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

Čj. ČTÚ-74 900 / 2014-620

Měření datových parametrů sítí pomocí TCP protokolu

(Metodický postup)

17.prosinec 2014

verze 0.4.5

Obsah

1. Úvod
2. Pojmy, definice a zkratky
3. Vymezení měřicích stran a přenosové trasy
3.1. Měřicí server
3.2. Měřicí terminál
3.3. Přenosová trasa
4. Postup měření
4.0. Úvodní ujednání a rizika
4.1. Identifikace MTU
4.1.1. Identifikace dle RFC 1191
4.1.2. Identifikace dle RFC 1981
4.1.3. Identifikace dle RFC 4821
4.1.4. TCP problémy se zjišťováním MTU přenosové cesty
4.2. Měření RTT
4.2.1. Použití ICMP ping
4.2.2. Použití rozšířených MIB statistik
4.2.3. Použití protokolu TWAMP
4.3. Měření BB
4.3.1. Měření dle RFC 2544
4.3.2. Měření dle RFC 5136
4.4. Potřebné výpočty
4.4.1. Výpočet BDP
4.4.2. Výpočet velikosti bufferu
4.4.3. Výpočet velikostí TCP RWND
4.5. Měření průtoku TCP dat
4.5.1. Doporučené kroky před spuštěním měření
4.5.2. Měřicí nástroje
4.5.3. Sekvence měření
4.5.4. Jedno nebo více TCP spojení
4.5.5. Další doporučení
4.6. Problematika měření v sítích s IPv6 či NAT
4.6.1. IPv4 vs. IPv6
4.6.2. Problematika měření v prostředí neveřejných IP adres a stavových firewallů
4.7. Fyzické a technologické parametry připojení a měření
4.8. Výpočet TCP metrik
4.8.1. Transfer Time Ratio
4.8.2. TCP Efficiency
4.8.3. Buffer Delay
4.8.4. Výpočet maximální teoretické propustnosti TCP v síti
5. Vyhodnocení výsledků
5.1. Postup vyhodnocení
5.2. Důvody odchylek od ideálních hodnot
5.3. Bezpečnostní úvahy
6. Zdroje

1. Úvod

Účelem tohoto dokumentu (dále jen „metodika“) je popsat a sjednotit postup pro měření reprezentativních datových parametrů pevných, mobilních, bezdrátových a jiných datových sítí, 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. Z této metodiky, založené na měření na 4. vrstvě dle modelu ISO/OSI, bude také patrné, že mezi datové parametry, které svým charakterem a významem mohou zásadně ovlivnit kvalitu a efektivitu datového přenosu, patří latence, rychlost přijímání a rychlost odesílání dat daného datového spojení.

Nutnou podmínkou pro měření průtoku TCP dat 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 4821, RFC 2923, RFC 4898, RFC 5357, RFC 2544, RFC 5136 a také doporučení ITU-T Y.1564.

2. Pojmy, definice a zkratky

Jitter - odchylka ve zpoždění mezi doručeními jednotlivých paketů

QoS (Quality of Services) - soubor metod, které jsou využity k zajištění požadované úrovně kvality služeb

TCP throughput - datový tok, který je měřen v určitém bodě a na základě TCP protokolu (v bitech za sekundu)

TCP TTD (Throughput Test Device) - vyhrazené zařízení, které generuje TCP provoz a měří metriku, jak je definována v této metodice nebo v RFC 6349

NUT (Network Under Test) - testovaná IP přenosová cesta

Path MTU (Maximum Transmission Unit) - maximální velikost datového rámce, který je schopen se přenést datovou linkou bez fragmentace

RTT (Round-Trip Time) - rozdíl času od odeslání prvního bitu příjemci po doručení posledního bitu příslušného TCP Acknowledgment

BB (Bottleneck Bandwitdh) - nejnižší hodnota šířky pásma celé měřené trasy

BDP (Bandwidth Delay Product) - násobek kapacity datové linky (v bitech za sekundu) a zpoždění mezi oběma konci této linky (v sekundách)

TCP RWND (Receive WiNDow) - velikost TCP okna na přijímací straně

Odesílací a přijímací socket buffer - Socketový buffer (zásobník) na odesílací a přijímací straně

TWAMP (Two-Way Active Measurement Protocol) - protokol umožňující obousměrné nebo round-trip měření metrik mezi síťovými zařízeními

Datová špička – časový interval, který odpovídá hodnotám, kdy průtok dat v sítí je větší nebo roven 2/3 maximální běžné hodnoty průtoku; obvykle se jedná o časový interval 14 – 22 hodin místního času v pracovní dny

Mimo datovou špičku - časový interval, který odpovídá hodnotám, kdy průtok dat v sítí je menší než 2/3 maximální běžné hodnoty průtoku; obvykle se jedná o časový interval 22 – 14 hodin místního času v pracovní dny a 0 - 24 hodin ve dnech pracovního klidu

PMTUD (Path MTU Discovery) - technika zjišťování MTU přenosové cesty

TT **(Transfer Time)** - doba přenosu datového bloku přes TCP spojení

TTR **(Transfer Time Ratio)** - poměr mezi aktuální hodnotou TT a ideální hodnotou TT

aTT **(Actual TT)** - aktuální doba přenosu datového bloku přes TCP spojení

iTT **(Ideal TT)** - doba, za kterou by daný datový blok měl být přenesen přes TCP spojení

TBS **(Transfer Block Size)** - velikost přenášeného datového bloku

$\max ATT$ **(Maximal Achievable TCP Throughput)** - maximální dosažitelný průtok TCP dat

$TCPe$ **(TCP efficiency)** - účinnost TCP přenosu

$\overline{RTT}$ - průměrná hodnota RTT za určitou dobu

$iRTT$ **(Ideal RTT)** - ideální (předpovězená) hodnota RTT

RTT_i - hodnoty jednotlivých vzorků RTT po vzorkování

3. Vymezení měřicích stran a přenosové trasy

3.1. Měřicí server (MS)

Měřicím serverem nazýváme měřicí stranu, která v případě sestupného směru poskytuje opačné straně služby (data) na vyžádání. Měřicí server by měl mít dostatečný výkon a nezávislost datového připojení tak, aby byla zajištěna prostupnost a garance datových parametrů.

3.2. Měřicí terminál (MT)

Měřicím terminálem nazýváme měřicí stranu, která v případě sestupného směru je ve funkci příjemce služby (dat). Přijímaná data jsou zaznamenávána k následnému vyhodnocení.

3.3. Přenosová trasa

Přenosovou trasou (cestou) 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.

4. Postup měření

Následující postup popisuje sekvenci kroků, které jsou nezbytné pro získání korektních dat měření. Před sekcí 4.5, která se plně věnuje samotnému měření TCP průtoku, jsou v sekcích 4.1 – 4.3 popsány nutné podmínky, jejichž splnění musí předcházet samotnému měření dle bodu 4.5. V případě nedodržení tohoto postupu může, a s největší pravděpodobností bude, docházet ke zkreslení výsledku špatným nastavením měřicích stran (hlavně z hlediska jejich přijímacích, respektive vysílacích kapacit).

4.0. Úvodní ujednání a rizika

Pomocí TCP protokolu nelze spolehlivě měřit nefunkční sítě (tzn. sítě, které jsou vystaveny velké ztrátě paketů nebo velkému jitteru). Dle RFC 6349 může jako reference sloužit práh 5% ztráty paketů a jitter s hodnotou 150 ms. Tyto či vyšší hodnoty již nasvědčují o poruchovém nebo mimořádném stavu sítě (např. přetížení), 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 sekcí 4.2 a 4.3).

Dále musí být zajištěno dodržení a respektování následujících ujednání:

- Zohlednění traffic shaping (může docházet ke zpožďování provozu některých služeb nebo omezování rychlosti provozu).
- Zohlednění traffic poling (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 TCP průtoku dle 4.5 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.

4.1. Identifikace MTU

Identifikace MTU přenosové cesty je zásadní pro správné nastavení měřicího systému tak, aby nedocházelo k fragmentaci, a bylo tak možné měřit přenosovou kapacitu co nejpřesněji, tzn.:

$$\mathrm{MTU(TCP\,TTD)} \rightarrow \mathrm{MTU(NUT)} \qquad [bit\,;bit] \qquad (1)$$

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 sítě mohou být použity následující metody:

1. Identifikace dle RFC 1191
2. Identifikace dle RFC 1981
3. Identifikace dle RFC 4821

Následující sekce krátce popisuje jednotlivé metody identifikace MTU přenosové sítě, avšak více podrobností je možné najít v příslušných doporučeních RFC.

4.1.1. 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 DF (Don't Fragment) = 1 (nefragmentovat). Pokud je nastavené MTU příliš velké pro danou přenosovou cestu (např. pro některý router na trase), pak daný síťový prvek paket zahodí a odpoví zpět odesílateli ICMP zprávou o nemožnosti průchodu paketu a zablokované možnosti fragmentace pomocí příznaku DF. Tato metoda může být použita pouze v případech, kdy síťový administrátor přenosové cesty neblokuje použití ICMP zpráv v síti (např. z „bezpečnostních důvodů").

4.1.2. 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 nefragmentovat.

Při absenci možnosti nastavení bitu „nefragmentovat" se zde využívá principu zaslání ICMPv6 zprávy (s obsahem „Packet Too Big") 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 pouze v případech, kdy síťový administrátor neblokuje použití ICMPv6 zpráv v síti (např. z „bezpečnostních důvodů").

4.1.3. Identifikace dle RFC 4821

Tento postup řeší situace, kde z nějakého důvodu (více se jim věnuje sekce 4.1.4) nelze využít předchozích dvou postupů identifikace MTU. Jedná se především o případy, kde je z nějakého důvodu blokováno zasílání ICMPv4 nebo ICMPv6 zpráv. Systém Windows i Linux umožňují využití implementace PMTUD protokolu pomocí volby Blackhole Router Detection, respektive tcp_mtu_probing.

4.1.4. TCP problémy se zjišťováním MTU přenosové cesty

Problémy se zjišťováním MTU přenosové cesty řeší doporučení IETF RFC 2923.

4.2. Měření RTT

Měření RTT stejně tak, jako identifikace MTU, je možné realizovat několika způsoby, které se od sebe liší přesností a robustností. Každé řešení respektuje a vychází z mezinárodního doporučení IETF.

Měření RTT je nezbytné k následnému výpočtu BDP, TCP RWND a velikostí Socket bufferů. Získané hodnoty budou následně využity k nastavení přijímací i odesílací strany tak, aby byla zajištěna dostatečná kapacita jak přijímací, tak odesílací strany před samotným měřením TCP průtoku.

4.2.1. Použití ICMP ping

Měření pomocí ICMP pingu může posloužit jako adekvátní odhad hodnoty RTT. Rozlišení tohoto měření dosahuje řádu ms (při využití linuxových systémů, či při použití jiných nástrojů je možné dosáhnout i výrazně vyšší přesnosti) a může být také použito k zjištění, zda daný síťový prvek odpovídá na PING nebo ne.

Důležité: Použití ICMP pingu pro odhad RTT může být při použití QoS v síti zařazen do jiné (prioritní) fronty a proto může být výsledek zkreslen.

4.2.2. Použití rozšířených MIB statistik

Další možností, kterou lze využít k odhadu RTT, je postup dle RFC 4898.

4.2.3. Použití protokolu TWAMP

Nejrobustnější a nejvhodnější metodou pro měření RTT je postup dle RFC 5357, kde je pro měření doporučeno využít protokolu TWAMP. Někteří výrobci síťových zařízení (Cisco či Huawei) používají vlastní proprietální řešení jako jsou Service Assurence Agent (SSA), respektive Network Quality Analysis (NQA). Avšak existují zde i implementace „čistého“ protokolu TWAMP, jedná se např. o nástroje diversifEye™ nebo IxNetwork emulator.

4.3. Měření BB

Před samotným měřením průtoku TCP dat je nutné provést měření BB nebo alespoň jeho odhad. V případě vyhrazených linek (spojení) lze považovat za BB hodnotu garantované šířky pásma dané linky na 3. (síťové) vrstvě dle modelu ISO/OSI nebo na internetové vrstvě dle TCP/IP.

Avšak pokud je pochybnost o hodnotě BB nebo je hodnota BB neznámá, je zapotřebí použít k měření BB některý ze způsobů měření pomocí bez-stavového protokolu (např. UDP). Měření je vhodné realizovat v obou směrech (downlink i uplink), zejména pokud se jedná o asymetrickou linku (např. ADSL, VDSL, apod.).

Měření by mělo být prováděno opakovaně, v různých časových intervalech a mimo datovou 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 BB může vzniknout nejen na základě přenosové kapacity linky, či zakoupené služby od poskytovatele, ale např. i nevhodným zařízením koncového uživatele (pomalý koncový router, přijímací terminál apod.), či použitím nevhodné přístupové metody (např. bezdrátová síť s velkým rušením, nastavením pomalého přenosového režimu, nedostatečné šířky pásma, nebo i nevhodného šifrování).

K měření BB lze znovu využít několik metod dle doporučení IETF:

1. Měření dle RFC 2544
2. Měření dle RFC 5136

4.3.1. Měření dle RFC 2544

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

4.3.2. Měření 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 ale toto doporučení neobsahuje žádné konkrétní postupy, jak lze BB měřit, pouze definuje pojmy a obecné matematické výpočty, proto jeho využitelnost je v dnešní době minimální.

4.4. Potřebné výpočty

Před samotným zahájením měření průtoku TCP dat je nezbytné provést potřebné výpočty a nastavení důležitých parametrů, jako jsou BDP, velikost bufferu a velikost TCP RWND. K těmto výpočtům použijeme hodnoty získané v sekcích 4.2 a 4.3, tzn. RTT a BB.

4.4.1. Výpočet BDP

Výpočet BDP provedeme jako roznásobení RTT a BB dle Rovnice 2.

$$BDP = RTT \cdot BB, \qquad [bit\ ;\ s\ ;\ bit \cdot s^{-1}] \tag{2}$$

kde BDP je násobek RTT (doba odezvy neboli zpoždění přenosu v obou směrech) a BB (šířky pásma).

4.4.2. Výpočet velikosti bufferu

Výpočet (nastavení) velikosti bufferu provedeme dle Rovnice 3.

$$BS \geq BDP, \qquad [bit\ ;\ bit] \tag{3}$$

kde BS je velikost bufferu (zásobníku) a BDP je násobek RTT a BB.

Výše uvedený vztah je v souladu s RFC 6349, avšak obecně lze doporučit postup stanovení (nastavení) BS jako

$$BS^{*} = 2^{\lceil \log_2 BS \rceil}, \qquad [bit\ ;\ bit] \tag{3a}$$

kde BS* značí doporučenou hodnotu původní hodnoty BS a znak $\lceil\ \rceil$ značí horní celou část.

4.4.3. Výpočet velikosti TCP RWND

Výpočet (nastavení) velikosti TCP okna na přijímací straně provedeme dle Rovnice 4.

$$RWND \geq \frac{BDP}{8}, \qquad [bit\ ;\ bit] \tag{4}$$

kde RWND je velikost přijímacího TCP okna a BDP je násobek BB a RTT.

Výše uvedený vztah je v souladu s RFC 6349, avšak obdobně jako v sekci 4.4.2, lze obecně doporučit postup stanovení (nastavení) RWND jako

$$RWND^{*} = 2^{\lceil \log_2 RWND \rceil}, \qquad [bit\,;bit] \tag{4a}$$

kde RWND* značí doporučenou hodnotu původní hodnoty RWND a znak $\lceil\ \rceil$ značí horní celou část.

Závěrem této sekce je vhodné poznamenat, že paušální nastavování BS a RWND na vysokou hodnotu může u pomalých BB vést k přetížení vyrovnávací paměti síťového prvku, jehož směrem TCP TTD vygeneruje v první fázi velké množství segmentů, které síťové zařízení nedokáže přes BB odeslat a proto dojde ke zbytečnému zahazování paketů vlivem velikosti bufferu síťového prvku přenosové trasy. V tomto případě je vhodné zvážit možnost využití strategie postupného náběhu RWND.

4.5. Měření průtoku TCP dat

Tato sekce definuje techniky měření TCP průtoku tak, aby bylo možné ověřit maximální dosažitelný průtok TCP dat. Pro měření průtoku TCP dat je nutné již znát RTT a BB dané linky, dle 4.2 a 4.3, potažmo mít dokončené potřebné výpočty dle 4.4 a mít splněnou nutnou podmínku dle 4.1.

Jelikož měření průtoku TCP dat dle této metodiky je podmíněno správnou funkčností nižších síťových vrstev, je před samotným zahájením měření zapotřebí se ujistit a ověřit funkčnost, propustnost, šířku pásma sítě a další parametry na 2. a zejména 3. vrstvě.

4.5.1. Doporučené kroky před spuštěním měření

- Po stanovení parametrů daného měření je vždy vhodné před samotným spuštěním testu ověřit programem pro zachytávání paketů, např. Wireshark, co se skutečně na síťovém rozhraní odehrává (jaké je skutečné RWND, zda a jak intenzivně dochází k opakovaným přenosům paketů a zda nedochází v průběhu přenosu k vyčerpání TCP RWND apod.).
- Není také na škodu v úvodní fázi měření vyzkoušet několik webových (HTTP) měřicích nástrojů (např. speedtest.net). Výsledky mohou posloužit jako určitá reference.
- Dále je doporučeno vyzkoušet i měření vůči jiným než standardním měřicím serverům tak, aby bylo možné porovnat a zjistit, zda nedochází k prioritizaci provozu na základě IP adresy pouze k těmto standardním (a tudíž známým) měřicím serverům. Vhodné je tedy provést měření vůči skrytým (běžně neznámým) měřicím serverům, veřejným měřicím serverům či využití tzv. síťových zrcadel, které slouží pouze k přesměrování („IP redirect“) síťového provozu k standardním 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 šířku pásma. Speciálním případem může být prioritizace portů, které využívají měřicí nástroje či terminály. V tomto případě by samozřejmě byly výsledky značně zkresleny. Zde je možné zvolit dva základní přístupy pro realizaci srovnávacího měření:
    - první spočívá ve využití „well-known“ portů i pro samotné měření (zde je avšak nutné měřicí server přepnout do režimu měření pomocí těchto portů) a

- druhý je založený na již popsané strategii „IP redirect“ nebo zde spíše strategii „IP forwarding“ (přesměrování portů) pomocí měřicího serveru či síťového zrcadla (v případě, že dochází zároveň i k prioritizaci IP adres).

- V případě, že je vysoká pravděpodobnost, že vědomě dochází k prioritizaci provozu směrem ke standardním měřicím serverů, 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.

4.5.2. Měřicí nástroje

Dnes již existuje několik měřicích nástrojů, které jsou schopny měřit TCP průtok. Jedním z nich je např. nástroj „iperf“. Tento nebo jiný nástroj je nainstalován na každou ze dvou měřicích stran, kdy jeden se chová jako klient a druhý jako server. Nástroj umožňuje manuálně nastavovat velikost jak odesílacího socket bufferu, tak velikost TCP RWND a to na obou stranách. Dosažitelný průtok může potom být měřen jak jednosměrně, tak obousměrně.

Avšak je vždy zapotřebí vzít v potaz výkon obou měřicích stran tak, aby nedocházelo k degradaci měření. Pro měření spojení o kapacitě vetší než 100 Mbit/s je dle RFC 6349 doporučeno využít dedikované testovací zařízení, avšak z hlediska vývoje techniky je možné považovat za rozumnou hodnotu okolo 200 Mbit/s. V případě využití technologie koncového uživatele je vždy potřeba brát na vědomí nominální výkon zařízení, zatížení běžnými aplikacemi i stáří zařízení. V těchto případech může i 50 Mbit/s být nad možnosti daného stroje. Dále nelze opomenout i dnes často využívanou techniku virtualizace, která rovněž může vést k dramatickému snížení výkonu dedikovaného stroje.

4.5.3. Sekvence měření

Přístup, sekvence a vyhodnocování výsledků měření jsou odlišné pro případ měření ve stacionárním bodě a pro případ drivetestu (měření za jízdy). Následující kapitoly uvádějí společné charakteristiky jednotlivých měření.

4.5.3.1. Měření ve stacionárním bodě

Pro měření ve stacionárním bodě je možné orientačně použít jednorázový test, avšak tento test je vhodný pouze jako testovací, pro první náhled nebo v případě měření stabilních sítí. Nicméně pro všechna měření ve stacionárním bodě je doporučeno provádět opakovaná měření s dostatečnou časovou a provozní diverzitou.

Doporučujeme proto provádět minimálně dvě hlavní, nezávislá měření s dostatečnou časovou diverzitou, tzn. minimálně jedno měření v datové špičce a minimálně jedno mimo datovou špičku. Jedno měření by mělo trvat minimálně 30 minut a rozestup začátků jednotlivých měření by měl být minimálně 1 hodina. V rámci jednoho měření bude tedy provedeno minimálně 15 testů v následující sekvenci:

Povinné sekvence:

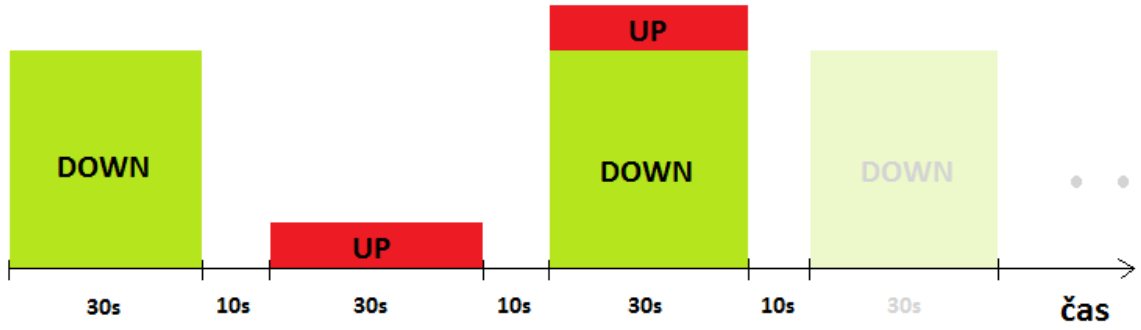
1. min. 30 s – Downlink test
2. min. 10 s – Pauza
3. min. 30 s – Uplink test

4. min. 10 s – Pauza

Volitelné sekvence:

5. min. 30 s – Downlink a Uplink dohromady
6. min. 10 s – Pauza

Sekvenci jednotlivých testů shrnuje graficky následující Obrázek 1:



Obrázek 1: Grafické znázornění sekvence a opakování testů v závislosti na čase

V případech, kdy je připojení nějakým způsobem omezeno, např. pomocí datového limitu FUP, je vždy zapotřebí zohlednit a předem odhadnout celkový objem přenesených dat. V opačném případě může měření vést např. k vyčerpání datového limitu a zneplatnění hodnot měření.

Délka jednotlivých testů v rámci sekvence musí být přizpůsobena tak, aby došlo k náběhu datového průtoku a jeho ustálení, ve kterém systém setrvá minimálně 15 - 20 s. Pro tyto účely je doporučeno provést testovací měření síťového připojení před každým měřením tak, aby bylo možné si udělat obrázek o stavu a kvalitě dané sítě.

V případě velmi pomalých linek v řádu max. stovek kbit/s (technologie GPRS, EDGE, vytáčené připojení apod.) je potřeba si uvědomit, že vždy dojde k přenosu pouze relativně malého množství paketů, a proto může dojít k potenciálně velké nepřesnosti měření. V těchto případech je tedy vhodné prodloužit základní měřicí interval (30 s) na minimálně trojnásobek (tzn. 90 s), aby výsledek dílčího měření byl přesnější.

Dále pokud aplikační software neumožňuje nastavení pořadí sekvence testů v doporučeném pořadí, je možné dané pořadí změnit bez toho, aniž by byla porušena integrita měření. Stejně tak je také možné vypustit sekvenci ohledně současného obousměrného testu nebo sekvenci pauz (prodlev) mezi sekvencemi měření.

4.5.3.2. Měření za jízdy

V případech, kdy je zapotřebí měřit služby mobilního charakteru, je možné využít i měření za jízdy (tzv. drivetest či „walktest“), např. za účelem zjištění pokrytí datovou rychlostí. V tomto případě je

měření kontinuální s předem definovanou vzorkovací frekvencí (např. 1 s), metrikou (např. kombinace úrovně radiového signálu a hodnoty průtoku dat v daném místě) a vyhodnocovací sítí (např. čtverec 100 x 100 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 drivetestů je zapotřebí mít na paměti několik skutečností, a to např.:

- 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

4.5.4. Jedno nebo více TCP spojení

V případě linek, kde je vysoká hodnota BDP by mělo dojít k rozdělení měření do více TCP spojení tak, aby došlo k co nejvěrohodnějšímu pokrytí celé šířky pásma. Počet TCP spojení by měl vycházet z následující Rovnice 5

$$N = \left\lceil \frac{BDP}{RWND} \right\rceil, \qquad [-; bit; bit] \qquad (5)$$

kde N je počet spojení, BDP je násobek RTT a BB, RWND je velikost TCP okna přijímací strany a označení $\lceil \ \rceil$ značí horní celou část.

Jako příklad může sloužit následující datové spojení s parametry: BB = 500 Mbit/s a RTT = 5 ms.

Výpočet:

$$BDP = RTT \cdot BB = 5\,ms \cdot 500\,Mbit/s = 312{,}5\,KB \cdot$$

$$N = \left\lceil \frac{BDP}{RWND} \right\rceil = \left\lceil \frac{312{,}5\,KB}{RWND} \right\rceil$$

V rámci každé sekvence tedy musí být navázán příslušný počet TCP spojení tak, aby bylo možné dosáhnout maximální šířky pásma dle Tabulky 1:

TCP RWND	Počet TCP spojení
16 kB	20
32 kB	10
64 kB	5
128 kB	3

Tabulka 1: Vztah mezi TCP RWND a počtem TCP spojení nutných pro pokrytí celé síťové šířky pásma

4.5.5. Další doporučení

- V úvodní fázi měření je doporučeno vždy provést měření i pro více TCP spojení, a to i v případě kdy není zdánlivě toto měření dle Rovnice 5 potřeba. Může totiž s ohledem na nastavení QoS parametrů sítě docházet k přidělení větší šířky pásma pro více spojení.
- TCP RWND o velikosti 128 kB nemusí být vždy k dispozici nebo pouze v případě použití TCP rozšíření *scale factor*. Dále je potřeba mít na vědomí, že u reálných implementací TCP může být programem nastavená velikost okna ignorována, či rekonfigurována na defaultní hodnotu (např. 64 kB).
- V případě použití jakéhokoliv aplikačního měřicího vybavení je nezbytné mít přístup ke konfiguraci a výpisům obou měřicích stran (klient i server). Výchozí hodnoty nastavení nemusí totiž být dostatečné a mohou vést k mylným výsledkům.
- Dále je potřeba identifikovat, zda používaný měřicí nástroj využívá pevně nastavené RWND či tuto hodnotu během měření ladí. Tato skutečnost velmi ovlivňuje měření.

4.6. Problematika měření v sítích s IPv6 či NAT

4.6.1 IPv4 vs. IPv6

Jelikož dnes již TCP protokol nemusí být zapouzdřen do IPv4 paketu, ale i do IPv6 záhlaví, může i na síti s nativní podporou IPv6 docházet k značnému rozdílu v měření datových parametrů mezi IPv6 a IPv4. Je tedy vhodné ověřit, zda je dostupné IPv6 připojení a v případě, že ano, provést měření i v situaci, kdy TCP spojení bude zapouzdřeno do IPv6 paketů.

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

V případě, že je z nějakého důvodu zamezena možnost inicializace síťového spojení sestupným směrem (od serveru ke klientovi), je nutné použít měřicí nástroj, který umožňuje reverzní inicializaci spojení při měření datových parametrů sestupného datového toku. Tato situace může nastat např. v sítích s NAT překladem neveřejných IP adres nebo v sítích s nastaveným stavovým firewallem, který blokuje segment TCP s příznakem SYN (navázání spojení z vnější strany).

4.7. Fyzické a technologické parametry připojení a měření

Měření by mělo být realizováno v konfiguraci (klient – server), i když nelze vyloučit i měření v konfiguraci klient – klient, pouze klient nebo pouze listener.

Serverová část měření by měla být realizována (umístěna) v centrálním (páteřním) uzlu datového připojení všech (ať už přímo nebo zprostředkovaně) poskytovatelů datových služeb. Podmínkou je dodržení co možná největší nezávislosti měřicího serveru na všech poskytovatelích tak, aby docházelo k co nejmenší chybě měření datových parametrů konkrétního poskytovatele.

Klientská část měření by měla být realizována (umístěna) co nejblíže místu sítě, které je poskytovatelem deklarované jako místo poskytování (předání) jeho služeb, avšak stále tak, aby měření kvality služeb poskytovatele probíhalo v místě obvyklém pro účastníka služeb nebo v místě daném smluvním vztahem mezi poskytovatelem a účastníkem. V případech, kdy realizace klientské

části měření v bodě výše uvedeném není možná, ať už z fyzických, technologických či jiných příčin, bude měření provedeno v co možná nejbližším možném bodě sítě.

Detailní a podrobné informace k jednotlivým technologiím budou k tomuto dokumentu přikládány formou příloh tak, aby bylo možné reagovat na technický vývoj beze změny metodiky měření.

4.8. Výpočet TCP metrik

Tato sekce nastiňuje tři základní metriky, které mohou být použity pro lepší porozumění a porovnání jednotlivých výsledků měření. Tyto metriky navíc umožňují porovnání průtoku TCP dat v různých síťových podmínkách a nastavení měřicích stran, proto by měly být měřeny během každého testu.

Na tomto místě je vhodné upozornit, že všechny níže uvedené metriky je nutné měřit v každém směru zvlášť.

4.8.1. Transfer Time Ratio

Transfer Time Ratio (TTR) je poměr mezi aktuální hodnotou TT a ideální hodnotou TT, dle následující Rovnice 6

$$TTR = \frac{aTT}{iTT}. \qquad [-;s;s] \qquad (6)$$

Aktuální hodnota TT je doba přenosu datového bloku přes TCP spojení, zatímco ideální hodnota TT je předpovězená doba, za kterou by daný datový blok měl být přenesen přes TCP spojení.

Ideální TT je odvozen od maximálního dosažitelného průtoku TCP dat na 4. vrstvě dle modelu ISO/OSI. Vztah mezi ideální TT a maximálním dosažitelným průtokem TCP dat vyjadřuje následující Rovnice 7

$$iTT = \frac{TBS}{\max ATT}, \qquad [s;bit;bit \cdot s^{-1}] \qquad (7)$$

kde iTT je ideální TT, TBS je velikost přenášeného datového bloku a $\max ATT$ je maximální dosažitelný průtok TCP dat.

4.8.2. TCP Efficiency

Druhá metrika reprezentuje množství TCP bitů, které nemusely být zaslány znovu. Tato metrika udává představu o chybovosti celého TCP spojení a nutnosti znovu-zaslání paketů po chybě na lince. Výpočet účinnosti TCP přenosu lze provést dle následující Rovnice 8

$$TCPe = \frac{TB - rTB}{TB} = 1 - \frac{rTB}{TB}, \qquad [-;bit;bit] \qquad (8)$$

kde $TCPe$ značí účinnost TCP přenosu, TB počet přenesených bitů a rTB počet bitů, které musely být po chybě zaslány znovu.

4.8.3. Buffer Delay

Tato metrika reprezentuje vztah mezi nárůstem RTT během testu průtoku TCP dat a vlastní (ideální) RTT. Vlastní (ideální) RRT znamená takové RTT, které je vlastní přenosové cestě za ideálních podmínek, tzn. bez zahlcení.

Průměrná hodnota RTT během testu průtoku TCP dat může být spočítána dle následující Rovnice 9

$$\overline{RTT} = \frac{1}{t}\sum_{i=0}^{N-1} RTT_i \,, \qquad [\,s\,;\,s\,] \tag{9}$$

kde $\overline{RTT}$ značí průměrnou hodnotu RTT za dobu t, N je počet vzorků RTT vzorkovaných po 1 s a RTT_i jsou hodnoty jednotlivých vzorků.

Veličina buffer delay (BD) může být potom reprezentována jako

$$BD = \frac{\overline{RTT} - iRTT}{iRTT} = \frac{\overline{RTT}}{iRTT} - 1, \qquad [-\,;\,s\,;\,s] \tag{10}$$

kde $iRTT$ je ideální RTT.

4.8.4. Výpočet maximální teoretické propustnosti TCP v síti

Jelikož jsou vždy výsledky měření TCP propustnosti ovlivněny protokolovou režií, je proto potřeba vzít v úvahu RFC 6349, sekci 4.1.1. ohledně výpočtu maximální teoretické propustnosti TCP protokolu v síti, která je vždy nižší než šířka pásma na nižších vrstvách. Pokud poskytovatel služeb nabízí a garantuje kapacitu síťového připojení na jiné než vrstvě TCP protokolu, je nutné tento rozdíl dle dané sekce RFC 6349 vzít v úvahu.

5. Vyhodnocení a interpretace výsledků

Výsledkem a výstupem celého testu by měl být report, který bude minimálně obsahovat:

1. Údaje o termínu a místě testování, technologii, postupu, chronologii měření apod.
2. Údaje o nastavení testovacího zařízení, minimálně v podobě základních parametrů, jako jsou BDP, Send Socket Buffer, TCP RWND
3. Hodnoty průtoku TCP dat pro každou testovanou hodnotu RWND
4. Volitelně i výsledky všech třech metrik dle 4.8

V případě odchylek od ideálních hodnot je zapotřebí zvážit možné příčiny dle následujících sekcí 5.2 a 5.3.

5.1. Postup vyhodnocení

Dle sekce 4.5 by výsledkem měření mělo být minimálně 15 hodnot průtoku TCP dat v každé z následující kategorii:

- v sestupném směru a datové špičce,
- ve vzestupném směru a datové špičce,
- v sestupném směru a mimo datovou špičku,
- ve vzestupném směru a mimo datovou špičku.

Výsledky jednotlivých měření je možné považovat za vzorky náhodné veličiny s distribucí podle log-normálního nebo normálního rozdělení. Proto vhodnou metodou pro kvalifikovanou a zároveň přehlednou reprezentaci výsledků dat může sloužit např. vyjádření hodnot ve tvaru medián společně s 90% intervalem spolehlivosti (α = 0,1). Výsledky také mohou být pro větší přehlednost vyneseny do trendového (burzovního) grafu v závislosti na čase.

V případě testování dostupnosti hlavních (známých) portů (služeb), je vhodné tuto skutečnost zpracovat do přehledové tabulky.

5.2. Důvody odchylek od ideálních hodnot

Důvody rozdílných výsledků mohou být různé, počínaje špatným nastavením měřicího systému až po zahlcení sítě a nedostupnost síťových zdrojů.

Více ohledně důvodů odchylek je možné nalézt v doporučení IETF RFC 6349, sekce 5.2 Result Interpretation.

5.3. Bezpečnostní úvahy

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

6. Zdroje

[1] IETF RFC 6349, B.Constantine, JDSU, https://tools.ietf.org/html/rfc6349, 2011

[2] IETF RFC 2697, J. Heinanen, Telia Finland, https://tools.ietf.org/html/rfc2697, 1999

[3] IETF RFC 1191, J. Mogul, DECWRL, https://tools.ietf.org/html/rfc1191, 1990

[4] IETF RFC 1981, J. McCann, Digital Equipment Corporation, https://tools.ietf.org/html/rfc1981, 1996

[5] IETF RFC 4821, M. Mathis, J. Heffner, PSC, https://tools.ietf.org/html/rfc4821, 2007

[6] IETF RFC 2923, K. Lahey, dotRocket, Inc., https://tools.ietf.org/html/rfc2923, 2000

[7] IETF RFC 4898, M. Mathis, J. Heffner, Pittsburgh Supercomputing Center, https://tools.ietf.org/html/rfc4898, 2007

[8] IETF RFC 5357, K. Hedayat, Brix Networks, https://tools.ietf.org/html/rfc5357, 2008

[9] IETF RFC 2544, S. Bradner, Harvard University, https://tools.ietf.org/html/rfc2544, 1999

[10] IETF RFC 5136, P. Chimento, JHU Applied Physics Lab, https://tools.ietf.org/html/rfc5136, 2008

[11] ITU-T Y.1564, ITU-T group, http://www.itu.int/rec/T-REC-Y.1564-201103-I/en, 2011