Český telekomunikační úřad
se sídlem Sokolovská 219, Praha 9
poštovní přihrádka 02, 225 02 Praha 025

Praha 12. července 2018

Návrh: verze 2.0

Český telekomunikační úřad (dále jen „Úřad“) v rámci svých kompetencí měří a vyhodnocuje vybrané parametry datových sítí. Měření a vyhodnocování vybraných parametrů sítí elektronických komunikací je v pevných a mobilních sítích sjednoceno v obecném metodickém postupu

**Měření datových parametrů sítí pomocí TCP protokolu,
který je zveřejněn a je ze strany ČTÚ uplatňován v případě kontrolních měření
na pevných i mobilních sítích.**

Měření jsou prováděna pomocí vlastních měřicích zařízení (terminálů) s jasně definovanými parametry, a to jak v pevných, tak i v mobilních sítích. Použitá měřicí metoda vychází z doporučení RFC 6349, „Framework for TCP Throughput Testing“.

I. Úvod

Účelem tohoto dokumentu (dále jen „Metodika“) je popsat a sjednotit postup pro měření reprezentativních datových parametrů pevných, mobilních, bezdrátových a jiných sítí elektronických komunikací, a to pomocí TCP protokolu. Metodika je úmyslně vedena v obecné rovině tak, aby bylo možné zobecnit měření datových parametrů a oprostit měření od fyzické vrstvy síťového provozu, a tedy i technologie. Fyzická vrstva síťového provozu (včetně jednotlivých rozhraní, místa připojení, terminálů apod.) bude pro každou technologii popsána a řešena v samostatné příloze, pokud to bude nezbytné. Z této metodiky, založené na měření na transportní vrstvě modelu ISO/OSI, bude také patrné, že mezi datové parametry, které svým charakterem a významem mohou zásadně ovlivnit kvalitu a efektivitu datového přenosu, patří dostupná informační rychlost přijímání a odesílání dat, zpoždění rámců, rozptyl zpoždění rámců, a hlavně ztrátovost rámců.

Nutnou podmínkou pro měření propustnosti TCP datového toku je dostupnost síťových zdrojů (IP adres, portů, služeb) a s tím související transparentnost síťových tras (v souladu se síťovou neutralitou).

Dokument plně respektuje nebo bere na vědomí mezinárodní doporučení IETF RFC 6349, RFC 2697, RFC 1191, RFC 1981, RFC 2544, RFC 2681, RFC 2923, RFC 4443, RFC 4656, RFC 4821, RFC 4898, RFC 5136, RFC 5357, RFC 7323 a také standardy ITU-T Y.1563 a ITU-T Y.1564.

II. Vymezení měřicích stran a přenosové trasy

1. Měřicí server

Měřicím serverem (MS) nazýváme měřicí stranu, která v případě sestupného směru poskytuje opačné straně služby (data) na vyžádání. Měřicí server je obecně zařízení připojené k síti internet v definovaném bodě. Měřicí server by měl mít dostatečný výkon a nezávislost datového připojení tak, aby byla zajištěna dostatečná prostupnost a garance datových parametrů, a to i v případě vícenásobného připojení měřicích zařízení v jeden okamžik. Měřicí server je součástí Měřicího systému elektronických komunikací (dále jen „MSEK“) pod správou Úřadu.

2. Měřicí zařízení (terminál)

Měřicím zařízením, terminálem, (MT) nazýváme měřicí stranu, která v případě sestupného směru je ve funkci příjemce služby (dat). Měřicím zařízením se rozumí terminál s příslušným obslužným softwarem, který je schopen provádět měření dle platných metodických postupů Úřadu a jehož výpočetní a síťový výkon je natolik vysoký, že žádným způsobem negativně neovlivňuje výsledky měření. Měřicí zařízení musí být schopno během měřicího procesu sledovat a zaznamenávat základní i rozšířený soubor datových parametrů pevných sítí elektronických komunikací, exportovat je ve standardizovaném formátu vhodném pro strojové či jiné vhodné zpracování a následně umožňovat přenést takto získané naměřené hodnoty do centrálního uložiště MSEK, nebo je uchovat v interní paměti.

3. Přenosová trasa

Přenosovou trasou (NUT) nazýváme takovou posloupnost přenosových uzlů, že mezi každými dvěma po sobě jdoucími přenosovými uzly existuje spojení a zároveň prvním přenosovým uzlem je MT a posledním MS. Měřená síť elektronických komunikací je taková síť, která je součástí přenosové trasy a do které bylo měřicí zařízení (terminál) během měření připojeno.

III. Postup měření

Následující postup popisuje sekvenci kroků, které jsou nezbytné pro získání korektních dat měření. Před částí 5, která se plně věnuje samotnému měření propustnosti TCP datového toku, jsou v částích 1 až 3 popsány nutné podmínky, jejichž splnění musí předcházet samotnému měření dle části 5. V případě nedodržení tohoto postupu může, a s největší pravděpodobností bude, docházet ke zkreslení výsledku měření špatným nastavením měřicích stran (hlavně z hlediska jejich přijímacích, respektive vysílacích kapacit).

1. Úvodní ujednání a rizika

Pomocí TCP protokolu nelze spolehlivě měřit nefunkční sítě elektronických komunikací (tzn. takové sítě, které jsou vystaveny velké ztrátě paketů nebo velkému rozptylu zpoždění paketů). Dle RFC 6349 může jako reference sloužit práh 5 % ztráty paketů a rozptyl zpoždění paketů s hodnotou 150 ms. Tyto či vyšší hodnoty již nasvědčují o poruchovém nebo mimořádném stavu sítě (např. přetížení, nedostatečné kapacitě sítě), zvláště pak v prostředí datových sítí na území ČR. Nelze také spolehlivě měřit sítě, kde dochází k poměrně rychlé variaci parametrů v čase (parametrů dle částí 2 a 3).

Dále musí být zajištěno dodržení a respektování následujících ujednání:

- Zohlednění „traffic shaping“, v tomto případě může docházet ke zpožďování provozu některých služeb nebo omezování celkové propustnosti.
- Zohlednění „traffic policing“, v tomto případě může docházet k monitorování provozu a následnému omezení nebo vyloučení provozu při překročení sjednaného limitu; popsáno v RFC 2697.
- Dostupnost služeb na jednom portu nemusí znamenat dostupnost služeb na jiných portech. Proto test propustnosti TCP datového toku dle části 5 je vhodné doplnit o srovnávací test měření portů – dostupnost známých portů.
- V každém bodě měření (testu) musí být zajištěna nezávislost měření – tzn. při každém měření nesmí být realizován žádný další datový tok, který není součástí měření, nebo dostupný datový průtok musí být natolik dostatečný, aby významně neovlivňoval výsledky měření.

2. Identifikace MTU

Identifikace MTU přenosové trasy je zásadní pro správné nastavení měřicího systému tak, aby nedocházelo k fragmentaci, a bylo tak možné měřit kapacitu přenosové trasy co nejpřesněji, respektive musí platit:

$$\mathrm{MTU\ (TCP\ TTD)} = \mathrm{MTU\ (NUT)};\ [\mathrm{B};\ \mathrm{B}]. \tag{1}$$

Pro identifikaci MTU přenosové trasy může být použito několik metod, které se od sebe liší převážně síťovou oblastí, ve které mohou být nasazeny. Pro správnou identifikaci MTU přenosové trasy mohou být použity metody:

- identifikace dle RFC 1191,
- identifikace dle RFC 1981,
- identifikace dle RFC 4821.

Následující části 2.1 až 2.4 stručně popisují jednotlivé metody identifikace MTU přenosové trasy, podrobnosti je možné najít v příslušných doporučeních IETF RFC.

2.1. Identifikace dle RFC 1191

Doporučení RFC 1191 nabízí pro IPv4 nejjednodušší a nejrychlejší způsob zjištění MTU. Jedná se o využití vlastností IPv4 paketů s pevnou volbou velikosti MTU a s nastaveným příznakem $\mathrm{DF} = 1$ (nefragmentovat). Pokud je nastavené MTU příliš velké pro danou přenosovou trasu, respektive pro některý síťový prvek na trase, pak daný síťový prvek IP datagram zahodí a odpoví zpět odesílateli ICMP zprávou o nemožnosti průchodu datagramu a zablokované možnosti fragmentace pomocí příznaku DF. Tato metoda může být použita pouze v případech, kdy síťový administrátor přenosové trasy neblokuje použití ICMP zpráv v síti.

2.2. Identifikace dle RFC 1981

Doporučení RFC 1981 nabízí pro IPv6 podobný princip identifikace MTU jako doporučení RFC 1191. Avšak z podstaty protokolu IPv6 není možné využít nastavení bitu příznaku $\mathrm{DF} = 1$. Při absenci této možnosti se zde využívá principu zaslání ICMPv6 zprávy (s obsahem „packet too big“ dle RFC 4443) tím síťovým prvkem, který není schopen paket dané velikosti přenést. Z této zprávy lze také jednoznačně identifikovat maximální velikost MTU daného síťového prvku. Nicméně tato metoda může být znovu použita opět pouze v případech, kdy síťový administrátor neblokuje použití ICMPv6 zpráv v síti.

2.3. Identifikace dle RFC 4821

Tento postup řeší situace, kde z nějakého důvodu (část 2.4) nelze využít předchozích dvou postupů identifikace MTU. Jedná se především o případy, kde je z nějakého důvodu blokováno zasílání ICMPv4 nebo ICMPv6 zpráv. Operační systém Windows i Linux umožňují

využití implementace standardizované techniky PMTUD (Path MTU Discovery) pomocí volby „black hole detection“ (BHD).

2.4. Problémy se zjišťováním velikosti MTU přenosové trasy

Problémy se zjišťováním velikosti MTU přenosové trasy řeší doporučení RFC 2923.

3. Měření zpoždění (Delay)

Zpoždění, Delay, si je možné představit v podobě uplynulé doby mezi odesláním prvního bitu segmentu TCP a příjmem posledního bitu odpovídajícího potvrzení segmentu TCP. Měření zpoždění, stejně jako identifikaci MTU, je možné realizovat několika způsoby, které se od sebe liší přesností a robustností. Počáteční měření zpoždění je doporučeno provést v procesu zkušebního intervalu. V rámci zkušebního intervalu je doporučeno stanovit hodnotu parametru bDelay, která odpovídá nejmenší naměřené hodnotě zpoždění nezatížené navázaným TCP spojením a dále hodnotu parametru minDelay, který odpovídá nejmenší naměřené hodnotě Delay během navázaného TCP spojení. Parametr bDelay se uplatní při stanovení TCP metriky BD, parametr minDelay je nezbytný k následnému výpočtu dále definovaných parametrů, jako jsou BDP, TCP RWNDmin a také velikosti tzv. socket bufferů. Výsledné hodnoty jsou následně využity k zajištění dostatečné kapacity jak přijímací, tak odesílací strany před samotným měřením.

3.1. ICMP ping

Použití ICMP pingu může být považováno za adekvátní způsob odhadu hodnoty zpoždění za předpokladu, že je zohledněna velikost datagramu. Nicméně vzhledem k povaze ICMP pingu není možné označit tuto metodu za dostatečně přesnou (problémy na straně síťových prvků, prioritizace QoS) a proto se nedoporučuje.

3.2. Použití rozšířených MIB statistik

Využití statistik dostupných v MIB pro měření hodnoty zpoždění dle doporučení RFC 4898.

3.3. Použití vhodných nástrojů

K měření zpoždění je vhodné použít iperf, FTP nebo jiné nástroje pracující na základě zachytávání paketů z testovacích TCP relací. Je důležité si uvědomit, že výsledky založené na zprávách SYN → SYN-ACK na začátku TCP relace by neměly být použity k měření hodnoty Delay.

3.4. Použití protokolu TWAMP

Nejrobustnější a nejvhodnější metodou pro měření zpoždění je postup dle RFC 5357, kde je pro samotné měření doporučeno využít protokolu TWAMP.

4. Měření BB

Před samotným měřením propustnosti TCP datového toku je nutné provést měření nejnižší hodnoty kapacity měřené přenosové trasy BB nebo její hodnotu odvodit na základě smluvních podmínek během procesu místního šetření. Z pohledu modelu ISO/OSI odpovídá hodnota BB fyzické vrstvě (L 1).

Pokud je pochybnost o hodnotě BB nebo je hodnota BB neznámá, je zapotřebí použít ke stanovení BB některý ze způsobů měření prostřednictvím bez-stavového protokolu (např. UDP). Měření je vhodné realizovat v obou směrech, zejména pokud se jedná o asymetrickou technologii sítě elektronických komunikací. Měření je doporučeno provádět opakovaně, tzn. v různých časových intervalech a mimo provozní špičku tak, aby bylo dosaženo relevantních hodnot a hodnoty byly v co nejmenší míře ovlivněny lokálními nebo časově proměnlivými výkyvy v dostupnosti síťových zdrojů. Je také zapotřebí mít stále na paměti, že na BB má vliv

nejen kapacita přenosové trasy daného datového spojení, či zakoupené služby od poskytovatele, ale např. i nevhodné zařízení koncového uživatele (pomalý koncový router, přijímací terminál apod.), či použití nevhodné přístupové metody (např. bezdrátová síť s velkým rušením, nastavení pomalého přenosového režimu, nedostatečné šířky pásma, nebo i nevhodného šifrování). K měření BB lze znovu využít několik metod dle doporučení IETF:

- měření BB dle RFC 2544,
- měření BB dle RFC 5136.

4.1. Měření BB dle RFC 2544

Tato metoda měření je vhodná pro kvalifikovaný odhad BB, nicméně je zapotřebí mít stále na paměti, že tato metoda měření BB byla navržena pro testování síťových prvků v laboratorních podmínkách.

4.2. Měření BB dle RFC 5136

Jedná se o měření dle RFC 5136, které je zaměřeno na měření v reálných podmínkách, proto měření dle tohoto standardu by se mělo stát standardní metodou odhadu BB. Bohužel, toto doporučení neobsahuje žádné konkrétní postupy, jakým způsobem BB měřit, pouze definuje obecné matematické výpočty, proto jeho využitelnost je v dnešní době minimální.

5. Matematický aparát

Před samotným zahájením měření propustnosti TCP datového toku je nezbytné provést potřebné výpočty a nastavení důležitých parametrů, mezi které patří BDP, velikost bufferu BS a velikost TCP RWND. K těmto výpočtům je nutné použít získanou hodnotu minDelay, respektive změřenou výchozí hodnotu zpoždění dle metod uvedených v části 3 a také stanovený parametr BB dle části 4.

5.1. Výpočet BDP

Výpočet BDP se provede násobením získaných hodnot minDelay a BB, respektive:

$$\mathrm{BDP} = \mathrm{minDelay} \cdot \mathrm{BB};\ [\mathrm{b};\ \mathrm{s},\ \mathrm{b/s}]. \tag{2}$$

5.2. Výpočet velikosti bufferu BS

Nastavení velikosti bufferu (BS) je nutné provést dle:

$$\mathrm{BS} \geq \mathrm{BDP};\ [\mathrm{b};\ \mathrm{b}]. \tag{3}$$

5.3. Nastavení velikosti TCP RWND

Nastavení velikosti TCP RWND okna na přijímací straně vychází z hodnoty parametru TCP RWNDmin, kterou je možné stanovit pomocí vztahu:

$$\mathrm{TCP\ RWNDmin} = \frac{\mathrm{BDP}}{8};\ [\mathrm{B};\ \mathrm{b}]. \tag{4}$$

Všeobecné nastavování BS a TCP RWND na vysokou hodnotu může u nízkých hodnot BB vést k přetížení vyrovnávací paměti síťového prvku, jenž směrem TCP TTD vygeneruje v první fázi velké množství segmentů, které síťové zařízení nedokáže odeslat přes BB, a proto dojde ke zbytečnému zahazování paketů vlivem velikosti bufferu síťového prvku.

5.4. Jedno nebo vícenásobné TCP spojení

Rozhodnutí, zda při samotném měření použít jedno nebo vícenásobné TCP spojení, závisí na velikosti BDP, respektive na hodnotě TCP RWNDmin, v souvislosti s nastavenou hodnotou TCP RWND okna na přijímací straně (např. 64 kB). Cílem využití vícenásobných TCP spojení je co nejvěrohodnější pokrytí celé kapacity přenosové trasy. Jestliže platí, že:

$$\mathrm{TCP\ RWNDmin} > \mathrm{TCP\ RWND};\ [\mathrm{B};\ \mathrm{B}], \tag{5}$$

měl by počet TCP spojení odpovídat výsledku rovnice (zaokrouhleno na nejbližší vyšší celé číslo):

$$n = \left\lceil \frac{\text{TCP RWNDmin}}{\text{TCP RWND}} \right\rceil;\ [\text{-; B, B}], \tag{6}$$

kde n je počet TCP spojení a TCP RWND představuje skutečně nastavenou velikost okna na přijímací straně. Příkladem může být situace, kde je účastníkovi k dispozici síť elektronických komunikací s kapacitou přenosové trasy $BB = 500\ \text{Mb/s}$ a $\text{minDelay} = 5\ \text{ms}$. Parametr BDP je možné stanovit podle rovnice (2), respektive $312{,}5\ \text{kB}$. V rámci každé sekvence testů musí být navázán příslušný počet TCP spojení tak, aby bylo možné dosáhnout maximálního využití kapacity přenosové trasy. Pokud nastavíme $\text{TCP RWND} = 64\ \text{kB}$, což odpovídá základnímu používanému maximu, měl by počet TCP spojení odpovídat hodnotě $n = 5$.

Obecné doporučení:

- Je vhodnější provádět měření pro vícenásobné TCP spojení, a to i v případě, kdy není zdánlivě měření s vícenásobným TCP spojením dle rovnice (5) potřeba. Může totiž s ohledem na nastavení parametrů sítí elektronických komunikací docházet k přidělení větší kapacity přenosové trasy. Proto je doporučeno využívat $n \geq 2$.
- TCP RWND o velikosti vyšší než $64\ \text{kB}$ nemusí být vždy k dispozici, jelikož je možné ho nastavit pouze v případě použití TCP rozšíření (tzv. „TCP window scale option“). Navíc může u reálných implementací docházet k situaci, kdy může být programem nastavená velikost okna ignorována, či rekonfigurována na defaultní hodnotu (např. $64\ \text{kB}$).
- V případě použití jakéhokoliv aplikačního měřicího vybavení je nezbytné mít přístup ke konfiguraci a výpisům obou měřicích stran. Výchozí hodnoty nastavení nemusí totiž být dostatečné a mohou vést k mylným výsledkům.
- Je nutné identifikovat, zda měřicí nástroj využívá pevně nastavené TCP RWND, případně hodnotu TCP RWND sám určí na základě stavu NUT před zahájením měření a dále ji během měření udržuje konstantní, případně tuto hodnotu během měření průběžně mění. Tato skutečnost výrazným způsobem ovlivňuje měření.

5.5. Výpočet hodnoty propustnosti TCP datového toku

Doporučení RFC 6349 definuje dvě odlišné metody výpočtu parametrů určujících hodnotu propustnosti TCP datového toku. První metoda výpočtu je teoretická, vycházející ze složení jednotlivých vrstev modelu ISO/OSI, a stanovuje ideální hodnotu propustnosti TCP datového toku TCP iTR. Druhá metoda je praktická a vychází z aktuálního stavu NUT. Výsledkem této metody je aktuální hodnota propustnosti TCP datového toku TCP aTR.

Příkladem může být technologie odpovídající standardu 100BASE-TX, kde je na první vrstvě modelu ISO/OSI dosahována rychlost $100\ \text{Mb/s}$ (NBR; „net bit rate“). Maximálně dosažitelná informační rychlost IR spojové vrstvy modelu ISO/OSI je limitována maximálním množstvím rámců FPS („frames per second“) dle rovnice (ethernetový rámec Ethernet II):

$$\text{FPS} = \frac{\text{NBR}}{(\text{IFG} + \text{Preambule} + \text{MAC DST} + \text{MAC SRC} + \text{Ethertyp} + 802.1\text{Q (802.1ad)} + \text{Payload} + \text{FCS}) \cdot 8};\ [1/\text{s; b/s, B}]. \tag{7}$$

V uvedeném případě, pokud budeme předpokládat, že $\text{IFG} = 12\ \text{B}$, $\text{Preambule} = 8\ \text{B}$, $\text{MAC DST} = 6\ \text{B}$, $\text{MAC SCR} = 6\ \text{B}$, $802.1\text{Q (802.1ad)} = 0\ \text{B}$, $\text{Ethertyp} = 2\ \text{B}$, $\text{Payload} = \text{MTU} = 1500\ \text{B}$ a $\text{FCS} = 4\ \text{B}$, dosahuje technologie 100BASE-TX dle vztahu (7) hodnoty $\text{FPS} = 8127\ 1/\text{s}$. Hodnota parametru TCP iTR na transportní vrstvě modelu ISO/OSI je v případě použití IPv4 protokolu jako protokolu síťové vrstvy bez volitelných částí záhlaví (20 B) a TCP záhlaví bez jakýchkoliv rozšíření (20 B) stanovena dle rovnice:

$$\text{TCP iTR} = (\text{MTU} - \text{IP}_{\text{header}} - \text{TCP}_{\text{header}}) \cdot 8 \cdot \text{FPS};\ [\text{b/s; B}, 1/\text{s}]. \tag{8}$$

V uvedeném případě je hodnota $\text{TCP iTR} = 94.92\ \text{Mb/s}$. Jestliže je v procesu měření TCP datové propustnosti využíváno rozšířené TCP/IP záhlaví (20 až 60 B), je nutné toto rozšířené záhlaví zohlednit ve vztahu (8). Metoda stanovení aktuální hodnoty propustnosti TCP datového toku TCP aTR vychází z kontinuálního měření zpoždění Delay a následného

stanovení průměrné hodnoty tohoto zpoždění $\mathrm{Delay(avg)}$ během daného testu. Průměrnou hodnotu zpoždění $\mathrm{Delay(avg)}$ je tedy možné definovat jako:

$$\mathrm{Delay(avg)} = \frac{1}{\mathrm{t}} \sum_{\mathrm{i}=0}^{\mathrm{N}-1} \mathrm{Delay_i}; [\mathrm{s; s, s}], \tag{9}$$

kde $\mathrm{Delay_i}$ označuje jednotlivé hodnoty Delay, které jsou kontinuálně měřeny s periodou $1\ \mathrm{s}$ a zaznamenávány během daného testu, a parametr t označuje celkovou délku trvání daného testu. Výslednou aktuální hodnotu propustnosti TCP datového toku $\mathrm{TCP\ aTR}$ transportní vrstvy modelu ISO/OSI je možné zapsat ve tvaru:

$$\mathrm{TCP\ aTR} = \frac{\mathrm{TCP\ RWND} \cdot 8}{\mathrm{Delay(avg)}}; [\mathrm{b/s; B, s}]. \tag{10}$$

5.6. Výpočet TCP metrik

Doporučení RFC 6349 definuje tři základní TCP metriky, které mohou být použity pro lepší porozumění a porovnání jednotlivých výsledků měření. Tyto metriky navíc umožňují porovnání TCP datového toku v různých síťových podmínkách a nastavení měřicích stran, a z těchto důvodů by měly být stanoveny během každého testu. Nezbytnou podmínkou je, aby všechny tři základní TCP metriky byly stanovené pro každý směr zvlášť.

5.6.1. TCP transfer time ratio

TCP transfer time ratio ($\mathrm{TCP\ TTR}$) je poměr mezi skutečně dosahovanou hodnotou $\mathrm{TCP\ aTT}$ (aktuální hodnotou doby přenosu) a její ideální podobou ($\mathrm{TCP\ iTT}$). Tuto TCP metriku, která definuje, kolikrát je skutečná doba TCP přenosu delší než její ideální hodnota, můžeme stanovit dle rovnice:

$$\mathrm{TCP\ TTR} = \frac{\mathrm{TCP\ aTT}}{\mathrm{TCP\ iTT}}; [\mathrm{-; s, s}], \tag{11}$$

kde $\mathrm{TCP\ aTT}$ je skutečně dosahovaná doba přenosu souboru dat prostřednictvím TCP spojení, zatímco ideální hodnota $\mathrm{TCP\ iTT}$ je předpovězená doba, za kterou by daný soubor dat měl být přenesen prostřednictvím TCP spojení. Ideální doba $\mathrm{TCP\ iTT}$ je odvozena od ideálně dosažitelné propustnosti TCP datového toku ($\mathrm{TCP\ iTR}$) na transportní vrstvě modelu ISO/OSI. Ideální dobu přenosu souboru dat $\mathrm{TCP\ iTT}$ je možné stanovit dle rovnice:

$$\mathrm{TCP\ iTT} = \frac{\mathrm{SD}}{\mathrm{TCP\ iTR}}; [\mathrm{s; b, b/s}], \tag{12}$$

kde SD označuje velikost souboru dat určeného k přenosu.

5.6.2. TCP efficiency

TCP efficiency ($\mathrm{TCP\ EFF}$) reprezentuje procento úspěšně přenesených bitů bez nutnosti jejich znovu zaslání. Tato metrika udává představu o chybovosti celého TCP spojení a nutnosti opětovného zasílání. Výpočet efektivity TCP přenosu lze provést dle následující rovnice:

$$\mathrm{TCP\ EFF} = \frac{\mathrm{TB} - \mathrm{rTB}}{\mathrm{TB}} \cdot 100; [\%; \mathrm{b, b}], \tag{13}$$

kde TB označuje počet přenesených bitů a rTB označuje počet bitů, které musely být po detekované chybě odeslány znovu.

5.6.3. Buffer delay

Buffer delay (BD) reprezentuje vztah mezi nárůstem průměrné hodnoty zpoždění $\mathrm{Delay(avg)}$ během daného testu a výchozí hodnotou zpoždění bDelay stanovenou před samotným zahájením daného testu. Výslednou hodnotu BD je možné definovat jako:

$$\mathrm{BD} = \frac{\mathrm{Delay(avg)} - \mathrm{bDelay}}{\mathrm{bDelay}} \cdot 100; [\%; \mathrm{s, s}]. \tag{14}$$

6. Měření propustnosti TCP datového toku

Tato část definuje techniky měření propustnosti TCP datového toku tak, aby bylo možné ověřit jeho maximální dosažitelnou hodnotu. Pokud protokol TCP nevyužívá dynamické regulační techniky pro optimální využití přenosového kanálu (automatické nastavení TCP RWND), je nutné znát parametry $\mathrm{minDelay}$ a BB pro danou přenosovou trasu, potažmo mít dokončené potřebné výpočty uvedené v části 5 a mít splněnou nutnou podmínku uvedenou v části 2.

Jelikož měření propustnosti TCP datového toku dle této metodiky je podmíněno správnou funkčností nižších síťových vrstev, je před samotným zahájením měření zapotřebí se ujistit a ověřit funkčnost, kapacitu přenosové trasy a další parametry na druhé a zejména třetí vrstvě referenčního modelu ISO/OSI. Doporučené kroky před spuštěním měření propustnosti TCP datového toku jsou následující:

- Základní ověření, např. pomocí dostupných testovacích nástrojů, které mohou naznačit očekávané hodnoty. Pro stanovení parametrů daného měření je doporučeno ověřit programem pro zachytávání paketů, např. Wireshark, co se skutečně na síťovém rozhraní odehrává (jaké je skutečné $\mathrm{TCP\ RWND}$, zda dochází k opakovaným přenosům paketů a zda nedochází v průběhu přenosu k vyčerpání $\mathrm{TCP\ RWND}$, apod.).
- Ověření, zda nedochází k prioritizaci provozu na základě IP adresy standardních (všeobecně známých) měřicích serverů. Je tedy vhodné provést prvotní měření propustnosti TCP datového toku vůči referenčním měřicím serverům.
- Vhodným postupem je i ověření plnění síťové neutrality, tzn. ověření, zda nedochází k prioritizaci provozu některé služby. V tomto případě zda např. nedochází k prioritizaci portů, které vyžadují větší kapacitu přenosové trasy. Speciálním případem může být prioritizace portů, které využívají měřicí zařízení (terminály). V tomto případě by samozřejmě byly výsledky značně zkresleny.
- V případě vysoké pravděpodobnosti, že vědomě dochází k prioritizaci provozu směrem ke standardním měřicím serverům, ať už na základě IP adresy, či portu, je nutné provést srovnávací měření dle výše uvedených bodů. Pokud se výsledky standardního a srovnávacího měření budou značně lišit, je nutné tuto skutečnost příslušně uvést ve výsledcích měření.
- Je vhodné provést doplňující, indikační, měření prostřednictvím veřejně dostupného nástroje pro měření aktuální kvality služeb přístupu k Internetu, např. NetMetr (měřící server v rámci MSEK).

6.1. Měřicí nástroje

Existuje několik měřicích nástrojů, které jsou schopny provádět měření propustnosti TCP datového toku. Tyto měřicí nástroje musí být implementovány na každou ze dvou měřicích stran, kdy se jedna chová jako klient a druhá jako server. Nástroj musí umožňovat manuální nebo automatické nastavení velikosti jak vysílacího bufferu BS, tak velikosti $\mathrm{TCP\ RWND}$, a to na obou stranách. Dosažitelná propustnost TCP datového toku by měla být následně měřena jednosměrně i obousměrně.

Je nutné vzít v potaz výkon obou měřicích stran tak, aby nedocházelo k degradaci měření. Z důvodu kvalitativního vývoje služby přístupu k síti internet je požadováno, aby součástí měřicího nástroje bylo rozhraní umožňující provádět měření do maximální rychlosti $\mathrm{NBR} \leq 1000\ \mathrm{Mb/s}$ (na straně měřícího serveru až do $\mathrm{NBR} \leq 10\ \mathrm{Gb/s}$). Z důvodů výkonové náročnosti měřicích procesů zvolených nástrojů při měření datových parametrů s rychlostí $\mathrm{NBR} > 100\ \mathrm{Mb/s}$ je doporučeno využít měřicí nástroje s dedikovaným hardware. V případě využití technologie koncového uživatele, např. při indikativním měření, je vždy potřeba brát na vědomí nominální výkon zařízení, zatížení běžnými aplikacemi i stáří zařízení. V těchto případech se může stát, že i měření rychlostí $\mathrm{NBR} \approx 50\ \mathrm{Mb/s}$ může být nad možnosti dané technologie koncového uživatele.

6.2. Sekvence měření

Přístup, sekvence a vyhodnocování výsledků propustnosti TCP datového toku jsou odlišné pro případ měření v pevných sítích elektronických komunikací a pro případ měření v mobilních sítích elektronických komunikací. V případě mobilních sítí elektronických komunikací se sekvence měření dále rozlišují na měření ve stacionárním bodě a na mobilní měření. Následující kapitoly uvádějí charakteristiky jednotlivých způsobů měření.

6.2.1. Měření v pevných sítích elektronických komunikací

Měření v pevných sítích elektronických komunikací z hlediska umístění měřicího zařízení (terminálu) odpovídá stacionárnímu měření. Pro všechna měření ve stacionárním bodě je doporučeno provádět opakovaná měření s dostatečnou časovou a provozní diverzitou.

Je doporučeno provádět tři hlavní, nezávislé, měření včetně dodržení dostatečné časové diverzity, tzn. minimálně jedno měření v provozní špičce a minimálně jedno měření mimo provozní špičku. Vzhledem k časové náročnosti procesu měření propustnosti TCP datového toku je přípustné provést všechny tři hlavní měření v provozní špičce.

Jedno měření by nemělo přesáhovat časový rámec 20 minut, ve kterém proběhne sekvence tří testů. Protože lze výsledné datové parametry měřicího procesu zařadit do souboru základních datových parametrů, tj. vzestupnou propustnost TCP datového toku (upload) $\mathrm{TCP\ aTR_{up}}$, sestupnou propustnost TCP datového toku (download) $\mathrm{TCP\ aTR_{down}}$ a zpoždění Delay, resp. $\mathrm{Delay(avg)}$, zavádí se označení základní test (basic test, dále jen „testB“). Jeden test kategorie testB musí garantovat délku měření propustnosti TCP datového toku v intervalu:

$$60\ \mathrm{s} < \mathrm{T_{TCP}} < 120\ \mathrm{s}, \tag{15}$$

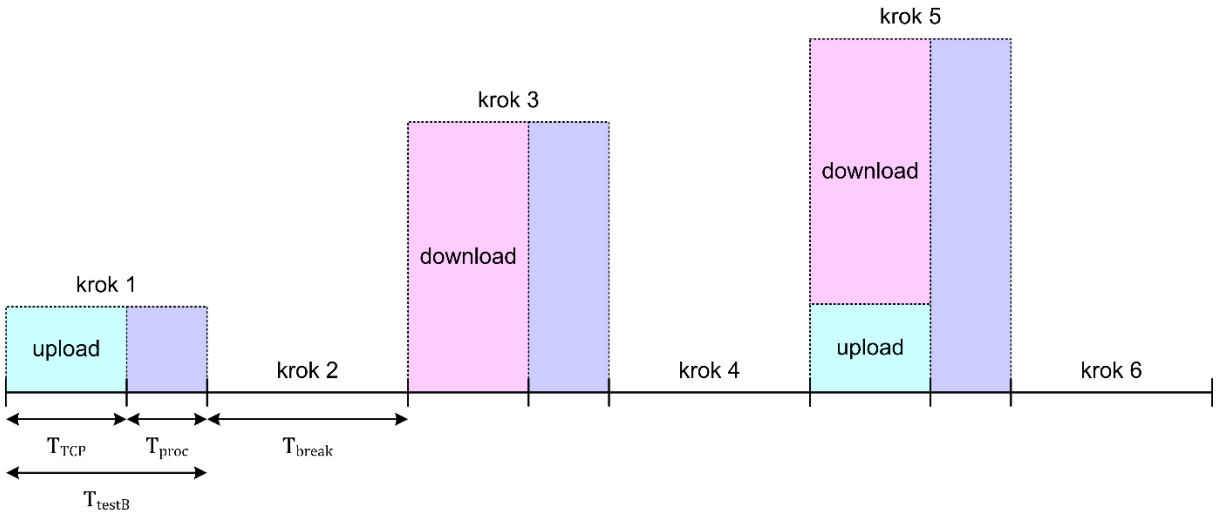
přičemž za doporučenou hodnotu délky měření propustnosti TCP datového toku lze považovat $\mathrm{T_{TCP}} = 90\ \mathrm{s}$. Důvodem stanovení této hodnoty je detekce velké opakující se odchylky od běžně dostupné rychlosti (BDR). Vzhledem k samotnému procesu zpracování naměřených hodnot ($\mathrm{T_{proc}}$) použitými měřicími nástroji by celková délka trvání jednoho testu neměla překračovat hodnotu $\mathrm{T_{testB}}$ (viz obr. 1):

$$\mathrm{T_{testB}} = \mathrm{T_{TCP}} + \mathrm{T_{proc}} \leq 150\ \mathrm{s}. \tag{16}$$

Výsledný proces měření by se měl skládat z následujících kroků (viz obr. 1):

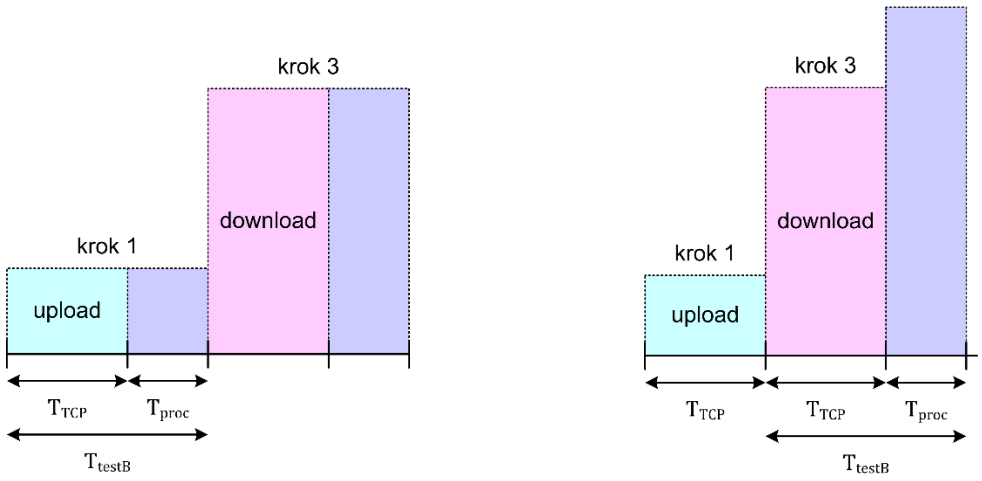
- krok 1 – jednosměrný test vzestupné propustnosti TCP datového toku (upload) $\mathrm{TCP\ aTR_{up}}$ včetně hodnoty zpoždění $\mathrm{Delay(avg)}$ o celkové délce testu $\mathrm{T_{testB}} \leq 150\ \mathrm{s}$,
- krok 2 – pauza (uložení předcházejících výsledků testu) o délce $\mathrm{T_{break}} \leq 120\ \mathrm{s}$,
- krok 3 – jednosměrný test sestupné propustnosti TCP datového toku (download) $\mathrm{TCP\ aTR_{down}}$ včetně hodnoty zpoždění $\mathrm{Delay(avg)}$ o celkové délce testu $\mathrm{T_{testB}} \leq 150\ \mathrm{s}$,
- krok 4 – pauza (uložení předcházejících výsledků testu) o délce $\mathrm{T_{break}} \leq 120\ \mathrm{s}$,
- krok 5 – obousměrný test propustnosti TCP datového toku (upload + download) $\mathrm{TCP\ aTR_{up}}$ a $\mathrm{TCP\ aTR_{down}}$ včetně hodnoty zpoždění $\mathrm{Delay(avg)}$ o celkové délce testu $\mathrm{T_{testB}} \leq 150\ \mathrm{s}$,
- krok 6 – pauza do zahájení další sekvence měření odpovídající časovému odstupu (uložení předcházejících výsledků testu, příprava na další test) o délce $\mathrm{T_{break}} \leq 120\ \mathrm{s}$.

Pokud měřicí nástroj neumožňuje nastavení pořadí sekvence testů v doporučené podobě, je možné uvedené pořadí změnit, aniž by byla porušena integrita měření. Stejně tak je možné vypustit obousměrný test propustnosti TCP datového toku (krok 5), nebo sekvenci pauz mezi jednotlivými testy (kroky 2, 4 a 6). Minimální přípustná podoba procesu měření propustnosti TCP datového toku se musí skládat z jednosměrného vzestupného testu (krok 1) a z jednosměrného sestupného testu (krok 3) propustnosti TCP datového toku.



Obr. 1: Doporučená podoba procesu měření propustnosti TCP datového toku

Možné kombinace realizace minimální přípustné podoby procesu měření závisí na použitých měřicích nástrojích. Teoreticky možné kombinace jsou uvedeny na obr. 2, přičemž se vzájemně liší pouze procesem zpracování naměřených hodnot.



(a) (b)

Obr. 2: Varianty minimální přípustné podoby procesu měření propustnosti TCP datového toku: (a) proces zpracování každého jednosměrného testu zvlášť, (b) proces zpracování všech jednosměrných testů na závěr samotného procesu měření

Měření musí být prováděno v rámci konkrétních demarkačních bodů (DeP x), které budou podrobně specifikovány v Metodice pro měření s vyhodnocení datových parametrů pevných sítí elektronických komunikací. Jako nejběžnější případ si lze představit provádění měření na straně koncového účastníka přímo na předávacím rozhraní služby. Primárně je nutné využít převodník (koncovou jednotku), který je dodáván zákazníkovi při aktivaci služby. Pokud to situace vyžaduje, je možné využít i jiný převodník, který je pro daný typ služby a technologie vhodný. Ve všech případech je ovšem nutné provést kontrolu, zda je k danému převodníku připojeno pouze měřicí zařízení (terminál), a to na všech rozhraních.

6.2.2. Měření v mobilních sítích elektronických komunikací

Měření v mobilních sítích elektronických komunikací z hlediska pozice umístění měřicího zařízení (terminálu) může odpovídat stacionárnímu i mobilnímu měření. Pro všechna měření ve stacionárním bodě je doporučeno provádět opakovaná měření s dostatečnou časovou a provozní diverzitou. V případech, kdy je zapotřebí měřit služby mobilního

charakteru, je možné využít i měření za jízdy (tzv. „drivetest“ či „walktest“). Typickým účelem je zajištění pokrytí dané oblasti mobilní datovou sítí elektronických komunikací. V tomto případě je měření kontinuální s předem definovanou periodou měření (např. $1\,\mathrm{s}$), metrikou (např. kombinace úrovně radiového signálu a hodnoty průtoku dat v daném místě) a vyhodnocovací sítí (např. čtverec $100 \times 100\,\mathrm{m}$). Aktuální pozice měření je za jízdy určována pomocí GPS přijímače, či aproximována dalšími prostředky (v případě nedostupnosti GPS signálu) a umístění přijímací antény je nutné zajistit takovým způsobem, aby byly minimalizovány negativní vlivy dopravního prostředku.

Při provádění mobilního měření je zapotřebí mít na paměti několik skutečností:

- „drivetest“ či „walktest“ lze provádět pouze v místech, kde je to možné (tzn. v případě automobilu na dálnicích, silnicích či cestách; v případě ručního („handy“) měření je možné prostory rozšířit o obchodní prostory, vlaky či jinak nepřístupné prostory),
- měření musí být zajištěno ve fyzikálních podmínkách dané technologie, hlavně s ohledem na rychlost pohybu a tím spojenou otázku Dopplerova jevu,
- měření datových rychlostí za jízdy je detailně popsáno v dokumentu „Postup při měření rychlosti přenosu dat v mobilních sítích dle standardu LTE“, zveřejněném v souvislosti s vyhlášením výběrového řízení za účelem udělení práv k využívání rádiových kmitočtů k zajištění veřejné komunikační sítě v pásmech 800 MHz, 1800 MHz a 2600 MHz.

IV. Vyhodnocení a interpretace výsledků

Výsledkem a výstupem celého měření propustnosti TCP datového toku by měl být záznam o měření, který bude minimálně obsahovat:

- Údaje o času a místě měření, měřených technologiích, postupu a chronologii měření.
- Údaje o nastavení měřicího systému (měřicího zařízení), tj. minimálně v podobě základních parametrů, jakými jsou BB, $\mathrm{minDelay}$, $\mathrm{TCP\ RWND}$ a MTU.
- Hodnoty propustnosti TCP datového toku, respektive ideální hodnotu propustnosti TCP datového toku $\mathrm{TCP\ iTR}$ a aktuální hodnotu propustnosti TCP datového toku $\mathrm{TCP\ aTR}$ pro každý směr odpovídající konkrétní hodnotě $\mathrm{TCP\ RWND}$ či dynamicky nastavované velikosti $\mathrm{TCP\ RWND}$, a to vždy současně s uvedením výsledného zpoždění $\mathrm{Delay(avg)}$. Dále výsledky TCP metrik uvedených v podkapitole Výpočet TCP metrik, minimální přípustná varianta v podobě uvedení alespoň $\mathrm{TCP\ EFF}$ a BD, a to pro každý směr.

V případě detekovaného výpadku služby nebo odchylek od očekávaných hodnot je zapotřebí zvážit možné příčiny. Podrobnosti postupu vyhodnocení a interpretace výsledků měřicího procesu budou uvedeny v hlavní části dokumentu a příslušných příloh Metodiky pro měření s vyhodnocení datových parametrů pevných sítí elektronických komunikací.

1. Postup vyhodnocení

Jak je uvedeno v podkapitole Sekvence měření, postup vyhodnocení naměřených výsledků propustnosti TCP datového toku je odlišný pro případ měření v pevných sítích elektronických komunikací a pro případ měření v mobilních sítích elektronických komunikací.

1.1. Pevné sítě elektronických komunikací

Dle podkapitoly Měření v pevných sítích elektronických komunikací je doporučeno provádět tři hlavní, nezávislé, měření propustnosti TCP datového toku, přičemž jedno měření by nemělo přesáhovat časový rámec 20 minut, ve kterém proběhne sekvence tří testů.

V rámci doporučené podoby procesu měření propustnosti TCP datového toku by výsledkem měření měly být následující výsledné hodnoty parametrů, které můžeme zařadit do souboru základních datových parametrů pevných sítí elektronických komunikací:

- vzestupný test propustnosti TCP datového toku $\mathrm{TCP\,aTR_{up}}$ včetně hodnoty zpoždění $\mathrm{Delay(avg)}$, součástí minimální přípustné podoby procesu měření, krok 1,
- sestupný test propustnosti TCP datového toku $\mathrm{TCP\,aTR_{down}}$ včetně hodnoty zpoždění $\mathrm{Delay(avg)}$, součástí minimální přípustné podoby procesu měření, krok 3,
- obousměrný test propustnosti TCP datového toku $\mathrm{TCP\,aTR_{up}}$ a $\mathrm{TCP\,aTR_{down}}$ včetně hodnoty zpoždění $\mathrm{Delay(avg)}$, krok 5.

Výsledky mohou být pro větší přehlednost vyneseny do podoby krabicového diagramu (boxplotu). V případě testování dostupnosti hlavních (známých) portů (služeb) je vhodné tuto skutečnost zapracovat do přehledné tabulky.

Podrobnější postup vyhodnocení naměřených výsledků propustnosti TCP datového toku s ohledem na Nařízení Evropského parlamentu a Rady (EU) 2015/2120 a s tím souvisejícího Vyjádření Českého telekomunikačního úřadu k vybraným otázkám přístupu k otevřenému internetu a evropským pravidlům síťové neutrality je uveden v Metodice pro měření s vyhodnocení datových parametrů pevných sítí elektronických komunikací.

1.2. Mobilní sítě elektronických komunikací

Podrobnější postup vyhodnocení naměřených výsledků propustnosti TCP datového toku s ohledem na Nařízení Evropského parlamentu a Rady (EU) 2015/2120 a s tím souvisejícího Vyjádření Českého telekomunikačního úřadu k vybraným otázkám přístupu k otevřenému internetu a evropským pravidlům síťové neutrality je uveden v Metodice pro měření s vyhodnocení datových parametrů mobilních sítí elektronických komunikací.

2. Důvody odchylek od ideálních hodnot

Důvody neočekávaných výsledků mohou být různé, počínaje špatným nastavením měřicího systému až po nedostatečnou kapacitu sítě a nedostupností síťových zdrojů. Podrobnosti důvodů odchylek je možné nalézt v doporučení RFC 6349, nicméně k jejich objasnění může významnou měrou pomoci provedení doplňujícího měření na základě standardu ITU-T Y. 1564, respektive stanovení kvalitativních datových parametrů dané NUT (zpoždění rámců FD, rozptyl zpoždění rámců IFDV a ztrátovost rámců FLR).

3. Bezpečnostní úvahy

Jelikož pro měření BB je zapotřebí použít bez-stavových protokolů, může být toto chování v měřicím procesu vnímáno síťovými operátory (poskytovateli) jako pokus o DoS či DDoS útok. Proto testování průtoku TCP dat může vyžadovat koordinaci s poskytovatelem internetového připojení.

3.1. Problematika měření v sítích s IPv6 a NAT

Vzhledem k možnosti zapouzdření TCP protokolu do IPv6 paketu může v dnešní době na síti elektronických komunikací s nativní podporou IPv6 docházet k značnému rozdílu v měření propustnosti TCP datového toku mezi IPv6 a IPv4. Je tedy vhodné ověřit, zda je dostupná IPv6 konektivita a v případě, že ano, provést měření i v situaci, kdy TCP spojení bude zapouzdřeno do IPv6 paketů.

3.1.1. Problematika měření v prostředí neveřejných IP adres a stavových firewallů

V případě, že je z nějakého důvodu zamezena možnost inicializace síťového spojení sestupným směrem server („remote“) → klient („local“), je nutné použít takový měřicí nástroj, který umožňuje reverzní inicializaci síťového spojení při měření sestupné propustnosti TCP datového toku. Tato situace může nastat např. v sítích elektronických komunikací s NAT nebo s nastaveným stavovým firewallem, který blokuje TCP segment s příznakem SYN (navázání spojení) z vnější strany.

3.2. Fyzické a technologické parametry

Měření propustnosti TCP datového toku by mělo být realizováno v konfiguraci klient („local“) → server („remote“).

Serverová část by měla být umístěna v centrálním (páteřním) uzlu datového připojení všech (ať už přímo nebo zprostředkovaně) poskytovatelů datových služeb elektronických komunikací (dále jen „poskytovatel“). Podmínkou je dodržení nezávislosti serverové části na všech poskytovatelích tak, aby docházelo k co nejmenší chybě měření propustnosti TCP datového toku konkrétního poskytovatele.

Klientská část by měla být umístěna co nejblíže rozhraní, které je poskytovatelem deklarované jako místo poskytování jím nabízených služeb (demarkační bod), při současném splnění podmínky měření propustnosti TCP datového toku v místě obvyklém pro účastníka služeb nebo v místě daném smluvním vztahem mezi poskytovatelem a účastníkem. V případě, že umístění klientské části ve výše uvedeném místě není možná, ať už z fyzických, technologických či jiných příčin, bude měření provedeno v co nejbližším možném bodě sítě.

V. Pojmy, definice a zkratky

BB (bottleneck bandwitdh) – nejnižší hodnota kapacity měřené přenosové trasy (b/s)

BDP (bandwidth-delay product) – je výsledek násobku kapacity přenosové trasy (b/s) a zpoždění mezi oběma koncovými zařízeními této přenosové trasy

BDR – označuje běžně dostupnou rychlost

bDelay (baseline Delay) – označuje nejmenší naměřenou hodnotu Delay nezatíženou navázaným TCP spojením při úvodním testovacím intervalu

BS (socket buffer) – buffer na přijímací nebo vysílací straně

Delay – je uplynulá doba mezi odesláním prvního bitu segmentu TCP a příjmem posledního bitu odpovídajícího potvrzení segmentu TCP

DF (don't fragment) – bitový příznak

Ethertyp – určuje pro Ethernet II typ vyššího protokolu

FCS (frame check sequence) – kontrolní posloupnost rámce je 4 B cyklický redundantní součet, který umožňuje detekci poškozených rámců (CRC32 residue s hodnotou 0xC704DD7B)

FPS (frames per second) – parametr 2. vrstvy modelu ISO/OSI definující počet přenesených rámců/s

IFG (inter-frame gap) – povinná mezera mezi dvěma rámci, (100BASE-TX $= 0.96\ \mu s = 12$ B)

IR – informační rychlost označující přenosovou rychlost na spojové vrstvě (L 2) dle modelu ISO/OSI

MAC DST – označuje MAC adresu cílového síťového rozhraní o délce 6 B

MAC SRC – označuje MAC adresu zdrojového síťového rozhraní o délce 6 B

MIB (management information base) – představuje objektově orientovanou sadu SNMP objektů, relací a operací na a mezi objekty. Je rozdělena do 5 oblastí, přičemž pro potřeby Metodiky je potřebná oblast performance management (monitoring dostupnosti, odezvy, průchodnosti a užití jednotlivých prostředků)

minDelay – označuje nejmenší naměřenou hodnotu Delay během navázaného TCP spojení při úvodním testovacím intervalu

MTU (maximum transmission unit) – označení pro maximální velikosti IP datagramu (TCP segmentu), který je možné vyslat daným síťovým rozhraním

n – počet TCP spojení

NAT (network address translation) – překlad síťových adres

NBR (net bit rate) – přenosová rychlost na fyzické vrstvě (L 1) dle modelu ISO/OSI

NUT (network under test) – označuje testovanou přenosovou trasu

PMTUD (path MTU discovery) – standardizovaná technika pro určení velikosti MTU

PPP (point-to-point protocol) – protokol spojové vrstvy ISO/OSI modelu (L 2) umožňující autentizaci, šifrování a kompresi přenášených dat

Preambule – označuje $8 \cdot 10101010$ a slouží k synchronizaci hodin příjemce (Ethernet II)

rozptyl zpoždění paketů – odchylka ve zpoždění mezi doručením jednotlivých paketů (jitter)

rTB – označuje počet bitů, které musely být po chybě zaslány znovu

SD – soubor dat

564 TB – počet přenesených bitů

565 TCP TTD (TCP troughput test device) – označuje zařízení, které generuje metriky provozu
566 a provádí měření, jak je definováno v rámci doporučení IETF RFC 6349

567 TCP RWND (TCP receive window) – označuje velikost TCP okna na přijímací straně

568 TCP RWNDmin (minimální TCP receive window) – označuje vypočtenou hodnotu TCP RWND
569 na základě hodnoty parametru BDP

570 TCP window scale option – umožňuje dle doporučení RFC 7323, „TCP extensions for high
571 performance“, zvýšit velikost TCP RWND až do hodnoty < 2^{30}, tj. do hodnoty < 1GB

572 traffic policing – prostředek pro monitorování provozu sítě elektronických komunikací za
573 účelem omezení maximální přenosové rychlosti prostřednictvím ořezání provozu

574 traffic shaping – prostředek pro řízení objemu provozu sítě elektronických komunikací za
575 účelem jeho rozložení a regulaci přenosové rychlosti

576 TWAMP (a two-way active measurement protocol) – označuje open protokol pro měření
577 obousměrných metrik přenosové trasy. Je založen na architektuře protokolu OWAMP
578 (RFC 4656) a také využívá stejnou architekturu a design

579 802.1Q – označuje VLAN Tagging, resp. umožňuje jednu fyzickou ethernetovou síť rozdělit na
580 více logických sítí (tzv. VLAN) pomocí rozšíření hlavičky ethernetového rámce o další položky

581 802.1ad – označuje koncept dvojitého VLAN Tagging

582