Body of European Regulators for Electronic Communications

BEREC

BoR (22) 72

Metodika BEREC k vyhodnocování nařízení o síťové neutralitě

14. června 2022

Obsah

1. Manažerské shrnutí

Tento dokument obsahuje metodiku BEREC pro regulatorní vyhodnocování, jejímž cílem je poskytnout vnitrostátním regulačním orgánům vodítka pro monitorování a dohled nad ustanoveními o neutralitě sítí obsaženými v nařízení o otevřeném internetu č. 2015/2120 [1] (dále jen „nařízení“) a případným volitelným zaváděním nástrojů pro měření síťové neutrality. Tato metodika má rovněž přispět k harmonizaci metod měření síťové neutrality. Tato aktualizovaná práce navazuje na předchozí pokyny BEREC k síťové neutralitě, monitorování kvality služeb přístupu k internetu (IAS) a osvědčených postupech.

Kapitola 3 obsahuje pokyny k harmonizované metodě měření kvality služeb. Jejím cílem je maximalizovat přesnost a konzistentnost měření a umožnit srovnání výsledků měření mezi různými členskými státy. Metoda měření rychlosti je standardně založena na vícenásobných spojeních transportní vrstvy a dokument popisuje následný výpočet měřené rychlosti. Tento dokument rovněž definuje přístupy k měření zpoždění, kolísání zpoždění a ztrátovosti paketů.

Kapitola 4 uvádí doporučení metod pro odhalování postupů řízení provozu, které mají dopad na jednotlivé aplikace, a obsahuje doporučení pro zjišťování postupů řízení provozu, které mají dopad na konektivitu a v konečném důsledku na možnost používat a poskytovat jednotlivé aplikace.

Kapitola 5 popisuje nejdůležitější faktory, které je třeba vzít v úvahu při vyhodnocování výsledků měření, a poskytuje pokyny pro shromažďování informací. Výsledky tak může ovlivnit řada faktorů v prostředí koncového uživatele. Mezi tyto faktory patří například využití Wi-Fi, výkon modemu a počítače a rádiové podmínky při měření rychlosti u mobilního přístupu.

Kapitola 6 poskytuje doporučení pro validaci, následné zpracování a analýzu shromážděných výsledků měření na úrovni trhu. Je zde probíráno téma agregace údajů pro účely vyhodnocování na úrovni trhu a jsou uvedeny pokyny pro monitorování obecné kvality služby přístupu k internetu (služby přístupu k internetu jako celek a dopadu specializovaných služeb na službu přístupu k internetu obecně) i jednotlivých aplikací využívajících služby přístupu k internetu.

Kapitola 7 uvádí další pokyny k tomu, jak by měly být výsledky měření rychlosti posuzovány ve srovnání se smluvními hodnotami rychlosti pro koncové uživatele.

A konečně, kapitola 8 uvádí pokyny ke kritériím, která by vnitrostátní regulační orgány mohly zohlednit při zajišťování vlastního certifikovaného monitorovacího mechanismu nebo při certifikaci mechanismů zajišťovaných třetími osobami, zatímco kapitola 9 hovoří o požadavcích na ochranu dat.

2. Úvod

BEREC vypracoval a následně aktualizoval tuto metodiku k vyhodnocování nařízení, která má vnitrostátním regulačním orgánům pomoci při monitorování a dohledu nad ustanoveními nařízení [1] o neutralitě sítí na základě různých nástrojů měření síťové neutrality a harmonizované metodiky měření ukazatelů kvality služeb.

Dále se předpokládá, že tato metodika měření síťové neutrality BEREC by mohla přispět k práci standardizačních organizací. Tato metodika navazuje na předchozí pokyny BEREC k síťové neutralitě, monitorování kvality služeb přístupu k internetu (IAS) a osvědčených postupech [2].

Podle nařízení mohou mít vnitrostátní regulační orgány při měření služeb přístupu k internetu několik cílů:

- měřící nástroje mohou jednotliví koncoví uživatelé používat k ověření, zda jsou plněny závazky, které jim poskytovatel služby přístupu k internetu poskytl (čl. 4 odst. 1 nařízení);
- měřicí nástroje lze použít ke zjištění postupů řízení provozu, které mohou být, či nejsou povoleny (čl. 3 odst. 3 nařízení);
- k určení "obecné kvality služby přístupu k internetu" lze použít měřicí nástroje. To je důležité pro posouzení, zda mohou být poskytovány jiné služby než služby přístupu k internetu (ve smyslu čl. 3 odst. 5 nařízení);
- měřící nástroje mohou být součástí monitorovacího mechanismu certifikovaného vnitrostátním regulačním orgánem, jak je uvedeno v čl. 4 odst. 4 nařízení.

Vnitrostátní regulační orgány mohou chtít dosáhnout dalších cílů při měření nebo zjišťování určitých praktik souvisejících se službou přístupu k internetu. BEREC poznamenává, že je na vnitrostátních regulačních orgánech, aby určily nejvhodnější měřicí nástroje, které budou sloužit jejich cílům. Různé cíle mohou určit použití různých měřicích nástrojů.

V tomto dokumentu BEREC popisuje metodiku měření rychlosti služby přístupu k internetu, aby vnitrostátní regulační orgány mohly posoudit výkon služby přístupu k internetu ve srovnání se smluvními hodnotami minimální, běžně dostupné a maximální rychlosti. Metodika rovněž poskytuje pokyny k některým kritériím, která by vnitrostátní regulační orgány mohly zohlednit při poskytování vlastních měřicích nástrojů jako ověřeného mechanismu nebo při certifikaci mechanismů zajišťovaných třetími osobami v souladu s nařízením a Pokyny BEREC k otevřenému internetu [3].

Cílem tohoto dokumentu je popsat metodiku měření, kterou by bylo možné kombinovat s crowdsourcingovým přístupem, aby bylo možné poskytovat měřicí nástroje většímu počtu koncových uživatelů. U crowdsourcingových měřicích nástrojů v prohlížeči nebo v aplikaci je obtížné nebo dokonce nemožné mít plnou kontrolu nad všemi faktory, které ovlivňují výsledky měření, jako třeba prostředí koncového uživatele. Tím vzniká možnost chyby ve výsledcích měření, které se nelze zcela vyhnout. Tato metodika poskytuje pokyny, jak zvýšit přesnost a spolehlivost výsledků těchto měření. Tím se zabývá kapitola 5.

BEREC uznává standardizované měřící přístupy od ETSI, ITU a IETF, avšak největší důraz klade na praktickou implementaci metodiky měření v crowdsourcingovém scénáři, kdy měření může provádět kterýkoli koncový uživatel a měřená metrika co nejvěrněji odráží reálné zkušenosti koncových

uživatelů s používáním internetu. Podrobněji o tom pojednává podkapitola 3.1.6.

Jak je navrženo v Pokynech BEREC k síťové neutralitě a monitorování kvality služeb přístupu k internetu z roku 2012 [2], metody měření musí zahrnovat jak službu přístupu k internetu jako celek, tak jednotlivé aplikace poskytované prostřednictvím služby přístupu k internetu. Metodika podporuje IPv4 i IPv6 – toto téma je dále diskutováno v relevantních případech.

Aktualizace v tomto dokumentu jsou považovány za obecně kompatibilní s předchozí verzí [8], a proto BEREC nepředpokládá, že by vedla k nutnosti provést významné změny již existujících systémů měření. To je však třeba zvážit případ od případu.

3. Měření kvality služby přístupu k internetu

Cílem této kapitoly je popsat doporučenou metodiku měření kvality služby přístupu k internetu, která vychází z kombinovaného cíle dosažení maximalizace přesnosti měření vyvážené potřebou umožnit veřejnosti snadný přístup k měřicímu nástroji a zajistit, aby výsledky měření byly srovnatelné mezi jednotlivými členskými státy. Doporučená metodika zahrnuje komplexní řadu témat. Všechna jsou široce a obecně diskutována. Je pak na vnitrostátních regulačních orgánech, aby tyto pojmy interpretovaly na základě své konkrétní situace a případně je odpovídajícím způsobem upravily.

Výsledky těchto měření lze využít také k následujícím účelům:

- aby si koncový uživatel mohl ověřit závazky, které mu poskytl jeho poskytovatel služby přístupu k internetu;
- pro monitorování obecné kvality služby přístupu k internetu, aby bylo možné potvrdit, že se výkon služby přístupu k internetu, s přihlédnutím k technologickému vývoji, vyvíjí dostatečně (viz kapitolu 6);
- vnitrostátní regulační orgány mohou údaje využít také ke zvýšení transparentnosti (např. interaktivní mapy zobrazující výkon v určité zeměpisné oblasti);
- aby bylo možné odhalit upřednostňování a/nebo omezování provozu vybraných aplikací ve srovnání s ostatními aplikacemi provozovanými přes službu přístupu k internetu (viz podkapitolu 4.2).

Podle bodu 166 Pokynů BEREC k implementaci nařízení o otevřeném internetu [3], by se „*[měření] neměla provádět pouze v rámci úseku zajišťovaného poskytovatelem internetových služeb*“ a rychlost by měla být počítána „*na základě uživatelských dat protokolu transportní vrstvy*“. Kromě toho se v bodě 140 uvádí, že „*[r]ychlosti by měly být uváděny na základě uživatelských dat protokolu transportní vrstvy, a nikoli na základě protokolu nižší vrstvy*“.

Zde popsaná metodika je zaměřena na měření kvality služby přístupu k internetu ve vzestupném (upload) i sestupném (download) směru. Je třeba poznamenat, že rychlost služby přístupu k internetu (podkapitola 3.1) je pouze jednou ze složek výkonu, který koncoví uživatelé pociťují, protože různé aplikace mají různé požadavky na zpoždění, kolísání zpoždění (podkapitola 3.2) a ztrátovost paketů (podkapitola 3.3) služby přístupu k internetu.

Pro úlohy měření zahrnující jak službu přístupu k internetu jako celek, tak jednotlivé aplikace využívající službu přístupu k internetu, je základním předpokladem, že měření se provádí na okraji sítě, která zajišťuje službu přístupu k internetu (tj. modem pro pevný přístup nebo prostřednictvím rádiového přístupu v případě mobilní služby přístupu k internetu). Je třeba také poznamenat, že u některých typů sítí je třeba přidělit zdroje dříve, než je k dispozici plná šířka pásma, a doba, po kterou dochází k přidělování zdrojů může být vnímána jako fáze snížené šířky pásma, a tedy snížené kvality. V některých starších sítích (např. v mobilních sítích 2,5G/3G) může taková fáze přidělování zdrojů trvat několik set milisekund, což má dopad na měřenou kvalitu. Takové přechodné chování může být zaznamenáno nebo může být vyřazeno v závislosti na účelu měření.

Pokud se měření provádí proti testovacímu serveru, měl by být tento server umístěn mimo síť služby

přístupu k internetu.[1] Mezi serverem a poskytovatelem služby přístupu k internetu by mělo být odpovídající připojení, aby se minimalizoval jakýkoli dopad na měření. Toho lze zpravidla dosáhnout umístěním měřicího serveru v národním internetovém propojovacím uzlu (IXP) nebo v jeho blízkosti. V závislosti na konkrétní vnitrostátní situaci mohou být měřicí servery umístěny na více než jednom místě IXP.[2] Mohou také existovat specifické důvody pro umístění měřicího serveru jinde, které by měly být posouzeny. V případě, že je k dispozici více umístění serveru, měl by nástroj vybrat, které z nich se použijí, na základě vhodných kritérií.

Hardware, na kterém běží měřicí server(y), by měl být připojen co nejblíže přepínači IXP, aby se minimalizovalo zpoždění (latence) způsobené komunikačními cestami. To znamená, že počet skoků mezi hlavním přepínačem IXP a testovacím serverem by měl být co nejmenší. To platí bez ohledu na to, zda implementace běží v síti poskytovatele hostingu, nebo přímo na hardwaru, který je pod kontrolou samotného vnitrostátního regulačního orgánu.

Vzhledem k tomu, že testovací provoz je internetovým provozem, doporučuje BEREC, aby vnitrostátní regulační orgány zajistily, že s provozem určeným k měření bude zacházeno stejně jako s ostatním provozem.

V případech, kdy server i klient vidí výsledky testů (např. měření rychlosti), se obecně za směrodatný zdroj výsledků měření považuje příjemce dat, ale doporučuje se, aby se pro účely analýzy ukládala měření klienta i serveru.

V mnoha případech je primárním výstupem měření (např. rychlosti stahování/odesílání dat (v bit/s), latence (v ms) nebo ztrátovosti paketů (v procentech)) ten výsledek, který je poskytován koncovému uživateli. Často je však vhodné, aby byla zaznamenána větší míra podrobnosti, než jaká se zobrazuje koncovému uživateli.

Monitorovací mechanismy na straně klienta by měly v co největší míře zmírnit (nebo alespoň identifikovat) matoucí faktory, které se vyskytují v prostředí koncového uživatele. Mezi tyto faktory patří například stávající křížový provoz a používání rozhraní Wi-Fi. Tomuto tématu se věnujeme samostatně v kapitole 5.

Monitorovací mechanismy na straně serveru by měly monitorovat dostupnou kapacitu měřicího serveru, jako je procesor (CPU), paměť, zdroje operačního systému atd., aby bylo možné odhalit překážky (místa s nedostatečnou kapacitou). Výsledky testů, které mohly být v důsledku těchto překážek zhoršeny, by měly tuto skutečnost odrážet.

Vyhodnocování výsledků měření se dále věnujeme v kapitolách 6 a 7. Certifikovaný monitorovací mechanismus je dále řešen v kapitole 8.

[1] To je v souladu s architekturou praktického systému měření, které BEREC popsal v předchozích publikacích [5].

[2] Zatímco obecná kvalita přístupu k internetu je nejlépe charakterizována tak, jak je popsáno, specifické koncové body internetu mohou mít odlišnou kvalitu, a tudíž odůvodňují další měření. Takovými koncovými body mohou být konkrétní sítě CDN nebo některé koncové body na okraji sítě (implementující široký koncept edge-computing, který je často zmiňován v souvislosti s 5G). Instalace komponent měřicího serveru na takové specifické koncové body může být obtížná, protože je obvykle pod kontrolou třetí osoby.

3.1. Měření rychlosti služby přístupu k internetu

3.1.1. Metoda měření rychlosti

BEREC založil tuto metodu měření na následujících požadavcích vnitrostátních regulačních orgánů na měření služby přístupu k internetu, zejména měření rychlosti, v regulačním kontextu:

- Multiplatformní – pokud je měření rychlosti iniciováno lidským koncovým uživatelem, musí být možné jej provést prostřednictvím zařízení, které obvykle používá pro přístup ke službě přístupu k internetu. Žádná umělá omezení v metodě by neměla bránit tomu, aby měření probíhalo na jiném hardwaru, jako jsou herní konzole/modemoví klienti/televizní přijímače atd.
- Koncoví uživatelé, kteří si měří rychlost služby přístupu k internetu, by měli být i nadále podporováni v rámci webového prohlížeče nebo v omezeném zkušebním prostoru (sandbox) aplikace v rámci zařízení; metoda nesmí vyžadovat ani zakazovat instalaci klientského softwaru pro osobní počítače.
- Výsledné měření rychlosti musí objektivně odrážet rychlost dostupnou koncovému uživateli, která může být ovlivněna faktory, jako je ztrátovost paketů nebo zpoždění (latence).
- Doba potřebná k provedení jednotlivého měření rychlosti by měla být dostatečně krátká, aby koncový uživatel nebyl z měření frustrovaný. Doba měření by měla zohledňovat také objem přenesených dat a měla by být pro koncového uživatele transparentní.
- Přestože se uznává, že každá implementace měření bude mít dolní/horní hranici rychlostí, při kterých se dosáhne přijatelné přesnosti, metoda by měla podporovat typické rychlosti dostupné na příslušných trzích. Metoda by měla být zejména připravena škálovat, aby podporovala rychlosti poskytované v optických sítích a sítích 5G.
- Metoda musí podporovat protokoly IPv4 i IPv6.

Ačkoli se tyto požadavky primárně zaměřují na měření rychlosti, v této kapitole jsou považovány za relevantní pro všechna měření služby přístupu k internetu.

Pro maximalizaci kompatibility v reálném prostředí se přesto doporučuje měřit rychlost odesílání/stahování dat na základě času potřebného k provedení paralelní sady řízených přenosů dat prostřednictvím protokolu HTTP(S). Tímto způsobem lze rychlost měřit na základě užitečného zatížení protokolu transportní vrstvy, jak je uvedeno v bodě 140 Pokynů BEREC k otevřenému internetu [3].

Tato metoda je podporována nejširší škálou příslušných platforem a splňuje výše uvedené požadavky. Proto je považována za vhodnou rovnováhu mezi konkurenčními požadavky na přesnost, nezávislost na platformě, snadnou implementaci a transparentnost. Tento postoj je také podpořen rozšířeným používáním protokolu HTTP(S) běžnými internetovými aplikacemi a službami, a proto odráží typické používání služby přístupu k internetu koncovými uživateli.

Pro vytížení měřené přenosové trasy se obecně doporučuje použít během testu rychlosti více spojení transportní vrstvy k jednomu serveru (nebo více serverům ve stejném fyzickém umístění). Počet připojení lze nastavit podle vlastností přenosové trasy (včetně odhadované rychlosti a zpoždění). Takový odhad může být založen na předběžném testu nebo na odhadovaném výkonu služby na základě jiných informací.

Test by měl být navržen tak, aby zátěž zpracování na straně odesílatele a příjemce byla nízká a umožňovala přesné měření vysokorychlostních připojení i na zařízeních s omezeným výpočetním výkonem.

V zájmu transparentnosti a uživatelské přívětivosti uznává BEREC výhody poskytování průběžných informací o zkoušce, například zobrazení grafu, který znázorňuje přibližnou hodnotu naměřené propustnosti během trvání testu. Test je proto specifikován tak, aby bylo možné zaznamenávat průběh přenosu dat na každé přípojce během testu v krátkých časových intervalech (např. 50-200 ms). Toho lze dosáhnout zaznamenáváním průběhu testu na každé přípojce v pevně stanovených časových intervalech nebo organizováním kontinuálního[3] přenosu bloků naměřených dat dané velikosti. V případě použití blokové implementace lze velikost bloku (a tedy i četnost příjmu bloku) nastavit na základě předběžného testu nebo na základě odhadovaného výkonu služby. Jedním z aspektů takového provedení je potřeba kontrolovat zdroje potřebné v koncových bodech ke zpracování přijatých dat.

BEREC uznává, že ztrátovost paketů a následné opakované přenosy paketů mají negativní dopad na propustnost spolehlivých protokolů transportní vrstvy, v tomto případě TCP (Transmission Control Protocol), a tím i na měřenou rychlost služby přístupu k internetu.

Doporučená metoda BEREC se řídí několika níže uvedenými koncepčními kroky. Tyto kroky mají být nezávislé na přesné verzi použitého protokolu HTTP(S) (v příslušných případech) a na tom, zda jsou připojení aktualizována na použití webových soketů, či nikoli.

Předběžný test

Předběžný test lze použít k předběžnému vyhodnocení vlastností služby přístupu k internetu, aby se zjistily některé parametry (např. počet připojení, velikost bloku) důležité pro následující hlavní test. Kromě toho, pokud je to možné, lze v této fázi zjišťovat informace o síťovém připojení (např. o mobilní technologii, rychlosti fyzického spojení atd.).[4]

K provedení předběžného testu lze použít různé metody, například provedení krátké kopie hlavního testu. Pro určení velikosti bloku lze použít příklad strategie spočívající v požadování bloků o násobcích pevné velikosti (např. 4096 bajtů), dokud přenos netrvá déle než předem definovanou dobu (např. 200 ms). Výsledné množství dat (4096 bajtů ^n) pak může být použito jako reference pro velikost bloku v hlavním testu.

Hlavní Test

Hlavní test začíná tím, že přijímající strana [5] oznámí, že je připravena zahájit měření. Vysílající strana pak začne odesílat data na každém spojení transportní vrstvy v postupných blocích bez zpoždění, případně s použitím parametrů určených během fáze předběžného testu. Pro následný výpočet rychlosti se zaznamenává doba přenosu a velikost každého bloku. Pro zmírnění účinků komprese by

[3] Kontinuální znamená, že data jsou odesílána bez (zamýšlených) přerušení jako nepřetržitý tok bajtů. To, že jsou interní data uspořádána do bloků, neznamená, že každý blok je požadován samostatně.

[4] V případě pevného přístupu k internetu lze ke shromažďování informací o prostředí koncového uživatele (Ethernet vs. Wi-Fi, RSSI, křížový provoz, inzerovaná rychlost, přístupová technologie atd.) použít rozhraní API. V této souvislosti francouzský regulační úřad Arcep specifikoval rozhraní „Access ID API“, které zavedli poskytovatelé internetových služeb ve Francii s cílem lépe charakterizovat prostředí koncových uživatelů a zvýšit spolehlivost testů měření kvality služby (QoS) na pevných linkách.

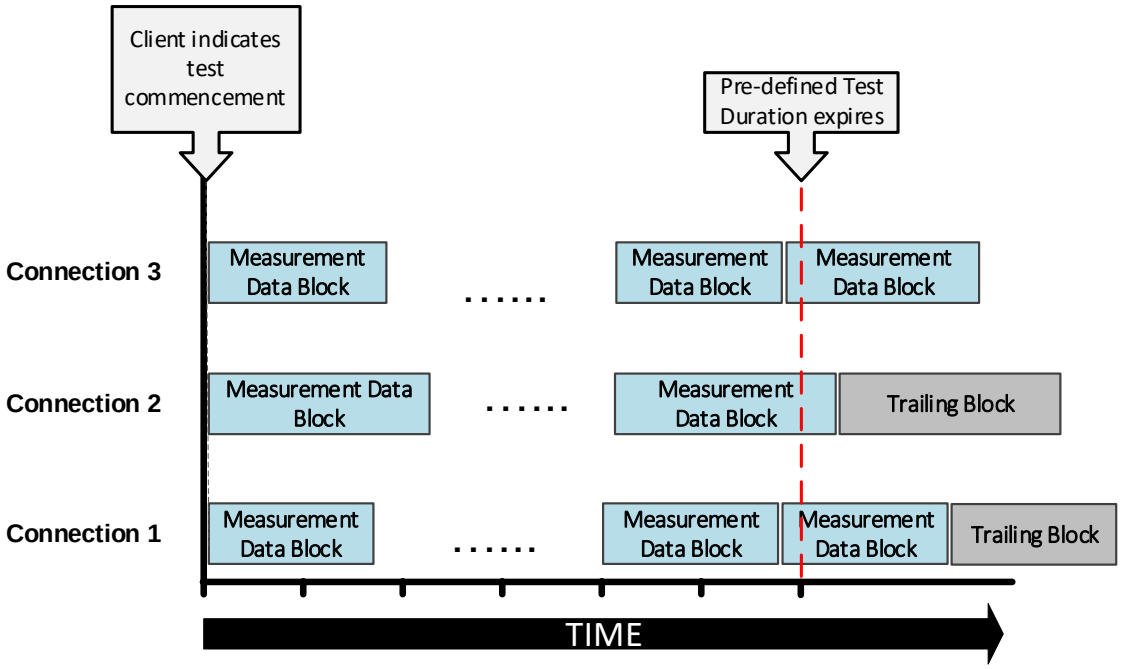
[5] U testů odesílání dat je příjemcem měřicí server, zatímco u testů stahování dat je příjemcem klient (koncový uživatel).

přenášená data měla být (pseudo)náhodná.[6]

Je třeba poznamenat, že, pokud je to možné, klient by měl provést pouze jeden požadavek na zahájení testu, aniž by musel provádět více požadavků na data, protože by to způsobilo zbytečné zpoždění a ovlivnilo měření rychlosti.

Tento přístup umožňuje přijímající straně analyzovat rychlost každého spojení po celou dobu trvání testu, a nikoli jako jedinou celkovou rychlost pro každé spojení, čímž poskytuje výše uvedený průběžný přehled.

Test se ukončí po uplynutí předem definovaného intervalu, nicméně u některých spojení může být nutné v přenosu „posledních bloků“ pokračovat (viz schéma níže), dokud všechna spojení nedokončí přenos měřicích bloků.



Obr. 1 - Koncepční pohled na test rychlosti

Obr. 1 výše má tento koncept ilustrovat v hrubém měřítku. Upozorňujeme, že po uplynutí doby trvání testu jsou „poslední bloky“ nadále odesílány přes spojení 1 a 2 až do dokončení posledního bloku dat z měření, které začalo před uplynutím doby trvání testu, v tomto případě na spojení 3.

Výpočet rychlosti

Výsledek měření bude obsahovat informace o objemu dat přijatých na každém spojení za daný časový interval, ze kterého se vypočítá rychlost.

Výslednou přenosovou rychlost vypočítá příjemce na základě dat přijatých ve všech spojeních v rámci

[6] Termín „pseudonáhodný“ znamená, že data by se měla typickému kompresnímu algoritmu jevit jako náhodná, přičemž jejich kryptografická kvalita zůstává irelevantní. Předem uložená „náhodná“ data tak mohou být znovu použita v rámci daného testu nebo pro následná měření, nebo data z testu downlinku (stahování dat) mohou být znovu použita pro test uplinku (odesílání dat).

všech měřicích bloků, včetně všech dat v záhlaví.[7] Je třeba poznamenat, že výpočet rychlosti přenosu dat na základě průměru vyhladí špičky, které se objevují při velmi nárazových přenosových rychlostech vyskytujících se v mobilních sítích.

Za účelem poskytnutí průběžných informací o testu uživateli, by se během měření ve směru upload mohla použít přibližná hodnota skutečné rychlosti naměřená odesílatelem. Alternativně by mohla být rychlost přenosu měřená serverem pravidelně sdělována klientovi.

Výpočet může zahrnovat celou dobu měření nebo může vyloučit jeden nebo více bloků měření (případně intervalů vzorkování) na začátku testu, aby se zabránilo započítání doby pomalého startu na transportní vrstvě a jakéhokoli jiného zpoždění způsobeného navazováním spojení.

Pokud se na jednom ze spojení objeví během testu chyba, může být efektivní doba testování zkrácena tak, aby skončila u posledního správně přijatého bloku na tomto spojení, chyba by měla být zaznamenána a zohledněna. V závislosti na čase chyby spojení může být celé měření vyřazeno.

Rychlost stahování i odesílání by měla být měřena stejným způsobem a uváděna v bitech za sekundu (např. kbit/s nebo Mbit/s). Všimněte si, že převodní koeficienty mezi mega a kilo musí být ze základu 10, nikoli ze základu 2 (tj. 1 Mbit/s = 1000 kbit/s, nikoli 1024 kbit/s).

3.1.2. Základní údaje o implementaci metody

Verze HTTP

Ačkoli volba verze protokolu HTTP je v zásadě volbou implementace metody, BEREC považuje za důležitá následující hlediska.

U testů založených na protokolu HTTP/1.1 se doporučuje, aby přenosy byly prováděny pomocí kódování přenosu po větších fragmentech (tzv. chunked transfer), které odesílající straně umožňuje odesílat části dat libovolné velikosti a přenos ve vhodnou chvíli zastavit. V tomto případě by každá část byla zastoupena jako blok měřených dat na Obr. 1.

Odesílatel by například mohl posílat bloky měřených dat v pevných částech o velikosti potenciálně určené v předběžném testu a zastavit je, jakmile uplyne celá doba trvání testu. Bez ohledu na zvolenou implementaci metody je důležité, aby každá část byla obsloužena okamžitě a bez jakéhokoli zpoždění, a je třeba zvážit, zda do výpočtu rychlosti zahrnout jakýkoli dodatečný objem dat přenesený v důsledku kódování typu Chunked Transfer Coding (nebo tzv. chunk extensions).

V případech, kdy výše uvedená implementace metody není možná, by měla být délka obsahu HTTP co největší, aby se minimalizoval počet po sobě jdoucích vzájemně navázaných požadavků potřebných k provedení testu.

Protokol HTTP/2 by ve výchozím nastavení multiplexoval všechny požadavky směrem ke stejnému serveru na jediném soketu TCP, a nepoužíval by tedy více spojení transportní vrstvy, jak je doporučeno výše. Aby se tomuto problému předešlo, lze případně použít více koncových bodů serveru ve stejném fyzickém umístění (nebo na stejném fyzickém hardwaru), avšak další relevantní

[7] Například hlavičky HTTP nebo režie rámců webových soketů. Ačkoli je to v zásadě relevantní, je třeba poznamenat, že hlavička HTTP jsou ve srovnání s objemem dat přenášených pomocí testu poměrně malá. Chyba způsobená nejistotou ohledně velikosti hlavičky (např. v důsledku komprese) tak může být zanedbatelná. Do výpočtu by v žádném případě neměly být zahrnuty hlavičky protokolů Ethernet nebo IP.

podrobnosti přesahují rámec tohoto dokumentu.

V době psaní těchto aktualizovaných Pokynů je protokol HTTP/3 stále poměrně nový a podrobnosti o jeho implementaci v populárních prohlížečích nejsou zcela známy. Ačkoli se má za to, že HTTP/3 a QUIC jsou slibné technologie, které v budoucnu pravděpodobně podpoří případ užití testování rychlosti podle BEREC, nemůže BEREC v tuto chvíli poskytnout konkrétní podrobnosti o jejich případné implementaci.

Počet spojení, parametry BDP a TCP

Testy by se obecně[8] měly provádět pomocí vícenásobného spojení transportní vrstvy (v praxi TCP), protože rychlost jednotlivého spojení je omezena výchozí maximální velikostí okna.

Na přenosových trasách s nízkým součinem šířky pásma a zpoždění (Bandwidth-Delay Product, BDP) může k zahlcení přenosové trasy stačit jediné spojení,[9] avšak dopad případné ztrátovosti paketů na snížení měřené rychlosti může být výraznější. Další informace jsou uvedeny v podkapitole 3.1.5.

V případech, jsou měřeny přenosové trasy s vysokou hodnotou BDP by měla být přijata opatření, která zajistí, že přenosová trasa může být stále zahlcena, aby byla zachována přesnost. Nejběžnějším přístupem je další zvýšení počtu spojení transportní vrstvy/TCP, ale je také možné upravit nastavení TCP pro server.

Implementace metody by měly zpracovávat typické hodnoty BDP v rozsahu měření.

Nepříznivý dopad ztrátovosti paketů z fyzikálních důvodů (např. bitové chyby způsobené rádiovým rušením v případě mobilních připojení nebo připojení Wi-Fi) na měření rychlosti závisí na algoritmu TCP Congestion Control použitém na klientovi a serveru.

Na základě známých parametrů TCP, které byly nakonfigurovány, v kombinaci s charakteristikami přenosové trasy zjištěnými během předběžného testu (pokud byl proveden) mohou implementace metody rozhodnout o vhodném počtu spojení, která se použijí v každém testu. Při zvyšování počtu spojení je však třeba vzít v úvahu omezení prohlížeče, protože je možné, že se nepodaří povolit dostatečný počet spojení, aby se přenosová trasa vytížila. Počet paralelních spojení podporovaných prohlížečem může také záviset na typu připojení a použitém rozhraní API prohlížeče.

WebSockets (RFC 6455)

V rámci protokolu HTTP(S) lze pro měření použít protokol WebSocket, který poskytuje duplexní spojení přes TCP s malou režií pro dostatečně velké datové rámce protokolu WebSocket. V tomto scénáři by každý blok měřených dat zobrazený na Obr. 1 odpovídal jednomu rámci WebSocket.

Při používání WebSockets by implementující strany měly vzít v úvahu výkonnostní rozdíly specifické mezi jednotlivými prohlížeči v konfiguraci protokolu a možnosti spojení, které mají prohlížeče k dispozici.[10] Při určování velikosti rámců WebSocket je třeba vzít v úvahu režii zdrojů způsobenou asynchronní povahou rozhraní WebSocket API, které mají prohlížeče k dispozici, a snažit se minimalizovat počet rámců na interval měření (tj. jeden rámec na blok měřených dat každých 50-200

[8] V některých případech může být vhodný test jednoho spojení, viz podkapitola 3.1.5

[9] Další informace o testech s jedním a více spojeními naleznete zde: https://en.arcep.fr/uploads/tx_gspublication/report-state-internet-2019-eng-270619.pdf#page=16

[10] Např. rozdíly ve výkonu v závislosti na „binaryType“ uvedeném v rozhraní API dostupném prohlížečům.

ms). Aby se minimalizovaly zdroje klienta, mohou být rámce WebSocket po přijetí okamžitě zahozeny.

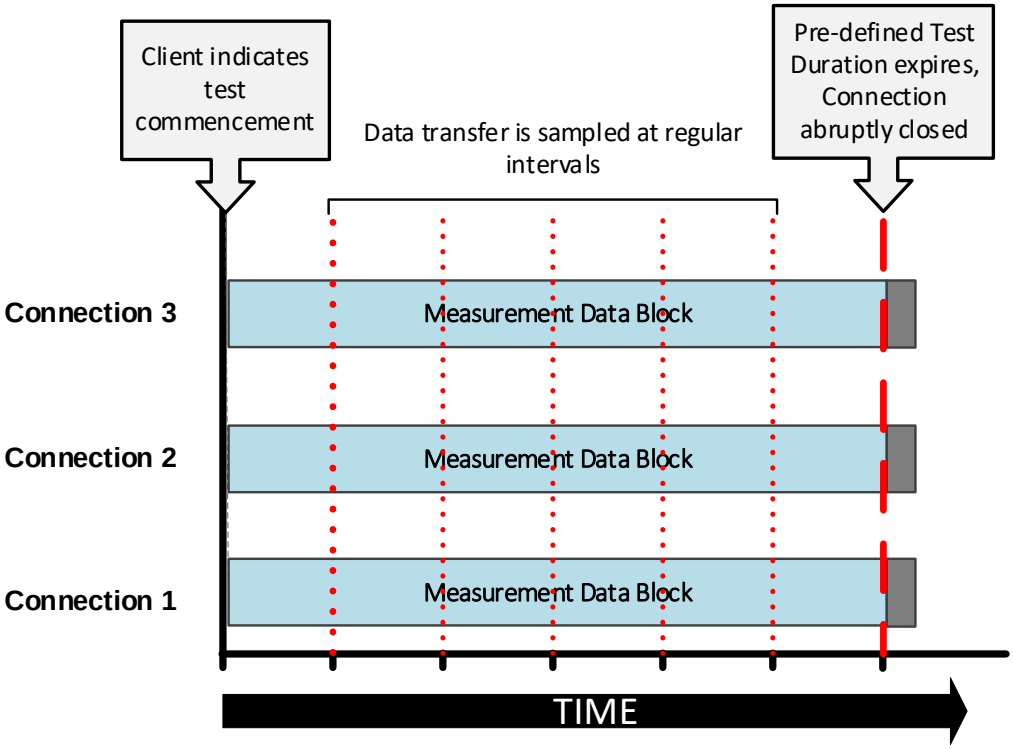
Je třeba poznamenat, že i při použití „socketů“ prostřednictvím WebAssembly tato připojení v praxi používají protokol WebSocket podle implementace prohlížeče.

Rozhraní API prohlížeče pro HTTP

Klienti v prohlížeči mohou zvolit rozhraní API, jako je XMLHTTPRequest nebo fetch API. V tomto případě by bylo možné nastavit dostatečně velkou velikost bloků měřených dat (a tedy i bloků HTTP) tak, aby přesáhly dobu trvání testu a odstranily riziko zpoždění mezi bloky měření. V tomto scénáři by bylo nutné:

a) využít událostí „průběh“ při použití XMLHTTPRequest nebo využít rozhraní Stream API při použití rozhraní fetch API k poskytování údajů o průběžném postupu stahování (viz Obr. 2), a

b) ukončit spojení a ukončit test po uplynutí předem definované doby trvání testu.



Obr. 2 – Vzorkování průběhu testu prostřednictvím rozhraní API v prohlížeči

Při implementaci je třeba dbát na to, aby kombinace hardware/OS/prohlížeče byla schopna v pravidelných intervalech přesně informovat o průběhu, aby u zařízení s omezenými zdroji nedocházelo k vyčerpání paměti a aby uzavření spojení nevedlo k nepředvídaným problémům.

Zabezpečení transportní vrstvy (TLS)

Vzhledem k tomu, že webové stránky na internetu stále častěji používají protokol TLS (ve formě protokolu HTTPS), doporučuje se jeho použití při testech rychlosti s výjimkou specifických případů, kdy jej klientský hardware nemůže udržet bez dopadu na výkon.

TLS poskytuje další výhodu v tom, že zabraňuje jakékoli manipulaci ze strany zprostředkujících proxy serverů[11] a nezpůsobuje žádný významný rozdíl ve výkonu nebo výpočetním zatížení zařízení koncového uživatele, protože šifrování je často podporováno hardwarem.

Pokud se šifrování nepoužívá, měly by se používat jedinečné adresy URL nebo příslušné hlavičky HTTP, aby se zabránilo ukládání do mezipaměti.

Dalším důvodem, proč doporučujeme používat protokol HTTPS na standardních portech jako užitečné zatížení TCP, je snaha zmírnit případná omezení spojení (například způsobená zprostředkujícími firewally nebo proxy servery v podnikovém prostředí), která by mohla vyplynout z volby méně často používaného protokolu/portu.

3.1.3. Různé informace

Měření musí být možné provádět jak přes IPv4, tak přes IPv6, přičemž verze použitá pro dané měření by měla být zaznamenána. Pokud má uživatel k dispozici obě verze protokolu, mohl by mít možnost si mezi nimi vybrat.

3.1.4. Srovnávání přesnosti a stability měření rychlosti a zpoždění internetu

Při srovnávání přesnosti měřicího systému se doporučuje provést srovnávací měření v několika skutečných internetových připojeních a v kontrolovaných (laboratorních) podmínkách, aby se zjistila přesnost a stabilita daného systému.

Tyto kontrolované laboratorní podmínky umožňují precizní kontrolu přesnosti měření rychlosti a zpoždění, zatímco testy prováděné na skutečném internetovém připojení mohou odhalit problémy, které se v laboratorním prostředí nevyskytují.

Jedním z možných principů srovnávání přesnosti měření rychlosti a zpoždění měřicího systému je nastavení/generování definovaných hodnot šířky pásma a zpoždění a provádění opakovaných testů s měřicím systémem na základě těchto nastavení.

Dalším způsobem srovnávání je použití „referenčního“ měřicího systému a porovnání naměřených výsledků testovaného měřicího systému s výsledky „referenčního“ měřicího systému.

K nastavení hodnot šířky pásma a zpoždění (obousměrného) pro takové testy lze použít několik nástrojů. Takovými nástroji jsou softwarově založené síťové emulátory šířky pásma (např. linuxový NetEm), možné funkce shaperů ethernetových routerů a profesionální či kalibrované přístroje.

Při kontrole přesnosti měření rychlosti se doporučuje definovat nastavení BDP, protože přesnost měření rychlosti může být do značné míry ovlivněna nejen šířkou pásma připojení, ale také zpožděním připojení (závislost na Bandwidth-Delay Product).

Rozsah šířky pásma použitý pro zkoušky přesnosti verifikace rychlosti by měl pokrývat specifikovaný rozsah šířky pásma měřicího systému. Pro testy je třeba zvolit typické hodnoty zpoždění. V rámci konkrétního rozsahu rychlosti a zpoždění by mělo být specifikováno více testovacích kroků (dvojic šířka pásma-zpoždění). Testy by se měly opakovat minimálně pětkrát pro každý pár BDP. Pokud

[11] Ačkoli jsou pro služby přístupu k internetu proxy servery zakázány nařízením o otevřeném internetu, mohou být stále používány v kancelářském prostředí, kde koncoví uživatelé mohou chtít provádět měření rychlosti pro informační účely. V této situaci by spuštění testu přes TLS na portu 443 zmírnilo případné rušení ze strany proxy serveru.

výsledek není dostatečně stabilní, je třeba provést více opakování.

Doba pauzy mezi jednotlivými opakováními by měla být zvolena tak, aby nezpůsobila nestabilitu měření, k čemuž by mohlo dojít, pokud by vyrovnávací paměť shaperu byla na začátku každého testu v nekonzistentním stavu.

Během měření je třeba zabránit křížovému provozu a doporučuje se sledovat využití procesoru a paměti zařízení použitých pro měření. Pro účely měření by měl být použit klientský počítač s typickým výkonem. Testy by se měly provádět a opakovat na více kombinacích operačních systémů a prohlížečů.

Hodnota šířky pásma měřená měřicím systémem a referenční hodnota (nebo konvenční hodnota) šířky pásma kanálu by měly být specifikovány na stejné vrstvě OSI. V případě, že to není možné a hodnota limitu šířky pásma je stanovena na nižší vrstvě OSI, je třeba poznamenat, že tento výpočet není vždy zcela přesný (například v důsledku možností hlavičky TCP povolených / zakázaných protokolem TCP během testu), což lze považovat za další faktor nejistoty nastavení měření.

3.1.5. Měření QoS pro jedno připojení vs. pro více připojení

Ačkoli se standardně doporučuje použít pro test rychlosti služby přístupu k internetu více připojení, v některých případech může být vhodný test jednoho připojení. Například rychlost jednoho připojení, která je podstatně nižší než rychlost více připojení, by mohla potenciálně odhalit problém, který stojí za prozkoumání, například pokud by prostředí poskytovatele služeb přístupu k internetu nebo koncového uživatele omezovalo rychlost jednoho připojení.

Nezřídka se stává, že testy s více připojeními vykazují rychlejší připojení než testy s jedním připojením, což může mít několik důvodů popsaných v podkapitole 3.1.2. Dalšími možnými důvody mohou být:

- pořadí příjmu paketů: připojení, u něhož například vysoký jitter nebo chybná konfigurace agregace přenosových tras znemožňuje zaručit, že pakety dorazí ve správném pořadí, výrazně sníží rychlost připojení;
- vytížení jádra procesoru v terminálu: test kvality služby s jedním připojením nemusí plně využít všechna jádra procesoru, na rozdíl od testů s více připojeními.

3.1.6. Metody měření stanovené jinými organizacemi

BEREC upozorňuje, že i jiné organizace zveřejnily metody měření propustnosti, které se od zde uvedené metody liší. ITU a Broadband Forum vydaly normy vystavěné na metodách měření kapacity IP založené na protokolu UDP.

Kromě toho, IETF zveřejnila dokument s názvem RFC 9097 *Metrics and Methods for One-way IP Capacity* na Standards Track. Současné prohlížeče však neumožňují přístup k nezpracovaným UDP socketům ani prostřednictvím rozhraní API prohlížeče, ani prostřednictvím sad nástrojů, jako je WebAssembly. Využití metody měření, která vyžaduje přístup k nezpracovaným soketům UDP, proto není podporováno v zařízeních koncových uživatelů, která budou používána k měření, a není vhodné pro splnění požadavků vnitrostátních regulačních orgánů popsaných v podkapitole 3.1.1.

3.2. Měření obousměrného zpoždění (ping) a kolísání obousměrného zpoždění

Pro měření obousměrného zpoždění lze v zásadě použít jakýkoli druh krátkého paketu IP (např. ICMP, UDP nebo TCP). Je však třeba vzít v úvahu následující skutečnosti:

- použití paketů ICMP mohou bránit omezení operačního systému. Dále mohou být zejména pakety ICMP blokovány firewally a antivirovým softwarem, a proto se nelze spolehnout, že budou dostupné pro měřicí nástroje;
- pakety TCP (po navázání spojení) podléhají řízení toku. K měření zpoždění by se dalo použít načasování třícestného handshake při navazování TCP spojení, které však TCP stack běžně neměří a nezpřístupňuje aplikacím;
- v prostředí webového prohlížeče je obtížné nebo dokonce nemožné odesílat/přijímat libovolné pakety UDP, které by mohly být použity pro účely měření obousměrného zpoždění.

Doporučuje se, aby se zpoždění měřilo odesláním a přijetím:

- paketů ICMP zprávy echo/reply, pokud je to možné, nebo
- krátkých UDP paketů, nebo
- krátkých TCP paketů, nebo
- rámců WebSocket ping/pong odeslaných serverem, na které klient okamžitě odpovídá (tyto pakety/rámce by měly obsahovat minimum dat, které odesílající straně umožní korelovat páry požadavek/odpověď). V případě, že nelze použít rámce PING/PONG, lze použít datové rámce WebSocket, nebo
- požadavky HTTP s odpovědí bez obsahu, např. pomocí metody HEAD nebo OPTIONS.

Je třeba poznamenat, že první měření při výpočtu zpoždění může být vysoké, a tudíž nereprezentativní v případě, že zjišťování trasy nebo sestavování spojení (např. vyhledávání DNS nebo sestavování spojení TLS) způsobují další zpoždění.

Klient by měl odeslat tolik měřicích paketů, kolik je možné v čase, který test umožňuje, přičemž je třeba dbát na to, aby neodeslal pakety tak rychle, že by to ohrozilo výsledky měření. Všechny jednotlivé hodnoty latence by měly být zaznamenány. Počet použitých měřicích paketů by měl být zvolen tak, aby byla zajištěna statistická významnost výsledku testu.

Kromě testu latence (který se provádí jako samostatný test) by mohl být proveden test latence při zatížení (zpoždění měřené během testu rychlosti) za účelem zjištění parametru „buffer bloat“, protože porovnání latence a latence při zatížení by mohlo naznačovat problémy v síti poskytovatele přístupu k internetu.

Bez ohledu na to, kdy bylo provedeno měření obousměrného zpoždění, se výsledné číslo vypočítá jako medián měření obousměrného zpoždění, přičemž se z výpočtu vyloučí všechna měření s uplynutím časového limitu v důsledku ztrátovosti paketů. Kolísání zpoždění (jitter) lze také odvodit

z kolísání zpoždění pozorovaného během zpoždění.[12]

3.2.1. Doplňková metodika pro delší měření

Aby bylo možné sledovat změnu zpoždění spojení po delší dobu, lze použít dodatečné měření zpoždění s dobou trvání definovanou uživatelem. Pro tento účel se doporučuje implementovat metodiku měření definovanou v dokumentu IETF RFC 2681 *Round-trip Delay Metric for IPPM*. Tato norma vyžaduje náhodný čas výběru vzorku, což vede ke statisticky spolehlivějšímu výběru vzorku.

3.2.2. Měření jednosměrného zpoždění

Norma RFC 2681 pojednává o některých problémech měření jednosměrného zpoždění na internetu. To by vyžadovalo vysoce přesnou synchronizaci hodin mezi klientem a serverem a implementaci aplikačního signalizačního protokolu pro výměnu informací o časování. BEREC proto považuje měření jednosměrného zpoždění za neslučitelné s výše uvedenými požadavky a nepraktické pro případy regulatorního využití.

3.3. Měření ztrátovosti paketů

Pokud se paket nepodaří doručit přes síť během určitého časového limitu, je pro účely měření ztrátovosti paketů považován za ztracený.

U spojení TCP je ztracený paket automaticky a transparentně znovu odeslán odesílatelem, což z pohledu uživatele vede ke snížení výkonu. Pokud platforma, na které se provádí měření výkonu, neposkytuje přístup k podrobným statistikám pro každé spojení TCP, není možné tento transportní protokol použít k měření ztrátovosti paketů.

Pokud je to možné, měly by být pro tento účel použity pakety ICMP echo nebo UDP, a to s ohledem na vše související, co již bylo popsáno pro měření obousměrného zpoždění.

Vzhledem k velmi nízké ztrátovosti paketů pozorované v moderních sítích a možné přechodné povaze jejich příčin (např. přetížení sítě, problémy s přenosem) se doporučuje provádět toto měření odesláním velkého počtu paketů za jednotku času, a to po dlouhou dobu. Stejně tak by rychlost odesílání paketů měla zohledňovat kapacitu spoje, aby nedošlo k ovlivnění měření. Počet paketů omezuje rozlišení měření, proto by měl být kromě poměru ztrát zaznamenáván i celkový počet odeslaných/přijatých paketů.

Minimální počet použitých paketů by měl vycházet z požadovaného rozlišení podle předpokládané ztrátovosti paketů pro měřenou metodu přístupu. Například ztrátovost paketů 0,1 % odpovídá ztrátovosti 1 z 1000 paketů. V této situaci by bylo zapotřebí podstatně většího počtu paketů, aby bylo možné stanovit spolehlivé výsledky s ohledem na požadovanou odchylku chybovosti.

Princip provádění dlouhodobých měření je však v rozporu s koncepcí crowdsourcingového měření z podnětu uživatelů: koncoví uživatelé nebudou akceptovat delší dobu čekání na prezentaci výsledků. Pro měření zpoždění a ztrátovosti paketů se sice upřednostňují testy s dlouhou dobou trvání, to však pravděpodobně přináší nutnost mít na pozadí delší dobu spuštěného měřicího klienta.

[12] Je třeba poznamenat, že počet měření zpoždění je poměrně omezený, takže odchylka těchto údajů má omezenou hodnotu.

4. Zjišťování různých postupů řízení provozu

V této kapitole jsou popsána doporučení pro zjišťování postupů řízení provozu, které ovlivňují konektivitu (podkapitola 4.1) a dosažitelnost (podkapitola 4.2) jednotlivých aplikací.

4.1. Měření konektivity

Tento dokument se zaměřuje na metodiku měření a neuvádí, které postupy řízení provozu jsou povoleny a které nikoli. Témata zahrnují detekci blokovaných nebo částečně blokovaných aplikací a obsahu (např. síťové filtrování obsahu, jako je blokování reklam a blokování webového obsahu) pomocí blokování komunikačních portů, adres URL a IP adres. Níže popsaná měření konektivity jsou proto nezbytnou součástí metodiky posuzování síťové neutrality a měla by být používána podle potřeb jednotlivých vnitrostátních trhů.

Obecně by zde popsaná měření měla platit stejně pro IPv4 i IPv6. Pro jiné protokoly než UDP/TCP (např. ICMP) není uvedena žádná metoda detekce, avšak i ty jsou považovány za relevantní v kontextu služby přístupu k internetu.

BEREC poznamenává, že přístup založený na crowdsourcingu může umožnit porovnání mnoha výsledků těchto měření od různých koncových uživatelů.

4.1.1. Blokování portů

Zda je provoz na určitých portech blokován či nikoli, lze zjistit navázáním spojení s testovaným portem pomocí příslušného transportního protokolu. U protokolu TCP lze port obvykle považovat za otevřený, pokud je možné na něj navázat obousměrnou komunikaci. Vzhledem k tomu, že UDP je bez spojení, musí systém měření definovat mechanismus zpětné vazby, který informuje o tom, zda byl paket přijat.

Měřící nástroje by měly být schopny testovat zablokované porty alespoň prostřednictvím následujících protokolů:

- IPv4 a IPv6;
- TCP a UDP;
- uplink (spojení od koncového uživatele k internetovému hostiteli) a downlink (spojení z internetu ke koncovému uživateli) a
- libovolné platné číslo portu UDP nebo TCP.

Je třeba také poznamenat, že překlad síťových adres (NAT), který mohou používat poskytovatelé internetových služeb a modemy/routery, ovlivňuje spojení sestupným směrem tak, že ve výchozím nastavení jsou všechny komunikační porty sestupným směrem blokovány. To je třeba vzít v úvahu při hodnocení výsledků měření.

Je důležité vzít v úvahu, že výsledky může ovlivnit i prostředí koncového uživatele (místní firewally nebo bezpečnostní software). V případě crowdsourcingového přístupu však může být možné porovnat velké množství výsledků od různých koncových uživatelů. Další informace o těchto tématech jsou uvedeny v kapitolách 5 a 6.

V případě, že významný podíl zkoumaných měření ukazuje na stejný postup vůči provozu, zvyšuje

se pravděpodobnost, že k těmto praktikám skutečně dochází v důsledku nastavení sítě operátora.

4.1.2. Blokování IP adres

Účelem tohoto testu je ad hoc způsobem zjistit, zda jsou určité IP adresy blokovány. Test se provede tak, že se pokusí připojit alespoň k portu, o kterém je známo, že na zvolené cílové adrese běží služba.

Úspěšné připojení na libovolný port (nebo dokonce jakákoli odpověď z této adresy) nestačí ke zjištění, že IP adresa není blokována, protože někteří poskytovatelé internetových služeb mohou pomocí prostředníků simulovat spojení, a dokonce odpovídat na navázané spojení. Proto se doporučuje také odeslat nějaká data a ověřit integritu přijatých dat.

Pokud se spojení nepodaří navázat nebo přijatá data neodpovídají očekávání, lze provést nové měření z jiného místa připojení nebo pomocí sítě VPN pro přístup k internetu mimo kontrolu poskytovatele připojení, aby poskytovatel připojení neviděl skutečnou cílovou adresu. Pokud je připojení přes proxy server úspěšné, lze to považovat za známku toho, že IP adresu blokuje něco v síti poskytovatele internetových služeb.

4.1.3. Manipulace s DNS

Manipulací s DNS se v kontextu nařízení [1] rozumí situace, kdy je od výchozího resolveru[13] poskytovatele internetových služeb obdržena odpověď DNS (na požadavek A nebo AAAA), která nepravdivě uvádí, že doména je neznámá, nebo je vrácena nesprávná IP adresa. Výsledkem této manipulace je přesměrování klienta na jinou adresu.

Manipulaci s DNS lze odhalit analýzou odpovědí na požadavky DNS na známé cíle (např. záznamy DNS konkrétních domén pod kontrolou vnitrostátního regulačního orgánu).

4.1.4. Detekce proxy serveru HTTP

Proxy server HTTP je prostředník, který je vložen do přenosové trasy pro HTTP spojení koncových uživatelů a který lze použít k filtrování nebo úpravě provozu. Proxy server HTTP může být transparentní nebo jinak skrytý.

Transparentní proxy server je prostředník, který může být nasazen poskytovatelem služby přístupu k internetu a funguje jako prostředník mezi klientem a cílovým webovým serverem. V tomto kontextu poskytovatel služby přístupu k internetu směruje HTTP provoz přes proxy server bez zásahu nebo vědomí uživatele. Transparentní proxy server HTTP lze zjistit kontrolou hlaviček HTTP, zda v nich není obsah specifický pro proxy server (HTTP_VIA, VIA, FORWARDED, CLIENT-IP).

Hlavičky požadavků HTTP (TRACE) by také mohly být kontrolovány, zda nedošlo ke změně mezi klientem a serverem a zda zachycující proxy server neprovádí vyhledávání DNS na základě falešné hlavičky hostitele. Skrytý proxy server by mohl být odhalen testem mezipaměti.

Některé proxy servery HTTP lze odhalit připojením k cílové doméně a kontrolou, zda je webový zdroj dostupný, a ověřením, zda je obsah totožný s obsahem přijatým přes proxy server mimo kontrolu poskytovatele internetových služeb.

Proxy server HTTP je možné odhalit také kontrolou vlastností odesílaného provozu, například

[13] Viz bod 78a Pokynů BEREC k otevřenému internetu [3].

příznaku TTL paketu IP.

4.2. Zjišťování postupů, které ovlivňují QoS jednotlivých aplikací

Účelem těchto měření je jednak navrhnout další ukazatele výkonu, které jsou bližší uživatelské zkušenosti, jednak zjistit upřednostňování a/nebo omezení konkrétních aplikací. Tyto postupy řízení provozu lze zjistit měřením některých níže popsaných klíčových ukazatelů výkonu (KPI) a porovnáním výsledků na základě následujících variant:

- porovnání stejných klíčových ukazatelů výkonu týkajících se podobných aplikací pro stejnou předplacenou službu přístupu k internetu,
- porovnání klíčových ukazatelů výkonu pro stejnou aplikaci s použitím ekvivalentního tarifu od jiného poskytovatele internetových služeb a/nebo
- porovnání klíčových ukazatelů výkonu pro stejnou aplikaci a stejnou předplacenou službu přístupu k internetu, ale s použitím VPN.

Tato měření lze provádět pro vybrané aplikace, webové stránky nebo platformy pravidelně nebo v cílených situacích podle potřeby.

Případy použití zahrnují prohlížení webu, streamování videa, přenos hlasu přes IP (VoIP), videokonference, streamování zvuku, cloudové služby nebo sdílení souborů peer-to-peer a další budoucí aplikace, které ještě nebyly vydány.

4.2.1. Omezení portu (throttling)

Aby bylo možné zjistit, zda je určitý port upřednostňován nebo je mu dávána menší přednost, je třeba porovnat výkon testovaného portu s výkonem kontrolního portu. V této souvislosti lze měření rychlosti na portu 443 považovat za základní hodnotu. Pokud dochází k výrazným a opakovaným odchylkám, může to znamenat, že může docházet k omezení portu (throttling).

4.2.2. Jednotlivé aplikace využívající měření výkonu služby přístupu k internetu

Měření výkonu jednotlivých aplikací může ukázat, zda se na nabídku služby přístupu k internetu vztahuje blokování nebo jakýkoli druh upřednostňování či omezování konkrétních aplikací. Některé z těchto postupů řízení provozu mohou být zjistitelné pouze při přetížení sítě, což bude vyžadovat distribuované měření v čase v různých segmentech sítě.

Nástroje pro zjišťování postupů řízení provozu pravděpodobně poskytnou spíše náznak přítomnosti takového postupu než jednoznačný výsledek. Pokud jsou například pozorovány rozdíly ve vypočtené hmotnosti webové stránky (počet bitů, které jsou přeneseny během načítání stránky), která byla načtena za podobných podmínek mezi různými poskytovateli internetových služeb, může to být indikátor pro zjištění blokování části webové stránky (např. reklamy) nebo komprese dat.

Dalším způsobem, jak zjistit postupy řízení provozu, by mohlo být porovnání výsledků měření týkajících se konkrétního poskytovatele internetových služeb, a to jak s VPN, tak bez ní. Klíčovou myšlenkou je použití proxy serveru VPN umístěného poblíž okraje sítě poskytovatele připojení k internetu k nahrávání a přehrávání síťového provozu generovaného libovolnými aplikacemi a jeho porovnání s chováním sítě při přehrávání tohoto provozu mimo šifrovaný tunel. Pokud se objeví

výrazné a opakující se odchylky, může to být jasný signál možného dopadu řízení provozu.

Měření na úrovni aplikace může většinou odhalit pouze přítomnost nepřípustného řízení provozu, nikoli však příčinu nebo odpovědný segment sítě.

5. Prostředí koncového uživatele

Jak je popsáno v kapitole 3, kvalita služby přístupu k internetu se měří prostřednictvím spojení typu end-to-end (klient-server). V pevném prostředí je klient umístěn na terminálu v doméně koncového uživatele, zatímco server je umístěn v blízkosti výstupního bodu sítě poskytovatele internetu směrem do sítě internet. Prostředí koncového uživatele představuje doménu koncového uživatele, která zahrnuje koncové zařízení koncového uživatele (TTE) a může zahrnovat jeho soukromou síť. Skládá se z různých prvků, z nichž některé mohou omezit kvalitu služby, jak ji vnímá koncový uživatel při používání služby přístupu k internetu.

V případě crowdsourcingových měření, která využívají zařízení poskytovaná koncovými uživateli, je TTE součástí hodnocení výkonu a může být omezením v tom smyslu, že skutečnou úroveň výkonu poskytovanou službou přístupu k internetu nelze během měření správně posoudit. Pokud se měření provádí pomocí specializovaných hardwarových sond, lze v zásadě vyloučit specifické omezující účinky způsobené zařízením dodaným koncovým uživatelem. Přístup k měření vyvinutý na základě požadavků vnitrostátních regulačních orgánů (viz podkapitola 3.1.1) však musí umožňovat měření pomocí prohlížeče, a proto nebyla koncepce a použitelnost použití hardwarových sond dále zohledněna. Specializovaná hardwarová sonda s vysokým výkonem připojená přímo k zařízení u zákazníka (CPE) by vyloučila většinu omezení způsobených klientským zařízením.

Ačkoli prostředí koncového uživatele je v tomto kontextu pouze prvkem přenosové trasy měření typu end-to-end, který nemusí vyžadovat zvláštní pozornost, pro některé účely je důležité mít znalosti o uspořádání prostředí koncového uživatele. Tak je tomu například v případě certifikovaného monitorovacího mechanismu (viz kapitolu 8), jehož cílem je posoudit pouze výkon, za který je odpovědná výhradně doména poskytovatele služby přístupu k internetu. Charakteristika prostředí koncového uživatele je také užitečná, pokud jde o následné zpracování měření, aby se zajistila přesná agregace na úrovni trhu (viz podkapitolu 6.3.3). To umožňuje odfiltrovat irelevantní měření, potenciálně zkreslená prostředím koncového uživatele, a zvýšit granularitu dat při hodnocení obecné kvality služby přístupu k internetu.

Ve smlouvách s koncovými uživateli obvykle umístění koncového bodu sítě (NTP)[14] představuje hranici mezi prostředím uživatele a doménou poskytovatele služby přístupu k internetu. Proto lze umístění koncového bodu sítě použít jako referenční bod pro identifikaci prvků, které mohou ovlivnit to, jak koncový uživatel vnímá výkon služby přístupu k internetu, nad rámec smluvního výkonu.

Tyto omezující faktory jsou uvedeny a popsány níže ve dvou samostatných podkapitolách s rozlišením mezi prostředím pevné sítě (viz Obr. 3) a mobilní sítě (viz Obr. 4).

Zda jsou výsledky měření těmito faktory významně ovlivněny, závisí na konkrétní konfiguraci prostředí koncového uživatele a technických vlastnostech příslušných prvků. Pro posouzení dopadu individuální konfigurace prostředí koncového uživatele je třeba analyzovat místní hardware a software. To může provést buď sám klient měření automatickými technickými zdroji, nebo to lze provést prohlášením koncového uživatele. Technická řešení bývají spolehlivější než prohlášení poskytovaná koncovými uživateli, ale vyžadují použití nainstalovaného softwaru na klientském

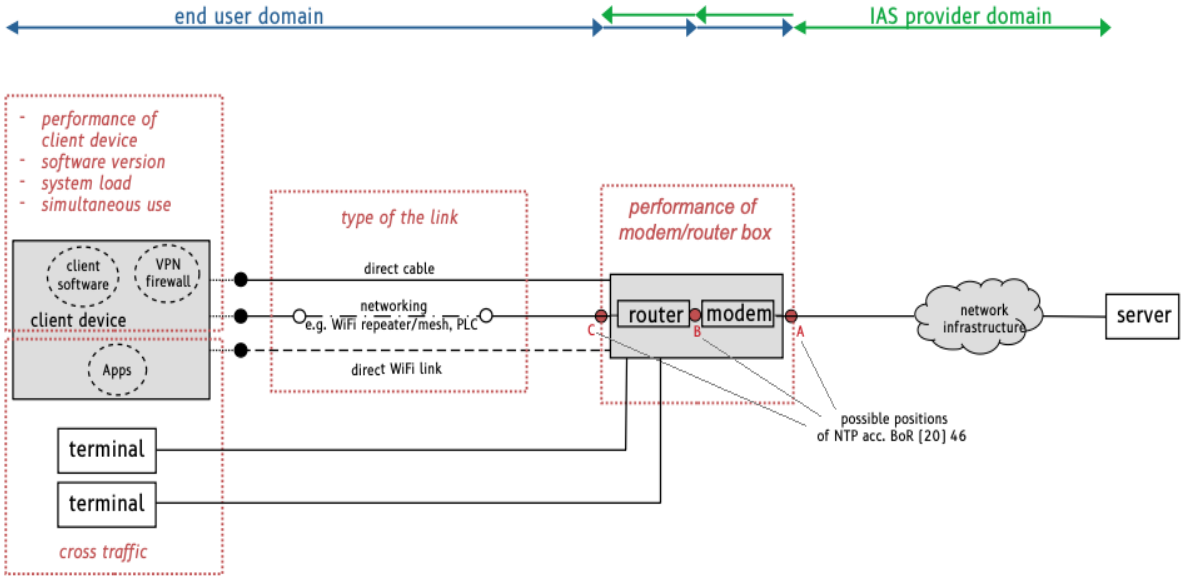
[14]Podle 19. bodu odůvodnění evropského kodexu pro elektronické komunikace (Kodex) představuje koncový bod sítě pro účely regulace hranici mezi předpisovým rámcem pro sítě a služby elektronických komunikací na jedné straně a předpisy pro telekomunikační koncová zařízení (TTE) na druhé straně.

počítači, aby bylo možné přistupovat k různým údajům popsaným níže.

Předpokladem technické analýzy je informovaný souhlas uživatele, který by měl měřicí klient vyžadovat před zahájením měření. Při zpracování a shromažďování informací o koncovém uživateli a prostředí koncového uživatele se řiďte pokyny z kapitoly 9.

5.1. Prostředí koncového uživatele v pevné síti

V následujících podkapitolách jsou nastíněny hlavní problémy, které by mohly bránit přesnějšímu měření výkonu (kvality) služby deklarované smluvními podmínkami. Tyto otázky by měly certifikované monitorovací mechanismy zohlednit při prezentaci výsledků měření.



Obr. 4 – Ilustrace prostředí koncového uživatele v pevné síti

Jak je uvedeno v následujících podkapitolách, různé faktory, které mají původ v prostředí koncového uživatele, mohou omezit úroveň výkonu posuzovanou měřením. Lze je zhruba rozlišit na dopady způsobené klientským zařízením, včetně jeho připojení, a dopady způsobené dalšími zařízeními v místní síti.

Při použití crowdsourcingových řešení, která se spoléhají na neznámé zařízení poskytnuté koncovým uživatelem, by měl být koncový uživatel například požádán, aby

- použil přímý spoj,
- zajistil použití aktuálního hardwaru a softwaru, a
- vyvaroval se současného používání jiných aplikací, které by mohly ovlivnit měření.

Případným negativním vedlejším účinkům křížového provozu z dalších zařízení lze předejít vypnutím nebo odpojením těchto zařízení od routeru/modemu během měření.

5.1.1. Výkon modemu/routeru

V případech, kdy výkon modemu není dostatečný k tomu, aby poskytoval datový tok potřebný k dosažení smluvní maximální rychlosti, není možné změřit skutečnou rychlost služby přístupu k internetu.

Výkon modemu/routeru může být také omezen verzí softwaru (firmwaru) operačního systému, takže k dosažení odpovídající úrovně výkonu může být zapotřebí aktualizovaný software. Vzhledem k tomu, že modem/router může poskytnout buď koncový uživatel, nebo poskytovatel internetového připojení, závisí odpovědnost za údržbu modemu/routeru, jako jsou aktualizace softwaru, nastavení konfigurace atd., na konkrétní situaci.

5.1.2. Typ spoje

V ideálním případě by spojení mezi klientským zařízením (terminálem koncového uživatele, na kterém je spuštěn software měřicího klienta) a modemem/routerem mělo probíhat prostřednictvím přímého kabelového propojení (obvykle Ethernet), které podporuje alespoň rychlost služby přístupu k internetu. Pokud je měření prováděno prostřednictvím spoje s nižším výkonem (např. Wi-Fi, powerline nebo bezdrátový opakovač), může dojít k dodatečnému zpoždění, ztrátovosti paketů nebo snížení propustnosti, takže nelze přesně změřit dostupný výkon služby přístupu k internetu. V případech, kdy se používá Wi-Fi, mohou být důležité informace o verzi Wi-Fi a síle signálu Wi-Fi.

Je třeba poznamenat, že měření v pevné síti lze provádět pomocí mobilního zařízení přes Wi-Fi, v takovém případě se kromě aspektů uvedených v podkapitole 5.2 použijí i aspekty uvedené v podkapitolách 5.1.1 a 5.1.6.

5.1.3. Výkon a zatížení klientského zařízení

Hardwarové a softwarové vybavení klientského zařízení by mělo v zásadě být vhodné pro přesné měření rychlosti. Pokud je však zatížení klientského zařízení z hlediska využití paměti RAM a/nebo procesoru příliš vysoké, klient měření nemusí být schopen generovat dostatečný provoz, aby vytížil službu přístupu k internetu, a měřený výkon tak nemusí odpovídat skutečnému výkonu služby přístupu k internetu. K tomu může dojít, pokud před zahájením měření není ukončen určitý software nebo aplikace.

Během měření by klientské zařízení také nemělo být v úsporném/nízkoenergetickém režimu (např. notebooky nepřipojené k externímu zdroji napájení).

Ačkoli by nic nemělo bránit tomu, aby spotřební elektronická zařízení, jako jsou herní konzole, set top boxy nebo televizory, plnila funkci měřicího klienta, v zásadě by se měl pečlivě zvážit výkon hardwaru/softwaru těchto zařízení, zejména v rámci certifikovaného měření, kdy by bylo vhodnější použít standardní počítače.

5.1.4. Verze softwaru klientského zařízení

Aby měřicí nástroj správně fungoval, může vyžadovat aktuální software, jako jsou operační systémy, prostředí běhu programů a verze prohlížeče (v případě měření v prohlížeči). Zastaralý software v klientském zařízení nemusí obsahovat důležité opravy pro ladění výkonu, ale také měřicí nástroj nemusí být kompatibilní s nejnovější dostupnou verzí softwaru. Kvůli tomu by měly být zdokumentovány informace o verzích softwaru (např. klientského operačního systému a aplikačního

softwaru, jakož i příslušných komponent na straně serveru) používaných při provádění měření.

5.1.5. Současné používání dalšího softwaru, jako je antivirový program a brána firewall

Software na pozadí, jako je virtuální privátní síť (VPN[15]), antivirový program, filtrování podle obsahu (např. rodičovská kontrola), brána firewall a/nebo jakákoli místní manipulace DNS, která interaguje s provozem měřicího klienta, by mohla omezit úroveň výkonu dosažitelnou měřicím zařízením a potenciálně ovlivnit výsledky testu. Takový software na pozadí by také mohl znemožnit detekci postupů řízení provozu, které mají dopad na jednotlivé aplikace.

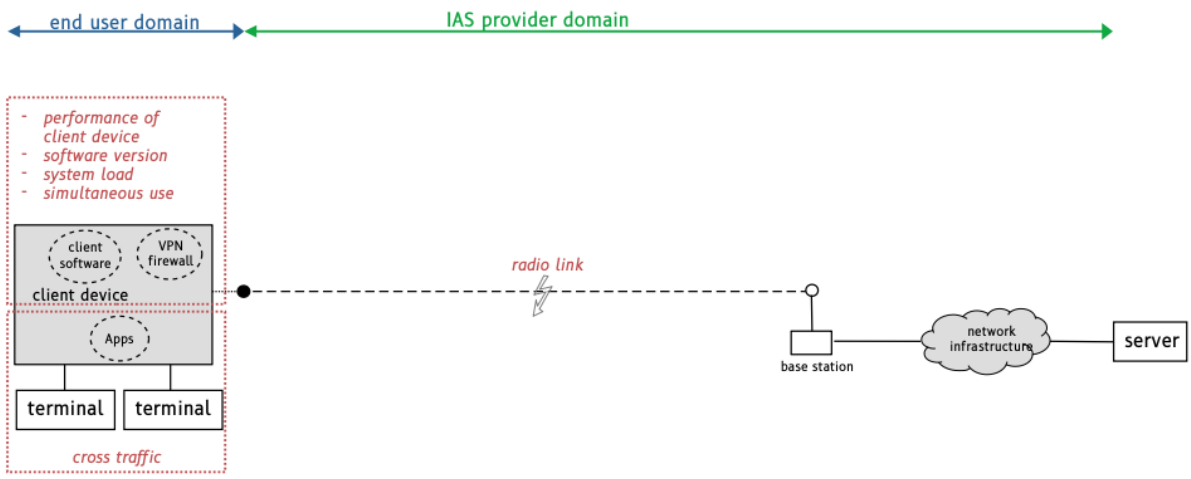
5.1.6. Křížový provoz

Souběžně s provozem měřicího klienta může být generován křížový provoz, například stahování/odesílání dat, streamování hudby, IPTV, videokonference a aktualizace softwaru běžící na pozadí. Ten spotřebovává kapacitu služby přístupu k internetu, a omezuje tak úroveň výkonu dosažitelnou měřením.

Všimněme si, že křížový provoz může být generován aplikací a/nebo operačním systémem v klientském zařízení nebo jiném zařízení a také jinými síťovými uzly v prostředí koncového uživatele.

5.2. Prostředí koncového uživatele v mobilní síti

Mobilní prostředí koncového uživatele má ve srovnání s pevným prostředím jednodušší strukturu. Koncový uživatel zpravidla používá pouze jedno klientské zařízení, které je přímo připojeno ke službě přístupu k internetu prostřednictvím rádiového spojení bez dalších zařízení. Prostředí koncového uživatele se tedy skládá pouze z mobilního telefonu, takže obvykle není třeba provádět podrobnou technickou analýzu prostředí mobilního koncového uživatele.



Obr. 5 – Ilustrace mobilního prostředí koncového uživatele

[15] Mezi sítě VPN patří ty, které jsou součástí operačního systému.

5.2.1. Výkon klientského zařízení

Výkon klientského zařízení (modelu telefonu) zapojeného do měření může omezit úroveň výkonu zjišťovaného měřením. Různé modely mají různý výkon: může to být způsobeno výpočetním výkonem a hardwarovými prvky zařízení, ale také výkonem jeho rádiového rozhraní z hlediska podporovaných standardů a přenosových rychlostí.

5.2.2. Současné používání dalšího softwaru, jako je antivirový program a brána firewall

Tento bod je popsán výše v části o pevném prostředí.

5.2.3. Verze softwaru klientského zařízení

Tento bod je popsán výše v části o pevném prostředí.

5.2.4. Křížový provoz

Výsledky měření by mohl ovlivnit křížový provoz generovaný různými aplikacemi spuštěnými na pozadí klientského zařízení. Je také možné, že koncový uživatel bude sdílet síťové připojení s jinými zařízeními pomocí sdílení (tethering) nebo mobilního routeru/modemu. V těchto případech může docházet ke křížovému provozu z dalších zařízení a v případě, že měřicí klient není spuštěn na terminálu přímo připojeném k rádiovému spoji, je třeba zvážit dopady výkonu lokálních spojení (v rámci domácí sítě LAN).

5.2.5. Metodika přístupu

Aby nedošlo k chybné interpretaci výsledků, měl by testovací klient ověřit, že pro test nepoužívá připojení Wi-Fi. Pokud to není možné, koncovým uživatelům by mělo být doporučeno, aby na zařízení po dobu testu vypnuli Wi-Fi.

5.3. Užitečné informace pro obohacení naměřených dat

Mohly by být shromážděny další informace, které by zvýšily celkovou hodnotu výsledků měření QoS a umožnily určit, zda se příčina špatného výkonu nachází u koncového uživatele nebo u poskytovatele internetových služeb. Tyto informace lze použít k identifikaci (a/nebo vyloučení) omezujících účinků v prostředí koncového uživatele, jak je uvedeno výše (podkapitoly 5.1 a 5.2).

Tyto dodatečné informace lze získat buď technickými zdroji (měřicím klientem nebo prostřednictvím jiných nástrojů, například rozhraní API na úrovni zařízení u zákazníka), nebo prostřednictvím prohlášení koncového uživatele. To umožňuje detekovat měření, u nichž je limitujícím faktorem prostředí koncového uživatele. Doporučuje se získávat další informace, pokud možno, technickými prostředky.

V případě problémů vnímaných koncovým uživatelem by tyto informace mohly být potenciálně použity k vysvětlení neuspokojivých výsledků měření a k identifikaci hlavní příčiny. Mohly by být také použity k lepšímu následnému zpracování výsledků měření pro účely agregace pro celý trh a případného zveřejnění.

Mezi typické informační prvky užitečné pro analýzu a interpretaci výsledků měření může patřit:

- IP adresa klienta (a serveru použitého při měření);
- čas a datum měření;
- informace přenosové trase (traceroute) spojení klient – server a server – klient;
- MSS (maximální velikost segmentu) a MTU (maximální velikost přenosové jednotky) klient/server;
- typ a omezení rychlosti síťových rozhraní klientského zařízení v pevném prostředí;
- typ a omezení rychlosti rozhraní rádiového spoje v mobilním prostředí;
- typ a verze firmwaru modemu/routeru;
- typ a verze softwaru operačního systému klientského zařízení;
- procesor (CPU) a RAM klientského zařízení;
- informace o hardwaru klienta, například model telefonu;
- úroveň křížového provozu (na klientském zařízení nebo v rámci sítě LAN);
- údaj o tom, zda testovací provoz mohl projít sítí VPN.

V pevných sítích sice informace o nabídce služeb přístupu k internetu, jako je typ tarifu, rychlostní limit, typ internetového připojení (FTTH, xDSL atd.), nejsou samy o sobě doménou koncového uživatele, ale jsou užitečné pro přesnou charakteristiku měřené pevné linky.

V mobilních sítích závisí dostupná rychlost mimo jiné do značné míry na kvalitě podmínek rádiového spoje. Proto je důležité získat a uložit informace o rádiových podmínkách, které panovaly během měření. Dostupné rádiové parametry se u různých technologií mobilních sítí a operačních systémů liší. Proto se doporučuje získat dostupné parametry poskytované mobilním telefonem. Kromě toho jsou v této souvislosti užitečné informace o podmínkách měření, jako to, zda se telefon vyskytuje uvnitř budovy či vně nebo zda je v pohybu.

Síť může být například technicky schopna poskytovat vyšší přenosovou rychlost, než umožňuje zakoupený tarif. To by mohlo mít významný dopady na provedená měření. Další možností může být, že po dosažení datového limitu koncového uživatele je rychlost omezena na velmi nízkou hodnotu.

Je třeba poznamenat, že možnost získání těchto údajů samotným měřicím klientem může být při měření prostřednictvím prohlížeče omezená, protože data z operačního systému nejsou přístupná a komunikace s ostatními zařízeními v rámci místní sítě není možná. V této souvislosti by mohlo být relevantní použití dalších řešení pro měření, jako je rozhraní API na úrovni zařízení u zákazníka pro načítání parametrů prostředí koncového uživatele během testu.

6. Metodika posuzování obecné kvality služby přístupu k internetu

Tato kapitola poskytuje rámec pro hodnocení obecné kvality služby přístupu k internetu, který se skládá z několika kroků shrnutých na Obr. 6 níže. Tyto jednotlivé kroky zahrnují shromažďování výsledků měření (podkapitola 6.1), validaci dat (podkapitola 6.2), následné zpracování a agregaci výsledků při zajištění reprezentativnosti databáze výsledků (podkapitola 6.3), analýzu výsledků (podkapitola 6.4) a také zveřejňování příslušných informací současně s hlášením zkreslení měření (podkapitola 6.5).

Obr. 6 - Metodika posuzování obecné kvality služby přístupu k internetu

Při definování obecné kvality služby přístupu k internetu je třeba vzít v úvahu různé kontexty, v nichž je tento pojem v nařízení [1] používán. Tento termín je popsán v souvislosti s posuzováním specializovaných služeb (čl. 3 odst. 5 a 17. bod odůvodnění) a v souvislosti s ochrannými opatřeními vnitrostátních regulačních orgánů na podporu obecného zlepšování a zabránění zhoršování služby přístupu k internetu (čl. 5 odst. 1 a 19. bod odůvodnění).

V prvním případě je třeba posoudit, zda je zbývající kapacita sítě po zavedení specializovaných služeb dostatečná. Vzhledem k tomu, že by bylo obtížné nebo nemožné tyto dvě kategorie služeb oddělit, navrhuje sdružení BEREC použít k takovému posouzení přístup tzv. „černé skříňky“. To znamená, že je třeba posoudit kvalitu obecné služby přístupu k internetu při externích měřeních. Vzhledem ke kolísavému využívání kapacity specializovanými službami v čase je třeba hodnotit výkon obecné služby přístupu k internetu nejen prostřednictvím izolovaných snímků. Proto jsou zapotřebí delší časové řady měření.

Co se týče druhého případu, znění čl. 5 odst. 1, podle něhož vnitrostátní regulační orgány „*podporují neustálou dostupnost nediskriminačních služeb přístupu k internetu na úrovni kvality, která dostatečně odráží technický pokrok*“, rovněž vyžaduje, aby vnitrostátní regulační orgány zajistily a měřily obecné zlepšování výkonu v čase. Metodika hodnocení musí kromě obecné kvality v určitém časovém okamžiku zohledňovat také přiměřený a pozitivní vývoj sledovaných ukazatelů výkonu.

Pevný přístup versus mobilní přístup

Vzhledem k tomu, že požadavky na transparentnost poskytovatelů internetových služeb (čl. 4 odst. 1 písm. d) nařízení) stanoví soubor konkrétních parametrů rychlosti pro služby pevného, resp. mobilního přístupu k internetu, je vhodné zvážit také samostatné posouzení obecné kvality

služby přístupu k internetu pro pevné a mobilní sítě.

6.1. Shromažďování/měření

Měření by mělo probíhat podle metodiky uvedené v kapitole 3 tohoto dokumentu.

Měřící nástroj generuje pro každé období měření sadu dat, která se ukládá do databáze. Existují dva základní přístupy k měření:

a) měření pomocí měřicích systémů s vyhrazenými klienty a servery v kontrolovaném prostředí, nebo

b) crowdsourcingové měření založené na měřeních iniciovaných koncovými uživateli za použití zařízení koncových uživatelů.

Obecné úvahy o tom, jak shromažďovat údaje o měření pomocí crowdsourcingových přístupů k měření, a diskuse o výhodách a nevýhodách tohoto přístupu jsou uvedeny ve *Zprávě BEREC o sledování kvality služeb přístupu k internetu v kontextu síťové neutrality* [4], viz podkapitolu 4.5.2.

Obecná kvalita služby přístupu k internetu by měla být posuzována pro celou účastnickou základnu. Výsledky měření, které jsou shromážděny z hodnocení specifické kvality pro jednotlivé účastníky, lze použít opakovaně. Za účelem obohacení výsledků měření lze přidat doplňující informace o prostředí koncového uživatele, a to buď prostřednictvím automatické detekce, nebo prostřednictvím koncového uživatele, jak je popsáno v kapitole 5.

6.2. Validace dat

V závislosti na zvoleném způsobu měření může být validace dat komplexní a rozsáhlá. Před agregací by měly být výsledky měření anonymizovány a záznamy by měly být normalizovány a nevhodné odfiltrovány.

U přístupu k měření založeného na předem ověřeném nastavení s použitím vyhrazených klientů a serverů mohou stačit základní kontroly věrohodnosti, jako jsou časové značky odpovídající plánu měření, správná identifikace klienta atd.

U crowdsourcingových přístupů k měření je třeba přijmout rozsáhlejší opatření, protože podmínky na straně klienta nejsou předem stanoveny, tj. není známo, zda prostředí koncového uživatele splňuje požadavky na přesné měření. To lze do určité míry zkontrolovat pomocí doplňkových informací (viz podkapitolu 5.3) získaných v době měření, které by měly být, pokud možno, ověřeny.

Proces ověřování (validace) informací poskytnutých koncovým uživatelem je vícestupňový. Takový proces začíná odstraněním nevěrohodných údajů a mohl by zahrnovat ověření identifikace poskytovatele internetových služeb, případně vyřazení těch údajů o poskytovatelích, které nejsou pro dané měření relevantní.

Křížová kontrola správného nastavení měření se provádí pomocí metadat výsledků měření, jak je popsáno výše. V závislosti na požadavcích prostředí koncového uživatele by se spolu s každým výsledkem měření měla shromažďovat určitá metadata. Takové záznamy mohou zahrnovat typ připojení (např. Ethernet, Wi-Fi), typ použitého koncového zařízení, stav koncového zařízení (např. zatížení procesoru, křížový provoz, paralelní aktivní aplikace), síťové prostředí (firewall) nebo

druh přístupové technologie služby přístupu k internetu (např. identifikace typu modemu) atd., jak je popsáno v podkapitole 5.3.[16]

6.3. Následné zpracování a agregace výsledků měření

6.3.1. Následné zpracování měření

Následné zpracování shromážděných dat je klíčovou fází pro eliminaci falešných, zmanipulovaných nebo nerelevantních měření. Umožňuje zajistit, aby výsledky byly reprezentativní a co nejvíce srovnatelné. Pomáhá také chránit před pokusy o podvod.

Vnitrostátní regulační orgány by měly zvážit zavedení účinných algoritmů zpracování dat, aby poskytovaly co nejspolehlivější výsledky. Je například obzvláště důležité, aby byla vyloučena měření získaná z cílového serveru, který se ukázal jako omezující faktor (zejména pokud je kapacita připojení serveru nižší nebo stejná jako kapacita testované přípojky). Dalšími příklady mohou být:

- sloučení více výsledků od stejného koncového uživatele ve stejném časovém rámci (například 1 hodina) u pevného přístupu;
- odhalování a odstraňování automatických testů, které jsou prováděny s cílem poškodit výsledky měření konkrétního poskytovatele internetových služeb.

6.3.2. Statistická reprezentativnost

Obecná kvalita služby přístupu k internetu by měla být posuzována pro celou účastnickou základnu. Pro zajištění reprezentativního souboru výsledků může být zapotřebí provést další opatření k doplnění stávajících výsledků.

Proto je třeba před analýzou výsledků měření posoudit potřebu dalších kroků, aby se zajistilo, že soubor dat statisticky odpovídá skutečnosti. V případě nedostatečných údajů nelze zaručit reprezentativnost. Jakékoli zjištěné zkreslení způsobené metodou testování, které by mohlo negativně ovlivnit vypovídací schopnost výsledků nebo jejich porovnatelnost, by mělo být zmírněno (například dodatečným měřením) a/nebo zveřejněno.

6.3.3. Agregace na úrovni trhu

Po zpracování naměřených dat lze výsledky agregovat. Na úrovni celého trhu by výsledky měření mohly být shrnuty do agregovaných hodnot pro různé kategorie, jako jsou nabídky služeb přístupu k internetu (typ tarifu, datový limit atd., pokud jsou k dispozici), poskytovatelé internetových služeb, zeměpisná oblast, typ technologie, generace mobilních technologií, typ mobilního zařízení atd.

Postupem času má uživatelská základna tendenci přecházet z jedné rychlostní třídy na druhou a z jedné přístupové technologie na jinou (například z DSL na optické připojení). Proto by také mohlo být relevantní agregovat výsledky měření nezávisle na těchto kategoriích. Taková agregace by mohla poskytnout cenné informace o vývoji obecné kvality služeb přístupu k internetu na úrovni trhu a pomoci vnitrostátním regulačním orgánům zaměřit své úsilí na podporu trvalé dostupnosti nediskriminačních služeb přístupu k internetu na úrovni kvality, která odráží technologický pokrok.

[16] Při shromažďování a zpracování informací je třeba zohlednit platná pravidla ochrany osobních údajů.

Agregované výsledky výkonu služby přístupu k internetu na úrovni trhu mohou být použity pro regulační dohled, včetně monitorování obecné kvality služby přístupu k internetu. V ideálním případě by monitorování obecné kvality služby přístupu k internetu bylo založeno na průběžném a nepřetržitém sběru výsledků měření, je však také možné provádět specifické měřicí akce podle potřeby.

Agregované údaje z měření na úrovni trhu by mohly být použity k monitorování toho, zda se celková[17] dostupná kvalita služby přístupu k internetu (např. rychlost, zpoždění a ztráta paketů) v průběhu času zlepšuje. Kromě toho je důležité posoudit, zda poskytovatel internetových služeb přistupuje k jednotlivým žádostem stejně (viz podkapitolu 6.4).

Kromě toho, aby se zohlednila skutečnost, že výkon sítě se může v rámci geografického pokrytí sítě značně lišit, měla by agregace zahrnovat místo měření s granularitou, která vyvažuje anonymitu koncového uživatele a úroveň podrobnosti potřebnou pro rozdělení hodnocení na menší geografické oblasti.

6.4. Analýza

Po agregaci měření by výsledky mohly být vyneseny do grafu v závislosti na vybraném rozměru (rozměrech) a čase (např. rychlost stahování pro danou síť 4G v průběhu času), což by vnitrostátním regulačním orgánům umožnilo extrapolovat reálné zlepšení obecné kvality přístupu k internetu pro pozdější analýzu. Tento přístup by mohl být použit k posouzení dopadu specializovaných služeb na celkovou kvalitu služeb přístupu k internetu.

6.4.1. Měření zlepšení obecné kvality služby přístupu k internetu

Na základě databáze výsledků měření se pro danou podmnožinu dat měření (např. pevný nebo mobilní přístup pro určitý region) vypočítá průměrná rychlost přijímání a odesílání dat za předchozí roky (například z pohledu pěti nebo více let). Pro tyto rychlosti by mohla být použita prediktivní funkce, která by předpovídala rychlost v následujícím roce s ohledem na faktory, jako jsou omezení základních přístupových technologií. V budoucích letech pak lze předpovězené hodnoty porovnat s hodnotami naměřenými v daném roce.

Toto hodnocení lze, s použitím jednotlivých agregačních faktorů, použít také na granulární úrovni (např. pro každého poskytovatele internetových služeb). To by lépe ukázalo, zda konkrétní poskytovatelé internetových služeb vykazují ve srovnání s ostatními obzvláště nízký výkon (vývoj).

Pokud jsou zjištěné průměrné naměřené hodnoty přijímání dat a odesílání dat výrazně nižší než předpokládané hodnoty[18] pro příslušné období, může to znamenat, že se celková kvalita služby přístupu k internetu v průběhu času dostatečně nezlepšila.

Kromě toho by hodnocení mohly doplnit další parametry QoS, jako je latence, jitter a ztrátovost paketů. Pokud je jeden nebo více těchto parametrů ve srovnání s předchozími roky výrazně horší, může to být způsobeno rostoucím přetížením sítě.

A konečně, aby bylo možné posoudit, zda v určitých zeměpisných oblastech dochází ke zhoršení celkové kvality přístupu k internetu, mohly by být výsledky měření, které jsou agregovány pro menší

[17] Může to být průměr nebo medián (nebo dokonce určitý k-tý percentil).
[18] S ohledem na příslušné intervaly spolehlivosti.

oblasti, analyzovány podle jednotlivých oblastí (např. podle krajů nebo obcí).

Každá předpověď by měla být doplněna informacemi o parametrech, které byly použity k jejímu stanovení, a to především s ohledem na údaje uvedené v podkapitole 6.5.

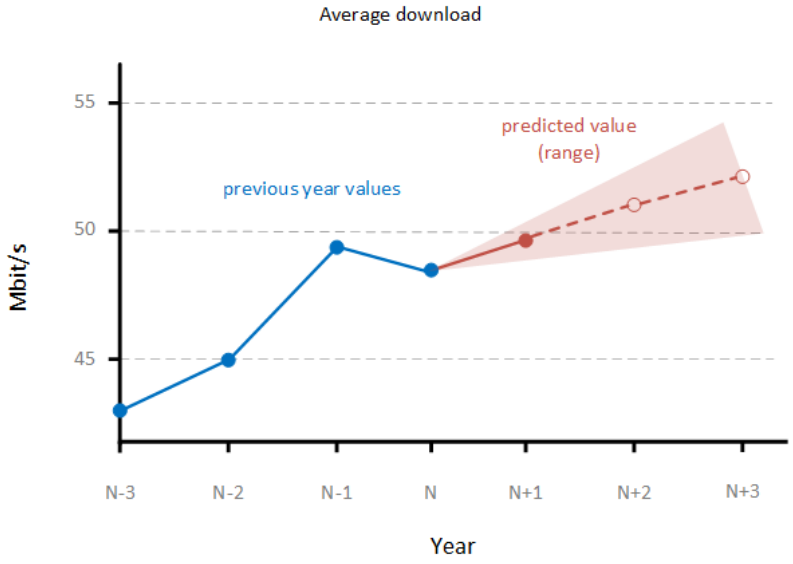
6.4.2. Ilustrace předpovědí

Na následujícím obrázku je uveden příklad, jak lze předpovědi použít pro vizualizaci trendů zjištěných ve zkoumaném souboru dat. Vnitrostátní regulační orgány rozhodnou, které parametry a jejich kombinace budou použity.

Dobře podložená předpověď časové řady vyžaduje podstatný soubor dat, pokud možno pokrývající historické období delší, než je předpovídané období. Kromě toho by měly být do modelu zahrnuty i případné sezónní rozdíly (např. rozdílná úroveň využívání širokopásmového připojení v zimě a v létě) vzhledem k jejich možnému dopadu na časové řady.

Obr. 7 ilustruje předpovědi možného vývoje některých klíčových ukazatelů výkonu v mobilních sítích v příštích několika letech. Všimněme si, že každý daný ukazatel výkonu bude mít horní hranici zlepšení, protože vývoj bude záviset i na technologii. Vnitrostátní regulační orgány musí tyto skutečnosti zohlednit při analýze svých zjištění.

Ilustrace předpovědi průměrné rychlosti stahování z mobilního telefonu na základě časové řady by mohla být provedena způsobem, jaký je uveden na Obr. 7. U tohoto příkladu mohl být pokles rychlosti v roce N způsoben zvýšeným počtem aktivních uživatelů v síti, který nebyl následován zvýšením kapacity sítě.



Obr. 7 - Příklad vizualizace předpokládaných trendů průměrné rychlosti stahování dat

6.4.3. Další analýza: dopad specializovaných služeb na službu přístupu k internetu

Podle čl. 3 odst. 5 druhého pododstavce nařízení [1] nesmí být specializované služby (SpS) poskytovány *„na úkor dostupnosti nebo obecné kvality služeb přístupu k internetu pro koncové*

uživatele". Úkolem vnitrostátních regulačních orgánů je proto kontrolovat, zda specializované služby nejsou poskytovány na úkor služby přístupu k internetu.

V Pokynech BEREC k otevřenému internetu, v bodech 106-115, je popsáno několik přístupů, jak na to mohou vnitrostátní regulační orgány dohlížet, včetně žádostí o informace od poskytovatelů internetových služeb, po nichž následuje posouzení plánů na rozšíření kapacity poskytovatele služeb přístupu k internetu.

Kromě toho by vnitrostátní regulační orgán mohl využít agregované výsledky měření kvality služby přístupu k internetu k analýze výkonu příslušné sítě v dané oblasti a porovnat výsledky před zavedením určité specializované služby i po něm. Pokud jsou naměřené hodnoty rychlosti po zavedení specializované služby obecně nižší, může to svědčit o tom, že specializovaná služba je poskytována na úkor služby přístupu k internetu. Vnitrostátní regulační orgány to mohou monitorovat např. sledováním vývoje výsledků měření průměrné rychlosti u jednotlivých poskytovatelů internetových služeb. Když zavedení specializované služby ovlivní obecnou kvalitu přístupu služby k internetu, může to být patrné i z celkových výsledků výkonu služby přístupu k internetu.

6.5. Zveřejnění

Údaje na úrovni trhu by mohly být rovněž využity pro účely transparentnosti tak, že budou uveřejňovány statistiky, jakož i interaktivní mapy zobrazující výkon pevné služby přístupu k internetu nebo mobilní služby přístupu k internetu v určité zeměpisné oblasti. Tyto údaje by tak koncovým uživatelům poskytly přehled o obecné kvalitě služby přístupu k internetu.

Při zveřejňování údajů na úrovni trhu by měla být zveřejněna jakákoli zjištěná odchylka související s metodikou měření, která by mohla negativně ovlivnit srovnatelnost, zejména při porovnávání poskytovatelů internetových služeb. Zveřejnění by také mohlo posílit transparentnost řady dalších parametrů, například:

- uvedení přesného období, na které se zveřejnění vztahuje;
- uvedení počtu testů pro technologii pevného nebo mobilního přístupu a pro každého poskytovatele internetových služeb;
- poskytnutí co nejvíce podrobností o provedeném zpracování dat (metody úpravy výsledků);
- uvedení místa testu, například v případě mobilní sítě by bylo vhodné uvést procento zákazníků v jednotlivých regionech, pokud se zveřejňují zjištění podle regionů, či procento testů provedených za jízdy (významná vzdálenost ujetá mezi začátkem a koncem testu, pokud je zachycena);
- upřesnění operačního systému: procento operačních systémů podle operátora zohledněné ve výsledcích pro pevnou síť a procento zařízení se systémem Android a iOS použitých pro mobilní síť;
- uvedení procenta testů provedených v protokolu IPv4 a v protokolu IPv6;
- uvedení rozdělení výchozích serverů v případě, že nástroj nabízí několik testovacích serverů: při zveřejnění by mělo být uvedeno rozdělení testů podle provozovatele s ohledem na výběr testovacích serverů;
- sdělení o dalších faktorech, které mohou významně zkreslit analýzu zveřejněných agregovaných výsledků na úrovni trhu. Například v mobilních sítích, kde existují významné

rozdíly vázané na zařízení, by výsledky mohly být rozděleny: např. podle typu zařízení pro každého operátora nebo uvedením procenta testů podle modelu chytrého telefonu na nejpoužívanějších zařízeních. V případě pevných sítí, pokud se při zveřejnění porovnávají různí poskytovatelé internetových služeb bez rozlišení přístupové technologie, se musí jasně uvést, že tato kombinace technologií používaných poskytovateli internetových služeb vnáší do výsledků významné zkreslení. Pokud je to možné, měla by být při zveřejnění uvedena i další možná zkreslení (omezení testovacího serveru, uživatelské zařízení atd.).

Kromě agregace na úrovni trhu by měly vnitrostátní regulační orgány zvážit zveřejňování výsledků měření jako otevřených dat, aby se zvýšila transparentnost. Další doporučení pro zveřejňování informací jsou k dispozici v kapitole 5 Pokynů BEREC stanovující podrobnosti o parametrech kvality služby [6].

7. Posuzování individuálních výsledků

Cílem této kapitoly je poskytnout vnitrostátním regulačním orgánům vodítka při posuzování výsledků měření u jednotlivých účastníků.

7.1. Vyhodnocení měření rychlosti

Rychlost širokopásmového připojení je běžně uváděným ukazatelem, který charakterizuje kvalitu nabídky širokopásmového připojení. Měření rychlosti lze provádět za účelem posouzení obecných i individuálních vlastností sítě. Interpretace výsledků těchto měření musí být co nejrealističtější, protože tyto informace mohou být relevantní pro dohled a vymáhání práva ze strany vnitrostátních regulačních orgánů.

Podle čl. 4 odst. 1 písm. d) nařízení, poskytovatelé internetových služeb ve svých smlouvách o připojení v pevné síti uvádějí minimální, běžně dostupnou, maximální a inzerovanou rychlost přijímání a odesílání dat. U tarifů mobilní sítě musí poskytovatelé internetových služeb uvádět odhadované maximální a inzerované rychlosti přijímání a odesílání dat. Tyto pojmy jsou dále specifikovány v Pokynech BEREC k otevřenému internetu [3].

Minimální rychlost

Podle bodu 143 Pokynů BEREC k otevřenému internetu ohledně pevných sítí platí, že *„Minimální rychlost je nejnižší rychlost, jakou se poskytovatel internetových služeb zavazuje poskytovat koncovému uživateli podle smlouvy (...). V zásadě by skutečná rychlost neměla být nižší než minimální rychlost, s výjimkou případů přerušení (výpadku) služby přístupu k internetu. (…)*“.

Pro ověření minimální rychlosti je třeba porovnat každý platný výsledek individuálního měření rychlosti s minimální hodnotou rychlosti definovanou ve smlouvě a zkontrolovat, zda není některé měření pod touto hodnotou.

Maximální rychlost a odhadovaná maximální rychlost

Podle bodu 145 Pokynů [3] ohledně pevných sítí platí, že „*Maximální rychlost je rychlost, jejíž dosažení může koncový uživatel očekávat alespoň někdy (např. alespoň jednou denně). (…)“*.

Jak je popsáno v bodě 153 Pokynů [3], ohledně mobilních sítí platí, že „*Odhadovaná maximální rychlost pro mobilní službu přístupu k internetu by měla být uváděna tak, aby koncový uživatel porozuměl realisticky dosažitelné maximální rychlosti u své služby v různých místech za realistických podmínek používání. (…)*“.

Pro ověření maximální a odhadované maximální rychlosti na základě dostatečně velkého souboru výsledků za příslušné období je třeba porovnat každé jednotlivé měření rychlosti s (odhadovanou) hodnotou maximální rychlosti definovanou ve smlouvě.

Běžně dostupná rychlost

Podle odůvodnění nařízení a bodu 147 Pokynů BEREC k otevřenému internetu [3] ohledně pevných sítí platí, že „*Běžně dostupná rychlost je rychlost, jejíž dosažení může koncový uživatel očekávat po většinu času během využívání služby*“, a „*Sdružení BEREC má za to, že běžně dostupná rychlost má dvě dimenze: číselné vyjádření rychlosti a dostupnost rychlosti během stanoveného období*

(jako procento), jako jsou např. špičky nebo celý den“.

Dále podle bodu 148 Pokynů BEREC k otevřenému internetu platí, že „*Běžně dostupná rychlost by měla být dostupná během stanoveného denního časového období.*“ Vnitrostátní regulační orgán může například stanovit požadavek, „*že běžně dostupné rychlosti by měly být k dispozici alespoň v době mimo špičku a 90 % doby ve špičce, nebo 95 % času po celý den; (…)“*.

Běžně dostupná rychlost by se měla vypočítat na základě výsledků řady několika měření rychlosti.

Inzerovaná rychlost

V případě pevné služby přístupu k internetu by podle bodu 150 Pokynů BEREC k otevřenému internetu [3] měly vnitrostátní regulační orgány „*V případě, že jsou rychlosti uvedeny v reklamě nabídky poskytovatele internetových služeb*“, zajistit, aby inzerovaná rychlost byla uvedena „*ve smlouvě pro každou nabídku služby přístupu k internetu*“.

V případě mobilní služby přístupu k internetu by podle bodu 156 Pokynů BEREC k otevřenému internetu [3], „*Inzerovaná rychlost pro nabídku mobilní služby přístupu k internetu ... měla odrážet rychlost, kterou může realisticky zajistit koncovým uživatelům.“*

Bod 151 Pokynů BEREC k otevřenému internetu [3] stanoví, že „*Vnitrostátní regulační orgány mohou v souladu s čl. 5 odst. 1 stanovit požadavky na to, jak se rychlosti definované ve smlouvě vztahují k inzerovaným rychlostem, například, že by inzerovaná rychlost neměla přesáhnout maximální rychlost definovanou ve smlouvě*“ ve vztahu k pevné službě přístupu k internetu. Stejně tak bod 157 Pokynů BEREC k otevřenému internetu [3] stanoví, „*že by inzerovaná rychlost pro službu přístupu k internetu uvedená ve smlouvě neměla přesáhnout odhadovanou maximální rychlost definovanou v téže smlouvě*“ ve vztahu k mobilní službě přístupu k internetu.

Měření lze použít k porovnání celkového výkonu poskytovatele internetových služeb s inzerovanými rychlostmi.

7.2. Další parametry QoS a hodnocení řízení provozu

Ostatní parametry spolu s rychlostí přispívají k ucelenějšímu obrazu kvality a přijatelné úrovně služeb pro konkrétní aplikaci nebo službu. Jedná se o ztrátovost paketů, zpoždění a kolísání zpoždění, jejichž metody měření jsou popsány v kapitole 3.

Přijatelná rozpětí těchto hodnot se u jednotlivých služeb liší. Například služba streamování videa založená na progresivním stahování může vyžadovat určitý datový tok s nízkou ztrátovostí paketů, ale nemusí mít přísné požadavky na latenci nebo jitter. Zatímco služba videohovorů/konferencí nemusí mít přísné požadavky na ztrátovost paketů, ale může být velmi citlivá na latenci a jitter.

V této souvislosti může vnitrostátní regulační orgán chtít definovat prahové hodnoty přijatelné výkonu pro různé služby. Tyto prahové hodnoty by mohly být použity na výsledky měření kvality služby s uvedením, které služby by byly na aktuální přípojce přijatelné. Taková informace by mohla mít uživatelsky přívětivou podobu, jako je označení barvami semaforu, červenou, žlutou a zelenou.

8. Certifikovaný monitorovací mechanismus

Jak je již uvedeno v podkapitole 7.1, podle čl. 4 odst. 1 písm. d) nařízení poskytovatelé internetových služeb ve svých smlouvách o připojení v pevné síti uvádějí minimální, běžně dostupnou, maximální a inzerovanou rychlost přijímání a odesílání dat. U přístupů v mobilní síti musí poskytovatelé internetových služeb uvádět odhadované maximální a inzerované rychlosti přijímání a odesílání dat.

Čl. 4 odst. 4 nařízení [1] definuje, že koncový uživatel může „*za pomoci mechanismu sledování ověřeného vnitrostátním regulačním orgánem*“ kontrolovat, zda skutečný výkon odpovídá tomu, co bylo uvedeno ve smlouvě. Tyto informace o měření mohou být použity pro uplatnění prostředků nápravy, které má spotřebitel k dispozici v souladu s vnitrostátními právními předpisy.

To zahrnuje rozhodnutí o tom, zda předplacená služba splňuje různé hodnoty rychlosti definované ve smlouvě a zda existuje „*velká a trvající či pravidelně se opakující odchylka“*. Upozorňujeme, že v některých členských státech nemusí být vnitrostátní regulační orgán příslušný k řešení sporů mezi spotřebiteli a podnikateli poskytujícími služby elektronických komunikací, včetně rozhodování o tom, zda existuje velká odchylka, a taková rozhodnutí může přijímat jiný orgán nebo subjekt.

Aby bylo možné vydat prohlášení buď o neexistenci velké odchylky mezi skutečným a uvedeným výkonem, nebo o existenci takové odchylky, které dává uživateli právo k aktivaci „*prostředků nápravy, které má spotřebitel k dispozici podle vnitrostátního práva*", měla by být z hlediska předpisů splněna řada podmínek, aby měl tento „důkaz“ právní hodnotu. Konečné rozhodnutí o tom, které „důkazy“ jsou dostatečné pro vyvolání právních důsledků, však stále závisí na rozhodnutí soudu. Rozhodnutí vnitrostátních regulačních orgánů by proto měla být přijímána transparentně; všechny údaje z měření by měly být k dispozici pro další právní úvahy příslušného soudu.

Nařízení [1] nevyžaduje, aby členské státy nebo vnitrostátní regulační orgán zřídily nebo certifikovaly monitorovací mechanismus. Proto je třeba poznamenat, že certifikovaný monitorovací mechanismus může být k dispozici pouze v některých členských státech. Nařízení nestanoví, jak by měla být certifikace prováděna, takže se jedná o vnitrostátní záležitost. Pokud vnitrostátní regulační orgán pro tento účel poskytuje monitorovací mechanismus, měl by být považován za certifikovaný monitorovací mechanismus podle čl. 4 odst. 4 nařízení. Vzhledem k tomu, že nařízení hovoří o „mechanismu sledování ověřeném *vnitrostátním regulačním orgánem*“, lze mít za to, že otázka, kdy certifikovat systém sledování a jak jej certifikovat, je na vnitrostátním regulačním orgánu podle vnitrostátních právních předpisů a okolností.

8.1. Pokyny ke kritériím pro certifikovaný monitorovací mechanismu

V tomto bodě jsou uvedeny pokyny ke kritériím, která by vnitrostátní regulační orgány mohly zohlednit při zajišťování vlastního certifikovaného monitorovacího mechanismu nebo při certifikaci mechanismů zajišťovaných třetími osobami v souladu s nařízením [1] a Pokyny BEREC k otevřenému internetu [3].

a) Certifikovaný monitorovací mechanismus by měl splňovat požadavky uvedené v kapitole 3 a zohledňovat úvahy uvedené v kapitole 5.

b) Certifikovaný monitorovací mechanismus by měl být v souladu s platnými právními předpisy, například s pravidly ochrany osobních údajů.

c) Koncoví uživatelé by měli být schopni jednoduše porovnat výsledky měření se smluvními hodnotami rychlosti.

d) Doporučuje se, aby vnitrostátní regulační orgán poskytl pokyny, v jakých případech je velká a trvající či pravidelně se opakující odchylka zjištěna certifikovaným monitorovacím mechanismem. Nedodržení jednoho ukazatele stačí k tomu, aby měl uživatel právo využít „*prostředky nápravy, které má spotřebitel k dispozici podle vnitrostátního práva*“.

e) Doporučuje se, aby vnitrostátní regulační orgán zajistil integritu fungování certifikovaného monitorovacího mechanismu v případě, že mechanismus zajišťuje třetí osoba. Doporučuje se rovněž zohlednit nezávislost a obchodní model subjektu poskytujícího monitorovací mechanismus, pokud jej neposkytuje sám vnitrostátní regulační orgán.

9. Ochrana osobních údajů

Pokud vnitrostátní regulační orgán zvažuje nabídku měřicího nástroje, měl by od samého počátku zvažovat otázky ochrany osobních údajů. Právní rámec pro tuto oblast lze nalézt mimo jiné v obecném nařízení o ochraně osobních údajů („GDPR“, nařízení (EU) 2016/679). Konkrétně je třeba zvážit druh údajů, které spadají pod pojem „osobní údaje“, a důvody, na jejichž základě lze tyto osobní údaje zpracovávat. Je třeba vzít v úvahu i další požadavky na ochranu údajů, jako je minimalizace údajů, práva subjektu údajů a požadavky na zásady ochrany osobních údajů.

Podrobnější přehled o tom, jaké aspekty je třeba do tohoto hodnocení zahrnout, naleznete v kapitole E dokumentu *Specifikace nástroje pro měření síťové neutrality* [7].

10. Odkazy

[1] Nařízení Evropského parlamentu a Rady (EU) 2015/2120 ze dne 25. listopadu 2015, kterým se stanoví opatření týkající se přístupu k otevřenému internetu a maloobchodní ceny za regulovanou komunikaci v rámci Unie a mění směrnice 2002/22/ES a nařízení (EU) č. 531/2012, EUR-Lex - 02015R2120-20181220 - EN - EUR-Lex (europa.eu)

[2] Pokyny BEREC o kvalitě služby v rozsahu pravidel o síťové neutralitě (BoR (12) 131), listopad 2012 (pouze anglicky), http://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/1101-berec-guidelines-for-quality-of-service-in-the-scope-of-net-neutrality

[3] Pokyny BEREC k provádění nařízení o otevřeném internetu (BoR (20) 112), červen 2020, https://www.berec.europa.eu/en/document-categories/berec/regulatory-best-practices/guidelines/berec-guidelines-on-the-implementation-of-the-open-internet-regulation-0 (anglicky), https://www.ctu.cz/sites/default/files/obsah/stranky/956/soubory/pokynyberecknncz2020fin.pdf (česky)

[4] Zpráva BEREC Report o monitorování kvality služby přístupu k internetu v kontextu síťové neutrality, BoR (14) 117, září 2014 (pouze anglicky), http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/4602-monitoring-quality-of-internet-access-services-in-the-context-of-net-neutrality-berec-report

[5] Zpráva BEREC Report o proveditelnosti studie kvality monitorování v kontextu síťové neutrality (BoR (15) 207), listopad 2015 (pouze anglicky), http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5576-feasibility-study-of-quality-monitoring-in-the-context-of-net-neutrality

[6] Pokyny BEREC stanovující podrobnosti k parametrům kvality služby (BoR (20) 53), březen 2020, https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/9043-berec-guidelines-detailing-quality-of-service-parameters

https://www.ctu.cz/sites/default/files/obsah/ctu-new/mezinarodni-organizace/pokyny_ke_qos_cz_fin-2021-04-18.pdf (neoficiální český překlad)

[7] Upřesňující dokument k nástroji pro měření síťové neutrality (BoR (17) 179), říjen 2017 (pouze anglicky), https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/7296-net-neutrality-measurement-tool-specification

[8] Metodologie BEREC k vyhodnocování nařízení o síťové neutralitě (BoR (17) 178), říjen 2017 (pouze anglicky), https://www.berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/methodologies/7295-berec-net-neutrality-regulatory-assessment-methodology