu. Jak to dopadlo hned na začátku prezentace, vidíte na následujícím obrázku.



Rozšíření záběru

Zpět ale k samotné síťové neutralitě: jako technický problém je už letitá. **Nová je naopak míra pozornosti, která je síťové neutralitě věnována.** A to i mimo komunitu lidí, kteří se zabývají právě technickými aspekty fungováním počítačových sítí obecně, a Internetu konkrétně.

Důvodem pro takovéto „zvýšení pozornosti“ je i skutečnost, že dnes již nejde zdaleka jen o „vyladění“ celého složitého systému po technické stránce. To je stále velmi důležité, ale snad ještě větší důležitosti začínají nabývat i další cíle a motivace.

Jednou z nich je **snaha „vyladit“ celý složitý systém tak, aby svému provozovateli prospíval co nejvíce i po komerční stránce. Tedy aby mu přinášel co nejvyšší výnosy, resp. zisky.** V době, kdy Internet již není výhradně akademický, ale funguje na komerční bázi, to musíme respektovat. Ale současně je na místě požadovat, aby to nebylo na úkor technického „vyladění“. Ani dostupnosti, pestrosti nabídky, cenové hladiny atd.

Jenže ani to není zdaleka všechno: do „vyladění“ celého systému se snaží čím dál tím více zasahovat i nejrůznější **další zájmy – od zájmů těch, kteří jsou držiteli určitých práv (např. práv duševního vlastnictví),** a chtějí si vynutit jejich dodržování specifickými úpravami v celém složitém systému a jeho fungování, až po specifické zájmy státu či jeho jednotlivých orgánů, které chtějí

mít čím dál tím detailnější přehled o čím dál tím více věcech. Či je chtějí různě ovlivňovat, řídit, či naopak zakazovat atd.

V neposlední řadě je nutné si uvědomit i to, že dnešní Internet je i jakýmsi kolbištěm, kde se ve vzájemném konkurenčním boji střetávají různé komerční subjekty: některé si konkurují přímo, a jiné spíše nepřímo. Všichni společně ale bojují o to, kdo si pro sebe ukousne největší část z pomyslného koláče výnosů, který je do značné míry společný a omezený.

Takto třeba **bojují mezi sebou (o výnosy) na jedné straně tradiční telekomunikační operátoři a internetoví poskytovatelé, zajišťující fungování sítí, a na straně druhé subjekty, které po těchto sítích poskytují své služby**. Dnes se o nich mluví jako o „online platformách“ – a jak jsem zde na Lupě popisoval v [minulém článku](#), Evropská komise z nich má pořádný strach (z toho, že mají evropskou digitální ekonomiku „v hrsti“ – a až na jedinou výjimku nejsou z Evropy).

Zpět ale k meritu věci: jestliže „vyladění“ celého složitého systému po technické stránce je netriviální a dlouhodobě se moc nedaří, pak jeho „vyladění“ i po výše naznačených dalších stránkách je ještě řádově složitějším úkolem. Skoro si troufnu konstatovat, že je to neřešitelným problémem.

Sít'ová neutralita jako nové klíčové slovo

S rozšířením „záběru“ sít'ové neutrality souvisí i to, že se z ní stalo nové klíčové slovo („buzzword“), kterým se stále častěji ohání i lidé z jiných oborů. Současně se změnil (rozšířil) i okruh konkrétních otázek a problémů, které jsou zařazovány do sít'ové neutrality a v rámci ní diskutovány – a které v pionýrských dobách vzniku Internetu ještě vůbec nebyly „na stole“. Jde zejména o:

- **snahy zasahovat do toho, jaké protokoly, služby či aplikace smí uživatelé využívat, případně jaká koncová zařízení mohou připojovat a používat.** Může jít např. o služby poskytované způsobem OTT (Over The Top), jako např. VOIP či IPTV, které mohou konkurovat „nativním“ službám konkrétních operátorů a providerů. Či o snahy zpomalovat (či úplně zablokovat) některé služby – například na bázi P2P – ještě před vyčerpáním objemových limitů v rámci FUP

příklad: omezování rychlosti

Služba	Typ služby	Max. rychlost	Reálná rychlost
Web browsing, e-mail	Web browsing, e-mail	100 Mbps	100 Mbps
FTP, video streaming (YouTube, stream.cz, VoIP)	FTP, video streaming (YouTube, stream.cz, VoIP)	100 Mbps	100 Mbps

Služba	Typ služby	Max. rychlost	Reálná rychlost
Web browsing, e-mail	Web browsing, e-mail	100 Mbps	100 Mbps
FTP, video streaming (YouTube, stream.cz, VoIP)	FTP, video streaming (YouTube, stream.cz, VoIP)	100 Mbps	100 Mbps

- Telefonica / O2 CR
- dříve:
 - docházelo k selektivnímu omezování rychlostí některých služeb (až na 0) ještě před dosažením objemového limitu FUP
- dnes:
 - do vyčerpání limitu FUP k selektivnímu zpomalování již nedochází

14

- snahy ovlivnit dostupnost nejrůznějším míst či objektů – například v podobě snah o blokování celých serverů, jednotlivých stránek, konkrétních souborů, streamů, či jen výsledků vyhledávání atd. Ať již na geografickém principu (jako dnes tolik zmiňovaný geo-blocking), či na jiných základech (v zájmu boje proti dětské pornografii, proti nelegálnímu obsahu, za dodržování práv duševního vlastnictví, kvůli právu být zapomenut atd.)

geo-blocking

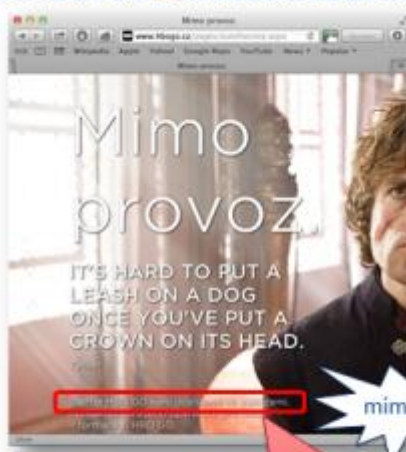


britský (BBC) iPlayer přehrává jen v UK (v ČR nikoli)

v ČR



mimo ČR



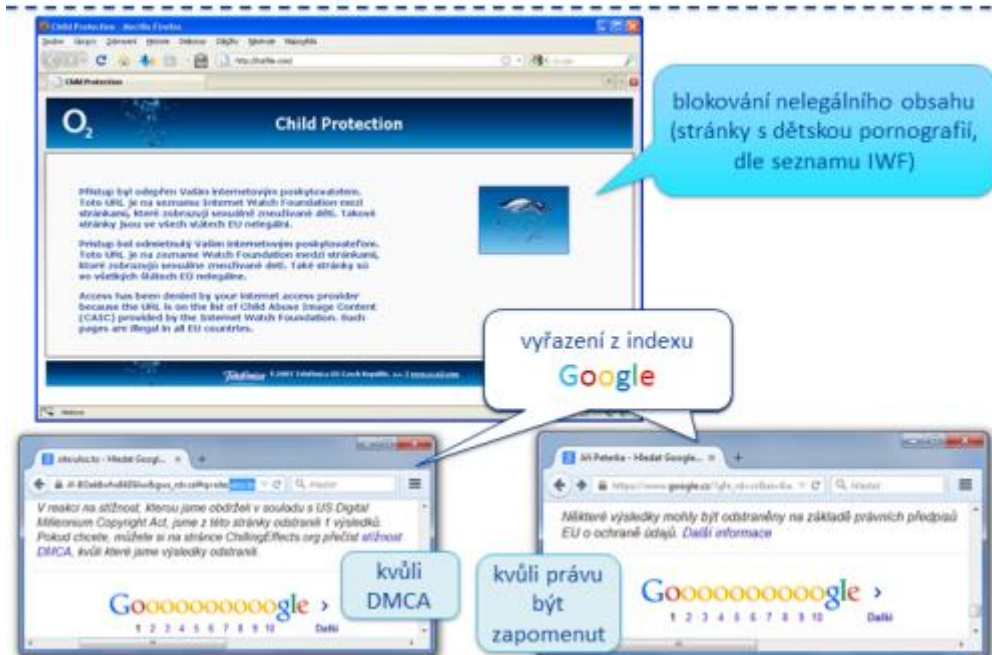
mimo ČR

Služba HBO GO není dostupná ve Vaší zemi

HORIZON GO Video není k dispozici
Omlouváme se, toto video není k dispozici mimo naši oblast z důvodu omezení autorských práv

18

jiné blokování



započítávání přenesených dat do různých kvót (nejčastěji v rámci FUP) - což vede k ovlivňování „poptávky“ ze strany uživatelů, a může být motivováno různými důvody: od potřeby předejít přetížení sítě, která nemá dostatečnou kapacitu, až po určité „směrování zájmu“ uživatelů na takový obsah, který je ze započítávání vyjmut (skrže tzv. zero rating).

příklad: zero rating

- česky: nezapočítávání (přenesených dat) do objemů FUP
- jiné stránky nejsou blokovány, ale jsou znevýhodněny tím, že „jejich data“ se započítávají do objemových limitů ve FUP

provider rozhoduje za svého zákazníka – vybírá a zvýhodňuje některé zdroje na úkor jiných



S tímto „rozšířením záběru“ pak souvisí i určitá **změna terminologie**, která ale ještě není zdaleka ustálená: místo o síťové neutralitě se začíná hovořit spíše o „volném Internetu“, „otevřeném Internetu“ či „svobodném Internetu“.

Je to patrné nejenom u [dnešní konference](#) (viz její podtitul: Konec volného Internetu?), ale třeba i na [jednáních o osudu tzv. Propojeného kontinentu](#): zde se v obecné rovině (například v tiskových zprávách, novinových článcích atd.) mluví o tom, že z celého záběru původního nařízení zůstal jen roaming a síťová neutralita. Ale [konkrétní diskutované texty](#) místo o síťové neutralitě hovoří o „otevřeném Internetu“ (Open Internet).

Má to asi i svou logiku: ony „nové“ aspekty jsou přeci jen srozumitelnější i lidem, kteří nejsou technicky zaměřeni. A hlavně: jde v nich o reálné peníze (výnosy, zisky), stejně jako o jiné reálné zájmy té či oné skupiny, či dokonce celých států.

Naopak technické aspekty, spojené s původním „užším“ významem síťové neutrality, se dostávají poněkud do pozadí. Nedostupná, nefungující, nebo jen špatně fungující síť či služba stále dokáže uživatele a zákazníka značně naštvat. Ale celý problém není černobílý ani úplně jednoduchý na vysvětlení a pochopení. A také neumožňuje tak snadno na někoho ukázat prstem a jednoduše říct, co dělá špatně a jak by to měl dělat jinak.

Jak funguje protokol IP?

Pojďme nyní již k tomu, co je síťovou neutralitou v původním smyslu (dnes asi: užším slova smyslu). Týká se to hlavně celkové koncepce protokolu IP (Internet Protocol) z rodiny protokolů TCP/IP, který je hlavním (a vlastně jediným) přenosovým protokolem. A ty jeho vlastnosti, které si budeme popisovat, se mezi jeho verzemi 4 a 6 (IPv4 a IPv6) neliší.

Snad nejpodstatnější vlastností protokolu IP, z pohledu síťové neutrality, je skutečnost, že se vůči všem přenášeným datům chová stejně. Všem měří stejným metrem a nezajímá se o to, co jsou přenášená data zač, od koho pochází a komu jsou určena. Takže nerozlišuje například to, zda právě přenáší nějakou část emailové zprávy, „kus“ živého videa, webovou stránku či cokoli jiného.

Tento neutrální přístup protokolu IP se pak odráží zejména v tom, že nikomu (žádnému druhu dat) nedává přednost, ani neposkytuje nějaké jiné (odlišné) zacházení. **Platí to i pro situaci, kdy mu „dojdou síly“ (hlavně ty kapacitní) a už nestíhá přenést všechna data tak, jak by měl. Přenášená data může na krátkou dobu pozdržet, v naději že za chvíli už bude mít volnější ruce.** Ale když ani to nepomůže, musí některá data zahazovat. Důležité je, že ani zde se na nic neptá a pozdržuje či úplně **zahazuje rovnoměrně. Všem stejně. Padni komu padni.**

Kromě toho **protokol IP vůbec negarantuje, že data přenesou správně.** Pokud totiž zjistí nějakou chybu v přenášených datech, jednoduše nepovažuje za svůj úkol postarat se o nápravu, poškozená data jednoduše zahodí a pokračuje dál. Analogicky pro ztracená data – vůbec po nich nepátrá, natož aby se snažil je nějak přenést znovu.

Důsledkem je pak to, **že protokol IP negarantuje, že data vůbec přenesou. Natož pak že je přenesou do nějaké konkrétní (maximální) doby.** Dobu, kterou bude přenos trvat (pokud vůbec bude úspěšný) nelze u protokolu IP jakkoli garantovat, a v praxi se skutečně může dosti významně měnit.

Komu to vadí a komu ne

Popsané vlastnosti protokolu IP způsobují, že když postupně přenáší jednotlivé části nějakého většího „datového celku“ (představujme si třeba přenos živého obrazu či zvuku), pak vůbec není

garantováno, jak pravidelně budou jednotlivé části dat doručovány. Pokud vůbec budou doručeny (a navíc správně, tj. bez chyb).

Takováto **nepravidelnost doručování moc nevadí klasickým „počítačovým“ službám**, jakými jsou přenosy souborů či elektronická pošta: ty totiž čekají, až přijmou všechna svá data, a teprve pak je zpracovávají. Ale u multimediálních služeb, zejména u živého přenosu zvuku a obrazu, je tomu jinak: zde jsou přenášená data „zpracovávána“ (přehrávána, zobrazována) průběžně, a proto jim na pravidelnosti hodně záleží.

Multimediální služby potřebují pravidelnost (doručování svých dat) proto, že lidské smysly jsou hodně citlivé na jakékoli nepravidelnosti: třeba u videa lidské oko nemusí zaregistrovat dílčí poškození jednoho okénka filmového pásu (pokud bychom použili terminologii klasického promítání obrazu), ale spolehlivě zaregistruje i velmi malé odchylky v rychlosti posunu filmového pásu. Natož pak úplné zastavení. Podobně u zvuku (audia).

Řečeno stručně a lapidárně: protokol IP se pro multimediální přenosy moc nehodí. A důsledky asi není třeba podrobněji rozvádět: všelijak „trhaná“ videa či nesrozumitelný zvuk jsme asi zažili všichni.

Proč se všichni tak tlačí do používání protokolu IP?

Je-li protokol IP tak „málo vhodný“ pro multimediální přenosy typu přenosu živého zvuku a obrazu, pak je jistě zajímavou otázkou, **proč se všechny služby a aplikace tak moc snaží, aby nad tímto protokolem mohly fungovat. Proč chceme telefonovat po Internetu/IP protokolu (skrže VOIP, neboli Voice over IP), či sledovat televizní vysílání, či jen různá videa na žádost?**

Odpověď naznačují slogany IP over Everything a Everything over IP: první z nich vypovídá o tom, **že protokol IP dnes funguje nad úplně každou technologií**, schopnou „alespoň nějak“ přenášet jednotlivé datové bity. Možná si to ani neuvědomujeme, ale právě díky tomu se dnes můžeme připojovat k Internetu mnoha různými způsoby, přičemž výsledný efekt by měl být v zásadě stejný (samozřejmě až na kvantitativní parametry, jako je rychlost, latence atd.).

Druhý slogan je pak konkrétním důsledkem prvního sloganu: když už IP funguje „nad vším“ (dokonce i [nad poštovními holubami](#), pozor ale na datum), pak snad každá služba chce umět fungovat nad protokolem IP – aby skrže něj i ona mohla být dostupná všude (fungovat „nad vším“). A to i tehdy, když pro ni protokol IP není vhodný.

Je řešením přístup hrubou silou?

Dnes jsme tedy v situaci, kdy je protokol IP stále intenzivněji využíván pro takové služby, se kterými původně nepočítal a není pro ně „stavěn“. Na místě je proto otázka, zda se s tím dá něco dělat – zda lze nějak ovlivnit jeho chování tak, aby byl pro multimediální služby vhodnější.

Takové možnosti samozřejmě existují, a dají se rozdělit do dvou skupin.

První z nich je možné označit jako „přístup hrubou silou“: na způsobu fungování protokolu se nic měnit nebude. Jen se dostatečně „nafouknou“ (předimenzují) kapacity, které má tento protokol k dispozici. Tedy hlavně přenosové kapacity (rychlosti přenosových cest atd.), ale třeba také kapacity směrovačů a dalších aktivních prvků v síti. Cílem je minimalizovat četnost případů, kdy protokolu IP „dojdou síly“ a musí nějaká data pozdržet či úplně zahodit.

Není to tedy skutečné řešení v tom smyslu, že by celý problém zcela eliminovalo – řeší jej pouze „statisticky“, tak aby k němu docházelo co nejméně často.

V praxi se ukazuje, že tento „přístup hrubou silou“ je relativně schůdný a jednoduchý. Zejména díky tomu, že nevyžaduje žádné zásahy do fungování protokolu IP. Na druhou stranu má své náklady - ale ceny přenosových (i dalších kapacit) postupně klesají. Jenže na druhé straně zase rostou požadavky uživatelů i nároky používaných služeb

Druhou možností (vedle „přístupu hrubou silou“) je nějak zasáhnout do způsobu fungování protokolu IP a změnit jeho neutrální přístup k přenášeným datům. Tedy nenechat ho, aby všem datům měřil stejně - ale umožnit mu, aby s různými daty zacházel různě. Aby jim nabízel různou „kvalitu svých služeb“. Proto se také v odborném žargonu hovoří o zavedení podpory QoS (od: Quality of Service).

Jak zasáhnout do neutrality protokolu IP?

Pro zavedení podpory QoS do protokolu IP je opět na výběr více možností. Různý přístup k různým datům může spočívat například v tom, že některá data dostanou přednost před jinými. Jinými slovy: zavedou se určité úrovně priority, a různá přenášená data se budou „hlásit“ k různým prioritám. Jenže: pokud se všechna data „přihlásí“ ke stejné úrovni priority, například k té nejvyšší, jsme zpět tam, kde jsme byli.

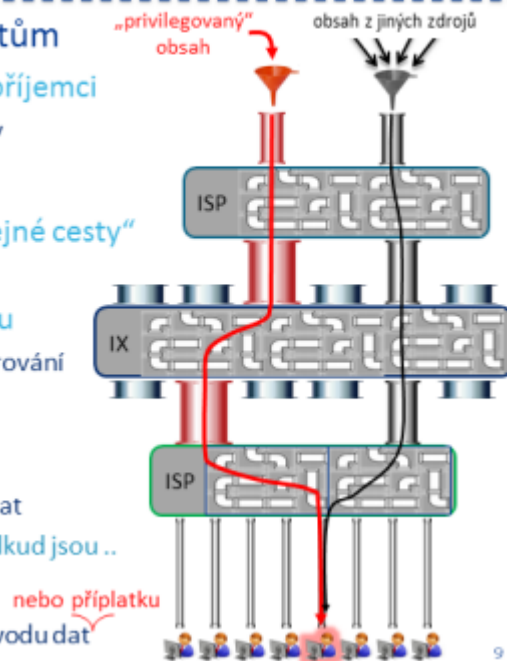
Další možností je umožnit, aby si protokol IP pro některá přenášená data vyhradil (v rámci jedné přenosové cesty) určitou kapacitu, a díky tomu jim mohl garantovat, že se na ně „vždy dostane“ – nejenom, že budou přeneseny, ale také že budou přeneseny včas (i pravidelně).

Obě právě naznačená řešení jsou v praxi možná, a existují i technické standardy, které říkají, jak by měla být realizována. Háček je v tom, že je to dosti komplikované, a hlavně: šance na nasazení (a fungování) podpory QoS je pouze v těch částech sítě, které má konkrétní vlastník (provider) ve své moci. Tedy jen v jeho síti. Šance na nasazení v celém (celoplanetárním) Internetu je prakticky nulová.

Existuje ale ještě jeden možný přístup: pro různá data vyhradit celé různé přenosové cesty. Tedy nechat jedna data „proudit“ skrze jednu přenosovou cestu, nejspíše s lepšími parametry (větší přenosovou kapacitou, menším přenosovým zpožděním atd.), a ostatní data nechat „protlačovat“ jinou přenosovou cestou, s horšími parametry.

jiné řešení (jak poskytnout „lepší zacházení“)

- „dát přednost“ určitým datům
 - na celé cestě od zdroje až k příjemci
 - nebo alespoň na části této cesty
- možnosti:
 - dát jim přednost v rámci „stejně cesty“
 - viz podpora QoS
 - najít pro ně jinou (lepší) cestu
 - skrze jiné než (standardní) směrování
- směrování dat v Internetu
 - standardně: je neutrální
 - není závislé na druhu/původu dat
 - neptá se, co jsou data zač, odkud jsou ..
 - možná alternativa:
 - směrování závislé na druhu/původu dat



Takovéto řešení je naopak poměrně snadno realizovatelné – ale jen „na začátku“ (u zdroje dat) a v páteřních částech sítě. Naopak u koncových uživatelů je více (samostatných) přenosových cest obvykle mimo ekonomickou i technickou realitu. Snad s výjimkou optických vláken „až k uživatelům“.

Porušení neutrality může být vhodné i nežádoucí

Právě naznačené porušení neutrality protokolu IP může být motivováno různými požadavky, a může sledovat různé cíle. Právě zde se přitom začínají různit názory na celou problematiku.

Z mého pohledu je možné „měřit různě“ podle druhu dat: dávat vyšší prioritu (nebo i garantovat podmínky) celým kategoriím multimediálních dat. Tedy třeba všem videím, a všem přenosům zvuku – bez ohledu na to, zda jde o video z YouTube, Stream.cz či odjinud. Či bez ohledu na to, zda jde o přenos telefonního hovoru třeba přes Skype, v rámci nějaké VOIP služby na bázi protokolu SIP apod.

Naopak nevhodné a nežádoucí by (z mého pohledu) bylo obdobné upřednostňování multimediálních dat nikoli na základě jejich charakteru (video, zvuk atd.), ale na základě jejich zdroje a cíle. Tedy třeba upřednostňování videa z YouTube před videem z jiných zdrojů.

Jenže ono to není zdaleka tak jednoduché: když už má být nějak porušeno striktně neutrální chování protokolu IP, pak nejde jen o to, co má být rozlišujícím kritériem: zda pouze druh dat, nebo i jejich původ/zdroj, případně další faktory. Jde třeba i o to, jak velká má být míra upřednostnění na straně jedné, a „znevýhodnění“ (ostatních dat) na straně druhé.

Opět je to o nějakém vhodném vyvážení – a zde je znovu důležité, jaké cíle toto vyvážení sleduje: zda jen technické a provozní, nebo i zájmy komerční, či dokonce nějaké další.

Pravidla řízení datového provozu a specializované služby

Hledání takového „vhodného vyvážení“ je skutečně pořádným oříškem. Jeho cílem přitom není nějak zakazovat providerům, aby si sami volili takovéto „vyvážení“ u služeb, které chtějí nabízet svým zákazníkům.

Jde spíše o „nastavení laťky“: o názor na to, jaká opatření porušující striktně neutrální chování protokolu IP jsou ještě žádoucí, vhodná či alespoň únosná pro fungování sítě a celkovou kvalitu poskytovaných služeb, a jaká opatření již jdou „nad“ tuto laťku.

Ale je to také o důsledcích této „laťky“: jak má být zákazník informován o tom, co je ještě služba přístupu k Internetu (která je stále „dostatečně neutrální“), a co již jsou „jiné“ služby (tzv. specializované služby, či služby „přístupu k síti internet s omezením“, jak je [označuje ČTÚ](#)). Či zda ony „jiné služby“ musí splňovat ještě nějaké další podmínky.

Například dnešní torzo tzv. Propojeného kontinentu, které původně trvalo na dosti striktním dodržování síťové neutrality, [nyní počítá](#) s možností poskytování specializovaných služeb. A pouze požaduje, aby to „nebylo na úkor“ služeb poskytování přístupu k Internetu.

Původní řešení L2

L1 Fyzická vrstva datových sítí

Optické trasy

L2 Linková vrstva datových sítí

Původní řešení L2

MetroEthernet – WAN Ethernet

L2,5 MPLS
