Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informatiky a kvantitativních metod

Modul pro testování propustnosti sítě

Bakalářská práce

Autor: Tomáš Bartoníček
Studijní obor: Aplikovaná informatika

Vedoucí práce: doc. Ing. Filip Malý, Ph.D.

Hradec Králové Duben 2018

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 27.4.2018 Tomáš Bartoníček

Poděkování:

Děkuji vedoucímu bakalářské práce doc. Ing. Filipovi Malému, Ph.D. za metodické vedení práce, své rodině a pracovnímu kolektivu za podporu během celého studia.

Anotace

Bakalářská práce popisuje aplikaci, pro testování síťové propustnosti a stability síťového spojení. Aplikace je modulem, který připojení testuje v periodických intervalech a podle různých aspektů vyhodnocuje, zda je stabilní a použitelné pro komunikaci a přenos dat nebo ne. Test spojení je komplexní – skládá se z několika subtestů (přítomnost síťového připojení, stabilita, rychlost, latence atd.). Použití modulu je cíleno především pro integraci v aplikaci pro mobilní zařízení (s připojením Wi-Fi nebo mobilní datové sítě), avšak postup testování lze použít s určitými obměnami i pro platformu PC a LAN připojení. Aplikace pro testování byla vytvořena ve vývojovém prostředí Android Studio – jedná se o modul, který lze integrovat do jiných aplikací, vyžadující pro svoji funkčnost spolehlivé síťové připojení.

Annotation

Title: Module for testing network throughput

The bachelor thesis describes application for testing network throughput and network connection stability. The application is a module it is testing connection in periodical intervals and it evaluates their stability and usability for communication and data transferring according several aspects. The test of the connection is complex – it contains some subtests (network connection presence, stability, speed, latency, etc.). Using of the module is focused to integration in application for mobile devices (with Wi-Fi connection or cellular data network) but the testing process is also ready for using on PC platform and LAN connection. The application has been created in IDE Android Studio – it is a module and it can be integrated to any other application which needs reliable network connection for its functionality.

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Oblast počítačových sítí zažívá v několika posledních letech obrovský rozvoj. Je součástí běžného života každého z nás, aniž bychom si to uvědomovali. Nejedná se přitom pouze o záležitost komerční sféry, ale i prostředí domácností. Nedostupnost internetového připojení způsobí u většiny dnešní elektroniky velmi omezenou funkčnost a sníženou použitelnost. Toto se týká počítačů, přenosných zařízení (tablety, mobilní telefony, chytré hodinky atd.), ale samozřejmě i elementů, poskytující služby ostatním uživatelům – firemní servery a datová centra.
Postupem času dochází ke zvyšování nároků na kvalitu síťového připojení kvůli provozu náročných aplikací, vyžadujících rychlý přenos velkých objemů dat, vysokou dostupnost a stabilitu. Požadavky stále narůstají, nicméně spolehlivé připojení k internetu nelze ani v dnešní době v některých případech považovat za samozřejmost, především pak u mobilních zařízení. Uživatel je často závislý na nepříliš stabilní datové konektivitě svého mobilního operátora, kde nelze zaručit bezproblémovost a kvalitu přenosu. Na případné problémy tohoto typu je nutné být v době rozmachu využívání „chytrých zařízení“ připraven a brát je v potaz.

Tato bakalářská práce popisuje základní pojmy síťové terminologie, metody měření sítě včetně popisu jednotlivých typů testů. Na základě těchto poznatků je vypracován postup pro testování chování sítě a měření její propustnosti. Vlastní navržené řešení je popsáno a zdůvodněno.
Postup je poté implementován v programovacím jazyce Java pro platformu mobilních zařízení s operačním systémem Android. Výsledkem implementace je mobilní aplikace, která dokáže otestovat propustnost sítě na základě dříve vypracovaného řešení testování.
Další část tvoří průběh samotného testování. Pro relevantnost je test opakován několikrát s různými koncovými zařízeními (příp. verzí operačního systému atd.).
Výsledky testů jsou porovnány a vyhodnoceny. Na základě výsledků je navrženo vylepšení postupu pro testování tak, aby test podával co nejpřesnější informace o reálném stavu sítě.

2 Základní terminologie oblasti počítačových sítí

Základní definice

Počítačová síť tvoří spojení mezi dvěma a více body (zařízeními) za účelem zajištění vzájemné komunikace a sdílení informací. Prostředky, kterými je spojení realizováno, umožňují koncovým bodům mezi sebou komunikovat podle předem daných pravidel. Sada těchto pravidel se nazývá protokol. Výměna zpráv mezi dvěma zařízeními probíhá skrze síťové prvky, kterými jsou koncové body vzájemně propojeny. *Celosvětovou globální počítačovou sítí je Internet, kam je připojena většina ostatních sítí (privátních či firemních)*. (1)

2.1 Základní rozdělení počítačových sítí

Rozdělení popisuje typy sítí podle jejich geografického rozsahu a použití.

PAN – Personal Area Network

Jedná se o sítě velmi malého rozsahu (typicky 1 místnost), sloužící pro spojení osobních zařízení, například mobilního telefonu, tabletu, přenosného počítače atd. *Často se zde používá bezdrátová technologie Bluetooth, případně Wi-Fi, kde realizace propojení zpravidla nevyžaduje hlubší znalosti v oblasti konfigurace sítí*. (2)

LAN – Local Area Network

Jde o nejpoužívanější typ sítě používaný pro spojení zařízení v rámci kanceláře, domácnosti nebo budovy. Zahrnuje v sobě i bezdrátové spojení zařízení pomocí technologie Wi-Fi (Wireless LAN, WLAN). Koncový uzel v tomto případě reprezentuje uživatelská stanice, server, tiskárna, síťové úložiště. *Komunikace v moderních LAN sítích probíhá nejčastěji podle protokolu Ethernet, typickým přenosovým médiem je metalická kabeláž.* (3)

MAN – Metropolitan Area Network

Slouží pro realizaci přechodu mezi LAN a WAN sítěmi. Používá se nejčastěji k propojení sítí v rámci města nebo pro spojení univerzitního kampusu. Jako přenosové médium je obvykle používán optický kabel.

WAN – Wide Area Network

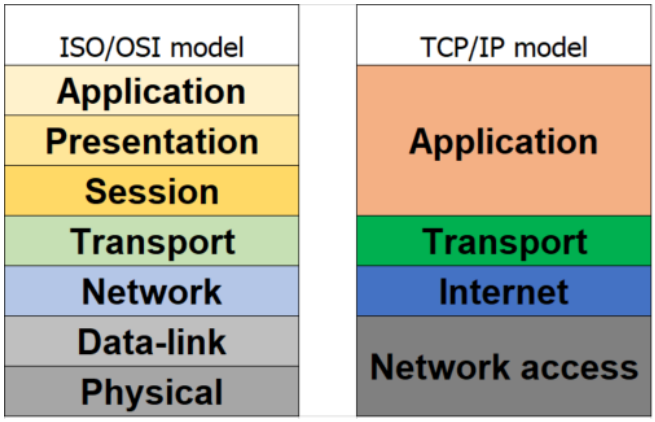
WAN sítě jsou využívány k realizaci spojení mezi LAN sítěmi. Příkladem WAN sítě je Internet. Zde se využívají síťová zařízení (jejich počet může být až několik desítek), která zajišťují směrování dat mezi sítěmi a zabezpečují tak doručení do požadovaného cíle.

2.2 Síťové modely

Z důvodu zvyšování složitosti struktury sítí bylo nutné vnitřní procesy rozdělit na několik částí (vrstev). Do nich lze zařadit i jednotlivý hardware a software používaný při realizaci síťové komunikace. *Model vrstev umožňuje celou síť lépe pochopit, urychluje řešení případných problémů a usnadňuje vývoj a návrh síťových aplikací – každá vrstva pracuje s příslušnými protokoly.* (1)

ISO/OSI model

Autorem ISO/OSI síťového modelu (Obrázek 1) je organizace ISO. Jedná se o standard pro průběh komunikace v počítačových sítích. ISO/OSI model má 7 vrstev, každá z nich poskytuje své služby vyšší vrstvě a provede určitou modifikaci dat (přidání hlavičky, rozdělení do segmentů atd.).



Obrázek 1 – Porovnání ISO/OSI modelu (vlevo) a TCP/IP modelu (vpravo)
Zdroj: Vlastní tvorba

TCP/IP model

TCP/IP model popisuje fungování síťového software. Oproti ISO/OSI modelu se skládá pouze ze 4 vrstev. Jeho aplikační vrstva zahrnuje veškeré služby aplikačních protokolů, interakci s uživatelem, udržování spojení. Transportní vrstva zajišťuje doručení segmentů dat mezi zdrojovou a cílovou aplikací (stejná funkčnost jako transportní vrstva u ISO/OSI modelu). Síťová vrstva provádí směrování paketů mezi sítěmi pomocí logické adresace. Nejnižší vrstva sítového přístupu nese odpovědnost za doručení paketů v rámci stejné sítě, za fyzický přenos dat po síťovém médiu a kódování signálu. *Najdeme zde používané protokoly ARP, PPP nebo Ethernet*. (4)

2.3 Základní síťové prvky

Repeater

Obrázek 2 – Repeater
Zdroj: https://www.cisco.com

Repeater (opakovač) přijímá signál, zesiluje jej a vysílá jej dál. Uplatnění nachází především při použití delších vodičů, kde je vyšší riziko slábnutí signálu a tím i pokles kvality přenosu. Pracuje pouze na fyzické vrstvě.

Hub

Obrázek 3 – Hub
Zdroj: https://www.cisco.com

Hub je jednoduché síťové zařízení, které provádí přeposlání příchozího signálu na všechny porty s výjimkou toho, ze kterého byl signál přijat. Rozděluje kolizní doménu.

Bridge

Obrázek 4 – Bridge
Zdroj: https://www.cisco.com

Bridge (síťový most) spojuje 2 segmenty sítě. Ve své paměti si udržuje tabulku MAC adres, na základě které poté provádí předávání dat. Pracuje na linkové vrstvě a rozděluje kolizní doménu.

Switch

Obrázek 5 – Switch
Zdroj: https://www.cisco.com

Přepínač neboli switch je dnes nejčastěji používán pro propojení koncových zařízení sítě (stanice, tiskárny, servery). Stejně jako bridge si udržuje v paměti přehled spojení „MAC adresa + fyzický port“. Z těchto údajů vytváří tzv. CAM tabulku (Content Addressable Memory), podle které data přeposílá. Switche mohou disponovat různým počtem portů – od nejmenších modelů určených pro domácí použití se 4 porty až po modulární řady switchů s několika stovkami portů. *Stejně jako bridge, i switch pracuje na 2. vrstvě ISO/OSI modelu (s výjimkou Layer 3 switchů s možností statického směrování). Rozděluje kolizní doménu.* (5) Konfigurovatelné switche umožňují dále seskupovat své porty do tzv. VLAN (Virtual LAN). *Každá VLAN má přiřazen identifikátor a pakety mohou být přepínány mohou být z jednoho*

síťového segmentu zasílány do jiného pouze v případě, pokud oba segmenty mají stejný identifikátor VLAN. (6)

Router

Obrázek 6 – Router
Zdroj: https://www.cisco.com

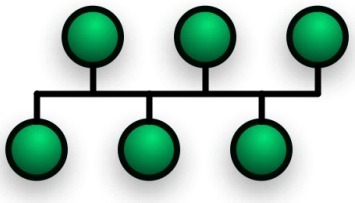
Router (označován také jako směrovač) provádí přeposílání dat mezi jednotlivými sítěmi. *Routovací tabulka, podle které se směrování provádí, v sobě obsahuje záznamy o připojených či vzdálených sítích a IP adresu sousedního routeru (případně fyzické rozhraní), přes který se do této sítě lze dostat. Směrovač pracuje na síťové vrstvě a rozděluje broadcastovou doménu.* (5)

2.4 Topologie sítí

Topologie sítě znázorňuje její fyzickou či logickou strukturu. Fyzická topologie zobrazuje propojení zařízení mezi sebou, zatímco v logické topologii lze vidět cesty a toky dat.
Existuje několik nejpoužívanějších síťových topologií, které se od sebe liší složitostí, náročností na instalaci, redundancí, počtem potřebných síťových prvků atd.

Bus

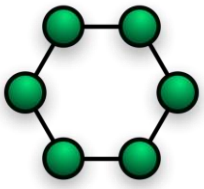
- Centrální médium je pouze jedno jediné (sdílená linka)
- K médiu jsou koncová zařízení připojena pomocí odboček
- Časté použití koaxiálního kabelu
- Riziko kolize při současném vysílání více stanic
- Při potřebě použití delšího síťového média je nutné zesílení signálu
- Bez možnosti redundance spojení



Obrázek 7 - Topologie "Bus"
Zdroj: https://commons.wikimedia.org

Ring

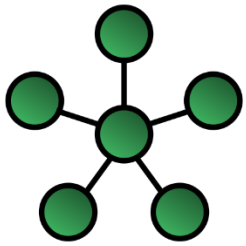
- Každé zařízení je spojeno se svým sousedem
- Spojená zařízení dohromady vytváří „kruh“
- Data se předávají pouze v jednom směru
- Zařízení si mezi sebou předávají tzv. „token“ – pouze ten, kdo ho má, může vysílat data



Obrázek 8 - Topologie "Ring"
Zdroj: https://commons.wikimedia.org

Star

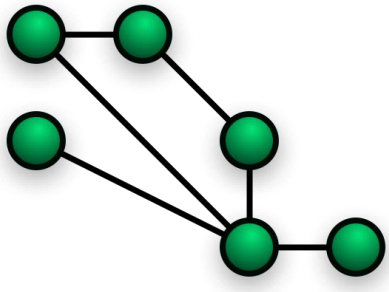
- Všechna koncová zařízení jsou spojena pomocí centrálního prvku
- Při poruše centrálního prvku je mimo provoz celá síť
- Centrální prvek je reprezentován nejčastěji switchem (dříve hubem)
- Nejčastěji používaná topologie v kancelářích a domácnostech
- Jednoduchá implementace



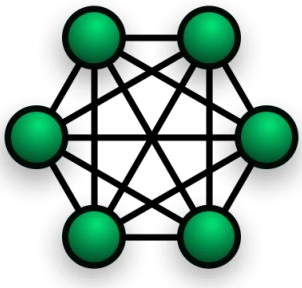
Obrázek 9 - Topologie "Star"
Zdroj: https://commons.wikimedia.org

Mesh

- Topologie využívaná ve WAN sítích (např. v Internetu)
- Do každého cíle se lze dostat několika cestami (redudance)
- Full-mesh, fully-connected ➔ speciální typ „Mesh“ topologie – každé zařízení má přímé spojení se všemi ostatními prvky



Obrázek 10 - Topologie "Mesh"
Zdroj: https://commons.wikimedia.org



Obrázek 11 - Topologie "Full-mesh"
Zdroj: https://commons.wikimedia.org

2.5 Síťové protokoly

Protokol je sada pravidel, které musí být při přenosu dat dodrženy. Protokoly mohou být otevřené (dostupné pro všechny) nebo proprietární (vyvíjené a používané pouze jedním výrobcem).

2.5.1 Linková vrstva OSI modelu

Ethernet

Protokol Ethernet popisuje přenos dat v rámci jednoho segmentu sítě. Data jsou rozdělena do částí a zapouzdřena do tzv. rámců (frames). Ethernet pracuje na technologii CSMA/CD (metoda detekování kolize). V dnešní době existuje několik verzí Ethernetu (Fast Ethernet, Gigabit Ethernet, 10Gigabit Ethernet), lišící se především v rychlosti přenosu dat.

ARP

Address Resolution Protocol zajišťuje získání MAC adresy ke konkrétní IP adrese. *Při potřebě komunikace zařízení A se zařízením B vyšle zdrojové zařízení zprávu pomocí broadcastu o zjištění konkrétní IP adresy. Na tuto zprávu odpoví zařízení, které má na svém síťovém adaptéru přiřazenou hledanou IP adresu. Pokud cíl není v segmentu, odpoví na žádost router (výchozí brána).* (7)

2.5.2 Síťová vrstva OSI modelu

IP

Internet Protocol, popisuje směrování dat mezi síťovými segmenty (proces routování), logickou adresaci sítě (pomocí IP adres). Data jsou zapouzdřena do paketů. Protokol dělíme na verze IPv4 a IPv6, liší se v počtu použitelných IP adres a způsobu jejich přidělování.

ICMP

ICMP je servisní protokol pro IP protokol. Poskytuje diagnostické nástroje a přenáší chybové hlášení při přenosu. Může být použit k otestování dostupnosti bodu v síti, měření latence, výpisu cesty do jiného bodu. *Chybovými kódy upozorňuje na překročení hodnoty TTL, nedostupnosti cílového bodu nebo neexistující záznam v routovací tabulce směrovače*. (8)

2.5.3 Transportní vrstva OSI modelu

TCP

Transmission Control Protocol – transportní protokol, který zajišťuje spojení typu klient-server. Je používán pro aplikace s požadavkem na bezchybný a spolehlivý přenos dat. Po přijetí každého segmentu dat je zkontrolována integrita dat pomocí atributu kontrolního součtu (checksum). Pokud je packet v pořádku, je odeslán ACK (acknowledgement) packet. *Navázání samotného spojení dvou bodů je provedeno pomocí tzv. 3-way handshake (SYN, SYN-ACK, ACK paket). Nevýhodou TCP protokolu je vyšší režie a tím i nižší rychlost přenosu. Velikost TCP hlavičky je 20 bytů. Používán je u aplikačních protokolů HTTP, FTP, SSH atd.* (7)

UDP

User Datagram Protocol – transportní protokol určený pro rychlé zasílání zpráv. Jedná se o tzv. nespojový protokol, nepoužívá navazování spojení s druhou stranou. Z tohoto důvodu disponuje rychlejším přenosem než TCP protokol. *Velikost hlavičky UDP je 8 bytů. Používá se u aplikačních protokolů DHCP, DNS, případně VoIP služeb.* (7)

2.5.4 Relační vrstva OSI modelu

NetBIOS

Network Basic Input Output Systém – poskytuje aplikační rozhraní (API) pro přístup ke vzdáleným počítačům a souborům, která jsou v nich uložena. *Pro připojení k PC jsou použity tzv. NetBIOS názvy. Pomocí tohoto názvu lze kontaktovat buď konkrétní stanici nebo celou skupinu (vysílání typu multicast). Ve své základní podobě funguje tento protokol pouze v rámci místní sítě a není routovaný.* (9)

2.5.5 Prezentační vrstva OSI modelu

SSL

Secure Socket Layer – protokol používaný pro šifrování komunikace mezi dvěma systémy. Zajišťuje zabezpečenou komunikaci mezi klientem a serverem a znemožňuje odposlouchávání síťového provozu. *Server odešle po připojení klienta certifikát a veřejnou část svého klíče. Klient ověří, zda je certifikát platný, jeho název se shoduje s názvem serveru a byl vydán důvěryhodnou certifikační autoritou. Pokud*

jsou tyto podmínky splněny, klient zašifruje data a odešle je serveru. Ten provede dešifrování pomocí privátní části svého klíče. (8) Typickým příkladem využití SSL je zabezpečené prohlížení webových stránek pomocí HTTPS protokolu.

2.5.6 Aplikační vrstva OSI modelu

HTTP

Hypertext Transfer Protocol – aplikační protokol sloužící k přenosu webových stránek. Web je fyzicky umístěn na webovém serveru a na klientské stanici ho lze zobrazit pomocí prohlížeče. HTTP je bezestavový protokol – po dokončení přenosu dat je relace ukončena. Klient a server přenášejí HTTP data pomocí požadavků (GET – požadavek klienta na získání konkrétní stránky, POST – nahraje data na webový server, HEAD – požadavek klienta na získání hlavičky webu). (9) Weby a jejich části jsou identifikovány pomocí tzv. URL adres, ty jsou složeny z domény a cesty, kde se požadovaný HTML soubor nachází. Šifrovaná varianta protokolu je HTTPS.

SMTP

Simple Mail Transfer Protocol – protokol umožňující přenášet e-mailové zprávy mezi servery. SMTP server naslouchá a čeká na započetí komunikace s klientem. *Použitím e-mailového klienta (MUA – Mail User Agent) nebo pomocí speciálních příkazů je možné zprávu ze serveru odeslat příjemci. Jiný server tuto zprávu přijme a uloží ji do schránky (MDA – Mail Delivery Agent), je tedy k dispozici pro přečtení příjemcem protokolem POP3 nebo IMAP*. (9) SMTP protokol implementují programy označované jako MTA (Mail Transfer Agent). Zabezpečenou verzí SMTP je SMTPS.

2.6 Základní síťové procesy

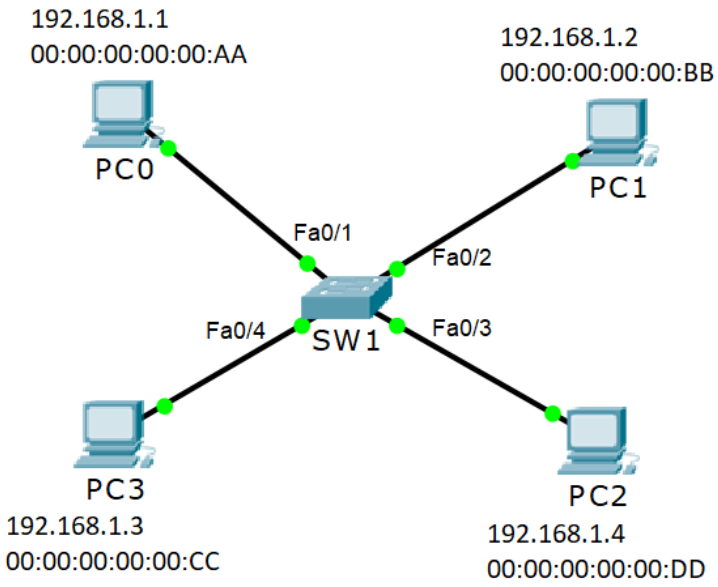
Síťové procesy popisují přenos dat z jednoho bodu do druhého. Liší se podle toho, zda jsou oba body umístěné ve stejné síti nebo ne. Tato kapitola vysvětluje dva nejpoužívanější postupy – přepínání a směrování.

2.6.1 Přepínání (switching)

Proces přepínání realizuje přenos dat v rámci jednoho segmentu sítě mezi koncovými body, identifikovanými MAC adresami. Jedná se o přenos na spojové vrstvě OSI modelu a je zprostředkován přepínačem (switchem).

V dnešní době se nejčastěji používá zapojení stanic v topologii hvězda (star). Počítačové sítě používají switche pro zajištění komunikace mezi hosty. Switch je zařízení s určitým množstvím vstupů a výstupů vedoucí ke každé zapojené stanici. (6)

Model sítě (Obrázek 12) zobrazuje typickou přepínanou síť.



Obrázek 12 - Model přepínané sítě
Zdroj: Vytvořeno pomocí SW Cisco Packet Tracer

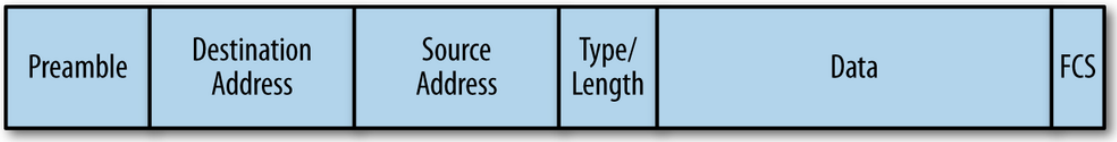
Popis procesu komunikace ze stanice PC0 do PC1

Při popisu je předpokládáno, že všechna zařízení byla právě zapnuta a nemají tedy uchované žádné další informace získané ze síťového provozu. Stanice mají přiřazeny uvedené IP adresy.

Pokud by předem byla známa pouze IP adresa cílové stanice, nikoliv MAC adresa, je nutné jí zjistit pomocí ARP dotazu.

1) PC0 provede vytvoří Ethernetový rámec se zdrojovou MAC adresou svého síťového adaptéru (AA) a cílovou MAC adresou počítače PC1 (BB).
2) PC0 tento rámec odešle skrze síťovou kartu.
3) Switch rámec přijme (na rozhraní Fa0/1) a hledá pro cílovou MAC adresu záznam ve své CAM tabulce. Protože je zatím prázdná a nemá tedy k portu Fa0/1 přiřazenou žádnou MAC adresu, vznikne v CAM tabulce nový záznam pro tento port s MAC adresou AA.
4) Switch nemá v CAM tabulce žádný záznam pro cílovou MAC adresu rámce (BB), rozešle proto rámec na všechna svá rozhraní kromě toho, na kterém byl rámec přijat pomocí broadcastového vysílání (Fa0/2, Fa0/3, Fa0/4).
5) Každá stanice připojená ke switchi musí přijatý rámec zpracovat a porovnat jeho cílovou MAC adresu (BB) s MAC adresou svého síťového adaptéru.
6) Stanice, jejichž MAC adresa se neshoduje s cílovou MAC adresou přijatého rámce (BB), rámec zahodí (PC3, PC4).
7) Stejným postupem při komunikaci z jiných stanic si switch doplní svoji CAM tabulku záznamy pro ostatní porty. Po naplnění tabulky tedy switch neprovádí rozesílání broadcastu, ale odesílá rámec pouze na port s cílovým zařízením.

Popis Ethernetového rámce



Obrázek 13 - Ethernetový rámec
Zdroj: https://www.safaribooksonline.com

Preamble – Slouží pro rozlišení rámců

Destination address – MAC adresa cílové stanice

Source address – MAC adresa zdrojové stanice

Type/length – určuje protokol, kterým jsou data zapouzdřena, případně velikost dat

Data – samotná data rámce

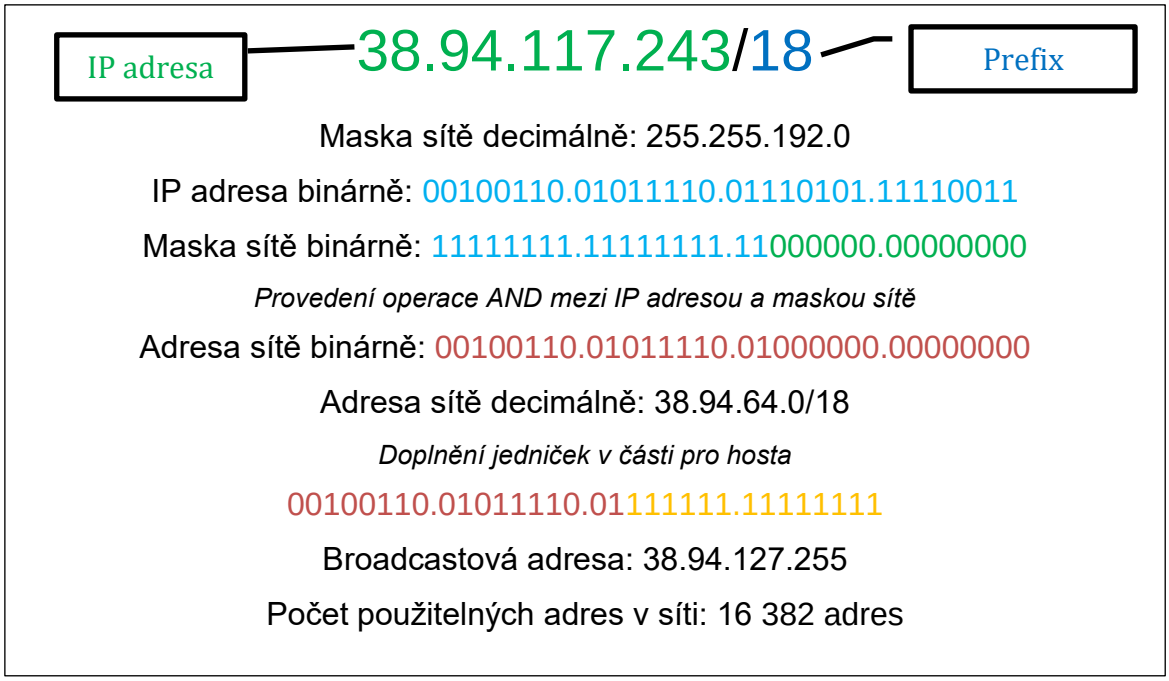
FCS – kontrolní součet rámce

2.6.2 Směrování (routing)

Proces přepínání je využíván v situacích, kdy je nutné přenášet data mezi různými sítěmi. Pracuje na síťové vrstvě OSI modelu a pro adresaci se využívají IP adresy.

2.6.2.1 IP adresy

IP adresa je 32bitové číslo u protokolu IPv4 (resp. 128bitové číslo u protokolu IPv6), které je rozděleno na 4 části (oktety, odděleny tečkami – např. 74.65.91.207). V rámci jedné sítě musí mít každé zařízení unikátní IP adresu. Nezbytnou součástí IP adresy je maska sítě. Jedná se o údaj, který určuje rozdělení IP adresy na síťovou část a část pro hosta.



IP adresy dělíme na 2 typy – veřejné a privátní. Veřejné IP adresy jsou používány pro identifikaci počítače v celém Internetu, zatímco privátní pouze v rámci jedné sítě a IP adresy z těchto rozsahů nejsou směrovány do prostředí Internetu.

Privátní IP rozsahy

Tabulka 1 - přehled privátních IP rozsahů

Rozsah	Maska sítě	Počet použitelných adres
10.0.0.0/8	255.0.0.0	16 777 214
172.16.0.0/12	255.240.0.0	1 048 574
192.168.0.0/16	255.255.0.0	65 534

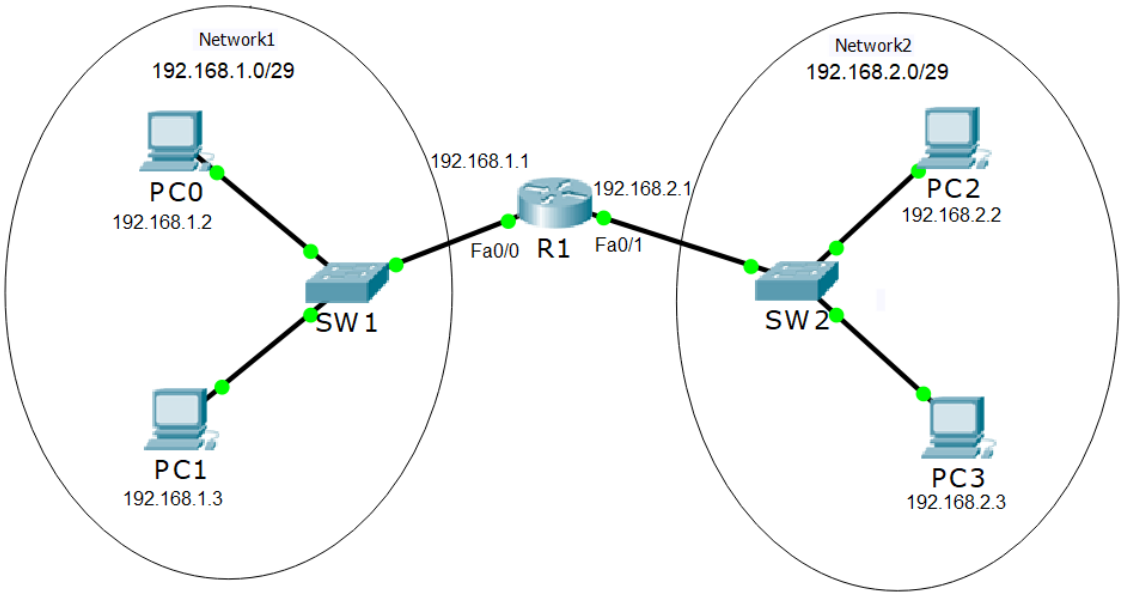
2.6.2.2 Třídy IP adres

IP adresy je také možné rozdělit do tříd, které určují masku dané sítě

Tabulka 2 - přehled tříd IP adres

Třída	Rozsah adres	Maska	Poznámka
Třída A	0 – 127.x.x.x	255.0.0.0	Používáno
Třída B	128 – 191.x.x.x	255.255.0.0	Používáno
Třída C	192 – 223.x.x.x	255.255.255.0	Používáno
Třída D	224 – 239.x.x.x	Rezervovaný rozsah pro multicast vysílání	
Třída E	240 – 255.x.x.x	Rozsah pro experimentální a vývojové účely	

Příklad směrování (routingu) bude znázorněn na modelu sítě (Obrázek 14):



Obrázek 14 - Model směrované sítě
Zdroj: Vytvořeno pomocí SW Cisco Packet Tracer

Popis procesu komunikace ze stanice PC0 do PC2

Při popisu je předpokládáno, že všechna zařízení byla právě zapnuta a nemají tedy uchované žádné další informace získané ze síťového provozu. Router má zapnutá obě rozhraní pro spojení se switchi, stanice a rozhraní routeru mají přiřazeny uvedené IP adresy, stanice mají informaci o výchozí bráně – rozhraní routeru.

1) PC0 vytvoří IP paket se zdrojovou IP adresou svého síťového adaptéru (192.168.1.2) a cílovou IP adresou počítače PC2 (192.168.2.2).
2) Počítač provede operaci logického součinu AND mezi cílovou IP adresou paketu a maskou sítě, ve které se PC0 nachází. Tím zjistí, že cílový počítač se nachází v jiné síti a je nutné paket odeslat výchozí bráně.
3) Paket je zabalen do Ethernetového rámce (cílovou MAC adresou bude adresa rozhraní Fa0/0 routeru R1) a je odeslán prostřednictvím síťového adaptéru (viz předchozí kapitola).
4) Router R1 přijme paket na rozhraní Fa0/0. Projde svoji routovací tabulku, kde má 2 záznamy o připojených sítích (viz Obrázek 15).
5) Zde nalezne záznam o síti 192.168.2.0/29, která je připojena na rozhraní Fa0/1 routeru R1.
6) Paket je odeslán z tohoto rozhraní a jeho hodnota TTL je snížena o 1.
7) Router pomocí ARP dotazu zjistí z cílové IP adresy i MAC adresu cílového počítače, paket zabalí do rámce a odešle ho z rozhraní Fa0/1 do switche SW2.
8) Switch SW2 rámec přijme a podle cílové MAC adresy jej odešle počítači PC2.

```
     192.168.1.0/29 is subnetted, 1 subnets
C       192.168.1.0 is directly connected,
FastEthernet0/0
     192.168.2.0/29 is subnetted, 1 subnets
C       192.168.2.0 is directly connected,
FastEthernet0/1
Router#
```

Obrázek 15 - Routovací tabulka routeru R1
Zdroj: Vytvořeno pomocí SW Cisco Packet Tracer

2.7 Bezdrátové sítě

Bezdrátovou sítí se rozumí propojení zařízení bez použití kabelu jako přenosového média. Oba přístroje musí podporovat danou bezdrátovou technologii a mít v sobě implementovanou potřebnou vysílací nebo přijímací část, která bude komunikaci zajišťovat. Technologie pro tento typ přenosu zažívají v posledních letech velký rozmach zejména z důvodu snadné instalace a minimální nutnosti konfigurace zařízení, což je využitelné především u přenosných mobilních zařízení a domácí elektroniky (chytré mobilní telefony, tablety, chytré hodinky, televizory, multimediální přehrávače atd.).

2.7.1 Technologie pro bezdrátový přenos

Následující přehled popisuje technologie, které se v dnešní době nejvíce využívají pro realizaci bezdrátového přenosu mezi zařízeními.

Bluetooth

- Poskytuje přenos dat na krátkou vzdálenost (několik metrů)
- Pracuje ve frekvenčním pásmu 2,4 GHz
- Umožňuje přenášet data i hlas (využití pro VoIP telefonii)
- Podporován mobilními telefony, notebooky a bezdrátovými periferiemi (počítačová myš, klávesnice, bezdrátový reproduktor)

WiMAX

- *Používán pro vysokorychlostní bezdrátové spoje mezi statickými body – propojení budov (spojení point to multi-point)* (10)
- Pracuje na principu mikrovlnného přenosu
- *Využívá frekvenčního rozsahu 2-11 GHz* (10)

Celulární sítě (WWAN)

- *Poskytují bezdrátový přenos dat v širokém geografickém rozsahu* (11)
- *Oblast vysílání a příjmu signálu je geograficky rozdělena do tzv. buněk pracujících na rozdílných frekvencích* (11)

- Vysílací dosah buňky je v řádu desítek km (závisí na frekvenci)
- Koncové zařízení je obslouženo buňkou v nejkratší vzdálenosti
- Rozděleno do několika generací (liší se především rychlostí připojení) – AMPS, CDMA, GPRS, 3G (UMTS), 4G (LTE)

Wi-Fi

- Využívá standard IEEE 802.11 a přístupovou metodu CSMA/CA
- Nejpoužívanější technologie pro bezdrátový přenos
- Podporované téměř všemi typy mobilních zařízení a domácí elektroniky
- Pracuje ve frekvenčních pásmech 2,4 GHz, 5 GHz (závisí na variantě)
- Existuje několik generací Wi-Fi sítí (802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ad)
- *Přístupové body (AP) připojují bezdrátové klienty (koncová zařízení) do LAN sítě – klienti spolu navzájem nekomunikují přímo, ale skrze AP* (12)

Proces připojení zařízení

1) Přístupový bod (AP) vysílá tzv. „beacon“ rámce, kterými propaguje bezdrátovou síť pro ostatní zařízení (rámec obsahuje SSID sítě a typ zabezpečení sítě)
2) Klient hledá vhodnou Wi-Fi síť vysíláním „probe requests“ na různých kanálech (rámec obsahuje SSID požadované sítě)
3) Přístupový bod odešle „probe response“ rámec jako odpověď na požadavek klienta. V něm odesílá informace o SSID sítě a typ zabezpečení sítě)
4) Proces pokračuje autentizací klienta. Pokud je síť otevřená (bez zabezpečení), žádost o autentizaci je vždy přijata. V případě zabezpečené sítě klient odešle rámec s typem zabezpečení a sdíleným klíčem.
5) Přístupový bod odešle odpověď na žádost o autentizaci. V ní je obsažen typ zabezpečení, sdílený klíč a informace, zda byla žádost potvrzena nebo zamítnuta.

6) Poslední částí přenosu je asociace klienta. Ten odešle „association request“ obsahující MAC adresu klienta (resp. jeho bezdrátové síťové karty), MAC adresu přístupového bodu (BSSID) a ESS identifikátor.
7) Přístupový bod odešle klientovi odpověď s informací o potvrzení, či zamítnutí žádosti.

(12)

Měření síly signálu Wi-Fi

Metody zabezpečení

Z důvodu neizolované komunikace je nutné bezdrátové připojení zabezpečit kvůli prevenci průniku útočníků do sítě. Následující způsoby se používají pro šifrování komunikace mezi klientem a přístupovým bodem:

- WEP – Jde o nejstarší zabezpečovací protokol, používaný v letech 1999-2004. Z bezpečnostního hlediska je však nedostačující kvůli použití jediného statického klíče pro šifrování veškeré komunikace (na rozdíl od novějších protokolů). Díky tomu lze klíč při odposlechu několika zašifrovaných paketů snadno dopočítat. V dnešní době se protokol WEP již nepoužívá.
- WPA – Nástupce protokolu WEP nabízel zvýšenou úroveň bezpečnosti zajištěnou zejména použitím předsdíleného klíče (PSK) pouze pro připojení k síti. Pomocí technologie TKIP byla pro každého klienta vygenerována sada klíčů, které se mění. Bezpečnost závisí především na komplexitě použitého předsdíleného klíče.
- WPA2 – Náhrada protokolu WPA. Hlavní změnou je podpora silnějšího šifrovacího protokolu AES. Ten poskytuje symetrické blokové šifrování pomocí 128, 192 nebo 256 bitového klíče.
- WPA/WPA2 Enterprise – Jedná se o zabezpečení přístupu k síti s využitím autentizačního serveru RADIUS namísto použití sdíleného klíče PSK. Tato metoda ověřování je určena především pro firemní prostředí s centrální správou identity uživatelů. Tím je znemožněno prozrazení sdíleného klíče

pro připojení (každý uživatel nebo zařízení používá své vlastní přístupové údaje).

Kromě těchto metod se pro zabezpečení přístup k síti používá metoda vypnutí vysílání SSID (identifikátor sítě) nebo filtrování na základě MAC adres zařízení. *Manuálně vytvořená tabulka adres na přístupovém bodu slouží k povolení nebo zakázání přístupu na základě fyzické adresy síťového hardwaru.* (12)

2.8 Metody měření sítě

V dnešní době existuje celá řada testů rychlosti dostupných na Internetu, které otestují rychlost stahování a odesílání dat. Toto však není jediný ukazatel stabilního připojení. Síť může být přetížena na jakémkoli uzlu kvůli vysoké zátěži, problémům s hardwarem nebo síťovým útokům. (13) Spolehlivé určení kvality připojení je tedy prováděno kombinací několika metod měření.

2.8.1 Měření latence a test dostupnosti hostitele (test ICMP ping)

Pro testování dostupnosti hostitele se nejčastěji používá nástroj protokolu ICMP – ping. Je obsažen ve všech operačních systémech a poskytuje jednoduchou možnost otestovat dostupnost a zpoždění (latenci) přenosu mezi místním a vzdáleným zařízením. *Latence je čas mezi odesláním dat ze zdrojového do cílového bodu.* (13) Nástroj ping vyžaduje jako parametr DNS název nebo IP adresu vzdáleného zařízení, dále lze určit velikost testovacího paketu (OS Windows ve výchozím nastavení odesílá paket o velikosti 32 bytů, unixové operační systémy velikost 56 bytů), maximální povolený čas pro odpověď a další parametry.

Pro svoji funkčnost využívá ICMP pakety typu „Echo request" (typ 0), vzdálený počítač na tyto žádostí odpovídá pomocí „Echo reply" (typ 8). (8)

Výsledný čas latence je rozdílem mezi časem odeslání paketu s žádostí o odezvu a časem přijetí odpovědi. (12)

```
root@server ~ # ping 8.8.4.4
PING 8.8.4.4 (8.8.4.4) 56(84) bytes of data.
64 bytes from 8.8.4.4: icmp_seq=1 ttl=57 time=7.99 ms
64 bytes from 8.8.4.4: icmp_seq=2 ttl=57 time=8.21 ms
64 bytes from 8.8.4.4: icmp_seq=3 ttl=57 time=8.17 ms
64 bytes from 8.8.4.4: icmp_seq=4 ttl=57 time=11.4 ms
^C
--- 8.8.4.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 7.992/8.952/11.429/1.436 ms
```

Obrázek 16 - Testování dostupnosti vzdáleného serveru nástrojem ping
Zdroj: Vlastní tvorba (systém Debian Linux)

Jitter

Při měření je také často udávána hodnota jitteru, která vyjadřuje průměrnou hodnotu rozdílů mezi jednotlivými naměřenými hodnotami ping testu.

Výpočet jitteru t_j lze provést následujícím způsobem:

$$n = počet\ úspěšně\ přijatých\ ping\ paketů$$

$$t_1 \dots t_n = hodnoty\ latence\ úspěšně\ přijatých\ ping\ paketů$$

$$t_j = \frac{\sum_{k=1}^{n-1} |t_k - t_{k+1}|}{n}$$

2.8.2 TCP connection test (TCP socket test)

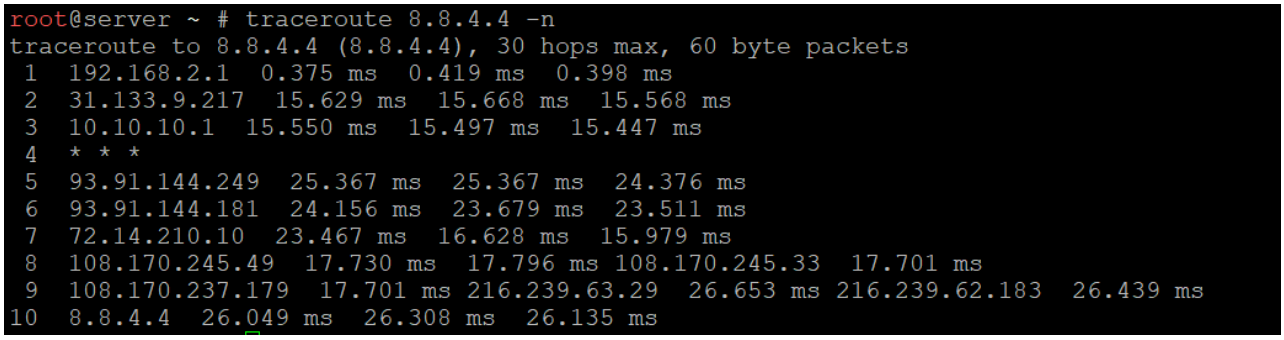
Tento typ testu se často používá jako náhrada za ICMP ping test pro otestování dostupnosti vzdáleného hostitele. Na rozdíl od nástroje ping nepoužívá servisní protokol ICMP, ale standardní TCP. Díky tomu je použitelný i tam, kde je ICMP protokol nepoužitelný (např. je blokován bránou firewall).

2.8.3 Zjištění cesty k hostiteli (test ICMP traceroute)

Nástroj traceroute (v OS Windows pod názvem tracert) slouží pro zjištění všech routerů po cestě z místního počítače ke vzdálenému cíli. Princip testu spočívá v zasílání paketů a postupným zvyšováním hodnoty TTL u každého dalšího paketu. Pokud je TTL hodnota paketu rovna nule, router paket zahodí a odešle zdrojovému počítači ICMP zprávu typu 11 (TTL exceeded). První paket je po začátku testu odeslán s TTL hodnotou 1.

Opakováním tohoto postupu se zdrojový PC dozví o všech routerech, přes které paket prochází do cíle. Je však nutné, aby routery ICMP pakety neblokovaly.

Stejně jako nástroj ping, i traceroute vyžaduje jako parametr minimálně DNS název nebo IP adresu vzdáleného serveru.

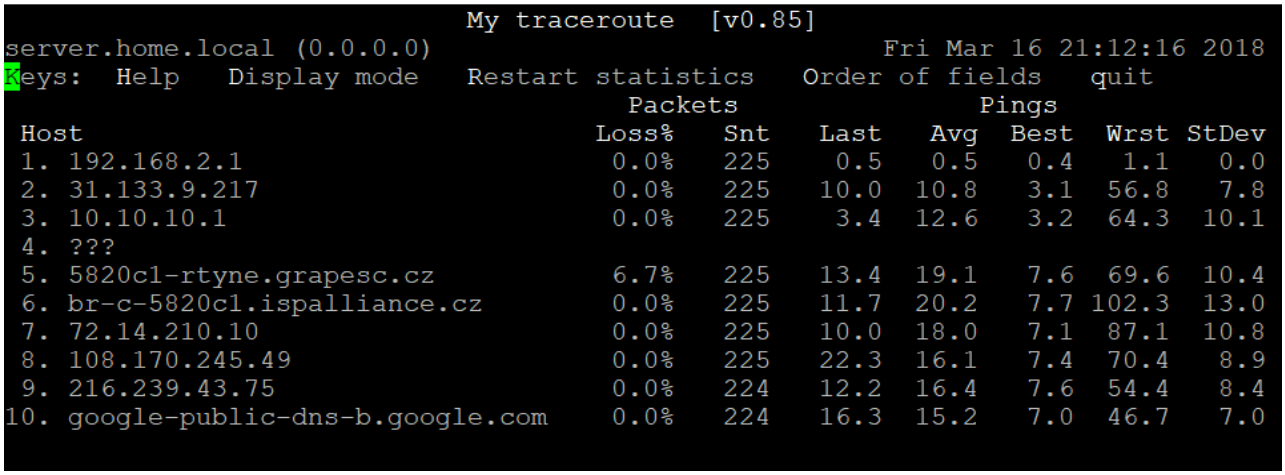


Obrázek 17 - Zjištění cesty k hostiteli nástrojem traceroute
Zdroj: Vlastní tvorba (systém Debian Linux)

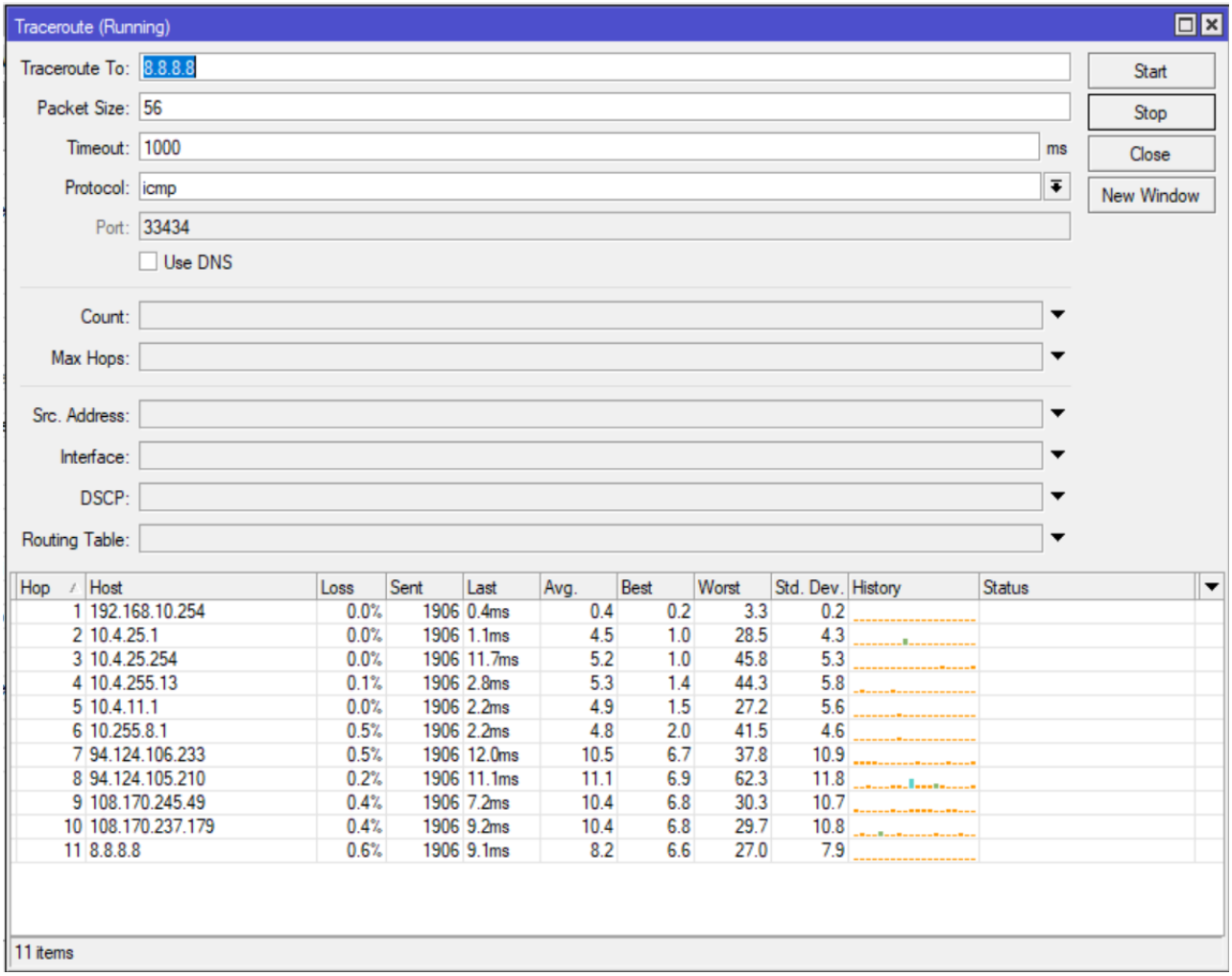
2.8.4 MTR test (My Traceroute, Matt's traceroute)

MTR test je kombinací dvou předchozích metod měření ping a traceroute. Nejprve je provedeno trasování a zjištění routerů (hopů) po cestě k hostiteli. Následně je spuštěn ping test na všechny hopy po cestě najednou. *Standardně je program mtr vestavěn ve všech unixových systémech a lze ho zprovoznit i v ostatních operačních systémech.* (14)

MTR test nachází uplatnění při řešení problémů se zpožděním na trase – umožňuje rychle a efektivně diagnostikovat, který prvek po cestě způsobuje zpoždění nebo zjistit, dochází-li na něm k výpadkům.



Obrázek 18 - MTR test v prostředí systému Debian Linux
Zdroj: Vlastní tvorba (systém Debian Linux)



Obrázek 19 - MTR test v prostředí systému RouterOS
Zdroj: Nástroj WinBox

2.8.5 Test rychlosti přenosu dat (download/upload speedtest)

Testování rychlosti přenosu určitého objemu dat patří mezi základní metody měření rychlosti sítě. Vždy je nutné rozlišit (především pak při testování rychlosti internetového připojení), zda je testován příjem nebo odesílání dat. Dalším nezbytným aspektem je volba serveru pro testování, neboť kvalita a rychlost připojení protistrany nesmí negativně ovlivnit výsledky testu.

Test rychlosti stahování

Pro testování rychlosti stahování dat se nejčastěji využívá webový server, na kterém jsou uloženy a publikovány soubory o různých velikostech (většinou s náhodně generovaným obsahem). Při započetí testu začne klient stahovat daný soubor ze serveru. Z informací o velikosti stahovaného souboru a doby stahování je vypočítána rychlost stahování.

Podle serveru Speedtest.net, by OOKLA (v dnešní době nejpopulárnější on-line nástroj pro měření parametrů připojení) zahrnuje efektivní postup měření rychlosti připojení k internetu tyto kroky:

1) *Klient ze serveru stáhne malé binární soubory za účelem odhadu přibližné rychlosti*
2) *Na základě výsledků tohoto odhadu je vybrána vhodná velikost souboru pro reálný test rychlosti stahování*
3) *Testovací soubory jsou stahovány až 30krát za vteřinu*
4) *Testovací soubory jsou rozděleny na 20 částí (každá z nich tvoří 5 % souboru)*
5) *Následně jsou výsledky stahování všech souborů seřazeny podle rychlosti. Dva nejrychlejší jsou odstraněny a poslední ¼ výsledků také. Z ostatních výsledků je vypočítán aritmetický průměr, který tvoří výsledek testu.*

Zdroj: (15)

Test rychlosti nahrávání

Testování rychlosti nahrávání (uploadu) je opakem testu rychlosti stahování. Klient odesílá (nahrává) soubory na server. Pro nahrávání souborů je využíván HTTP POST požadavek.

Nástroj Speedtest.net, by OOKLA využívá pro test rychlosti nahrávání tento postup:

1) *Klient na webový server nahraje malý soubor dat pro odhad rychlosti nahrávání*
2) *Na základě výsledků tohoto odhadu je vybrána vhodná velikost souboru pro reálný test rychlosti nahrávání*
3) *Každý soubor je pojmenován náhodným řetězcem znaků pro zabránění použití mezipaměti*
4) *Test je prováděn se vzorky jednotné velikosti, pomocí skriptu na straně serveru, který zajistí nahrání souboru HTTP POST požadavkem.*
5) *Data jsou odesílána v několika samostatných vláknech (až ve 4) pro zajištění co nejlepší saturace připojení*
6) *Výsledky nahrávání souborů jsou seřazeny podle velikosti a aritmetickým průměrem rychlejší poloviny výsledků je určena konečná rychlost.*

Zdroj: (15)

3 Návrh vlastního řešení

Praktické ověření navrženého postupu testování je implementováno formou mobilní aplikace „Network Test Tool“ pro zařízení s operačním systémem Android. Aplikace je vytvořena v jazyce Java pomocí vývojového prostředí Android Studio. Pro potřeby samostatného použití a z důvodu snazší ovladatelnosti je vybavena i jednoduchým grafickým uživatelským rozhraním, které lze v případě potřeby snadno pozměnit (Obrázek 20 - Ukázka rozhraní mobilní aplikaceObrázek 20).
Nástroj pro demonstraci testování komplexně vyhodnocuje stav připojení v pravidelných intervalech, dále informuje o výsledcích dílčích testů. Vše je přehledně zobrazeno na hlavní obrazovce aplikace, odkud může uživatel aplikaci ovládat.

3.1 Součásti aplikace

- Zjištění aktivních síťových rozhraní
- Zjištění síly Wi-Fi signálu (hodnota RSSI) a frekvenčního pásma Wi-Fi
- Překlad DNS názvu na IP adresu
- Test ICMP ping
- Test TCP ping
- Download speedtest
- Upload speedtest

3.2 Technické parametry aplikace

Aplikace vyžaduje pro svůj běh zařízení s operačním systémem Android v minimální verzi 5.0. Tuto nebo vyšší verzi systému využívá přibližně 84,3 % zařízení (údaj k 16. 4. 2018). Při běžném provozu využívá přibližně 35 MB RAM paměti, během testů rychlosti spotřeba vzroste na cca 50 MB operační paměti. Generované soubory pro test rychlosti přenosu dat vyžadují cca 130 944 kB volného místa.
Z hlediska oprávnění vyžaduje aplikace přístup k informacím o stavu internetového připojení zařízení, přístup k Internetu. Nemá tedy žádné zvláštní požadavky na oprávnění.

3.3 Funkcionální princip řešení (mobilní aplikace)

Ihned po spuštění aplikace dojde k detekci aktivních síťových rozhraní (Wi-Fi nebo mobilní datové připojení). Pro možnost spuštění dalších testů je nutné, aby alespoň jedno rozhraní bylo aktivní. Pokud je aktivní rozhraní Wi-Fi připojení, aplikace zjistí přidělenou interní IP adresu zařízení a sílu Wi-Fi signálu (v grafickém rozhraní je zobrazena procentuálně i v jednotkách dBm.

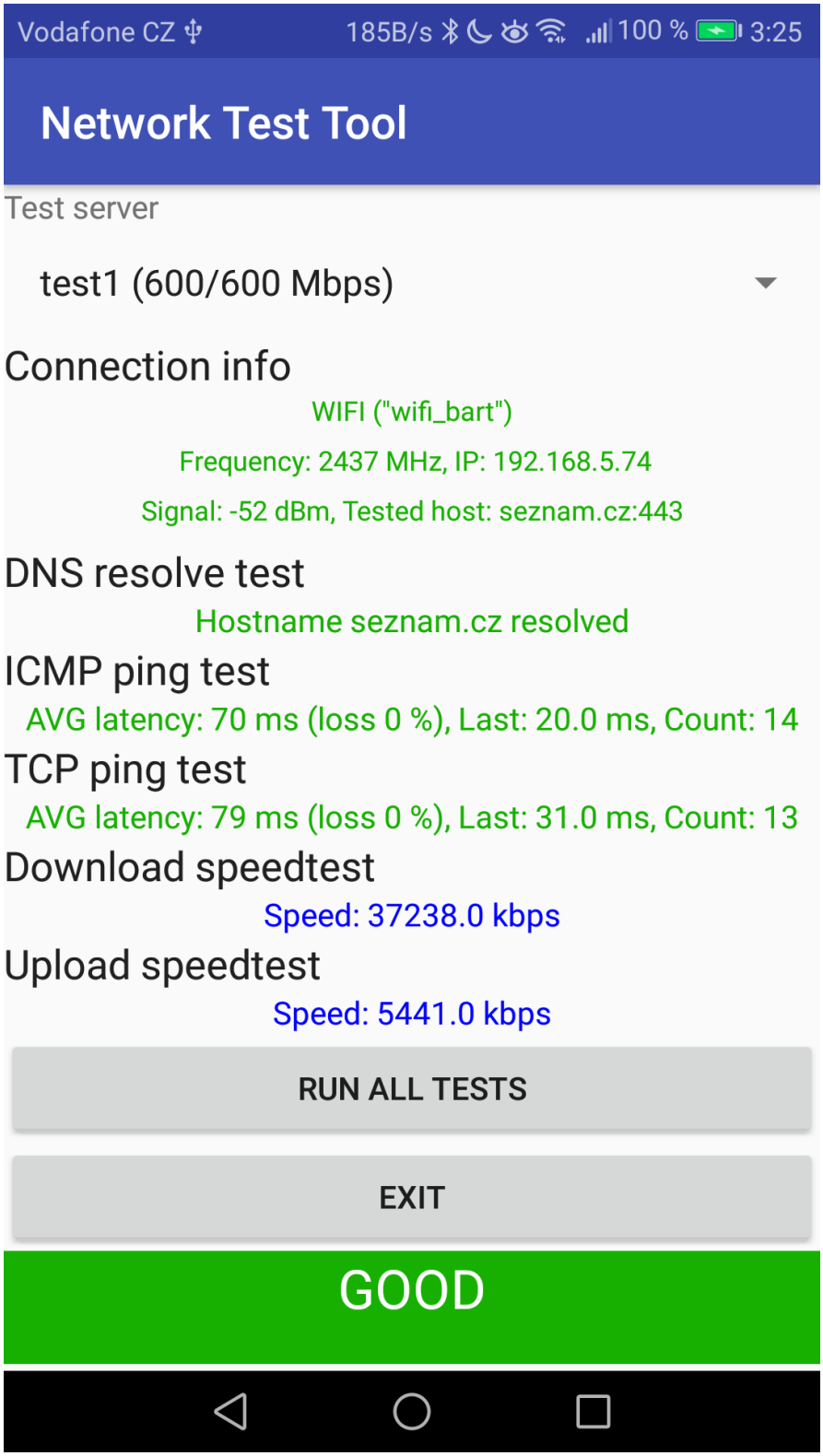
Dále aplikace provede test DNS překladu testovaného socketu, ICMP ping test adresy vzdáleného hosta a TCP ping test socketu. Pokud se ICMP ping test nezdaří a skončí neúspěšně, výsledné latence budou vypočítány pouze z výsledků TCP ping testu.

Při startu aplikace je také vybrán jeden ze serverů pro testování rychlosti internetového připojení. Výběr je uskutečněn podle těchto parametrů: dostupnost serveru, rychlost internetového připojení serveru, přičemž uživatel má možnost manuální změny tohoto serveru.

Po dokončení TCP ping testu je proveden test rychlosti stahování a nahrávání souboru (download speedtest a upload speedtest) vůči dříve zvolenému testovacímu serveru. Nejprve je proveden test stahování a po jeho skončení se spustí test nahrávání. Spuštění testů rychlosti je možné kdykoliv později manuálně. Aplikace však spustí testování rychlosti pouze v případě, že je zařízení připojeno k Wi-Fi, při mobilním datovém připojení se s ohledem na datový limit FUP, čeká na potvrzení uživatele z důvodu.

Výsledky ze všech testů jsou průběžně zpracovávány vyhodnocovacím algoritmem, který určuje celkovou kvalitu připojení ke vzdálenému systému a zobrazí jej na hlavní obrazovce aplikace.

3.3.1 Ukázka rozhraní mobilní aplikace



Obrázek 20 - Ukázka rozhraní mobilní aplikace
Zdroj: Vlastní tvorba

4 Implementace, testování

Tato kapitola popisuje implementaci postupu testování v programovacím jazyce Java (přizpůsobené operačnímu systému Android). Dále jsou zde uvedeny informace potřebné pro stanovení podmínek jednotlivých testů, určení výsledků a seznam použitých testovacích zařízení včetně jejich technických parametrů.

4.1 Zjištění dostupnosti připojení

- Vytvoření proměnné třídy WifiManager s uloženou informací o handleru systémové služby WIFI_SERVICE
- Hodnota boolean získaná pomocí metody isEnabled() třídy WifiManager vyjadřuje, zda je v systému Wi-Fi zapnutá či deaktivovaná.
- Vytvoření proměnné třídy ConnectivityManager s uloženou informací o handleru systémové služby CONNECTIVITY_SERVICE
- Vytvoření proměnné třídy NetworkInfo pomocí metody getNetworkInfo() třídy ConnectivityManager. Jako parametr metody je uveden typ připojení
- Hodnota boolean získaná pomocí metody isConnected() třídy Network info vyjadřuje, zda je Wifi připojená či odpojená
- Vytvoření proměnné třídy ConnectivityManager s uloženou informací o handleru systémové služby CONNECTIVITY_SERVICE
- Hodnota proměnné netInfoCellular je vyjádřeno, zda jsou mobilní data povolená či nikoliv.

4.2 DNS resolving test

- Vytvoření nové instance třídy java.net.InetAddress, kde bude uložena získaná IP adresa hostitele
- Vytvoření nového vlákna
- Zjištění IP adresy pomocí metody getByName() s parametrem DNS názvu hostitele
- Není-li DNS překlad úspěšný, metoda getByName() vrátí výjimku UnknownHostException (do proměnné remoteHost je uložena IP adresa loopback rozhraní)
- Spuštění vytvořeného vlákna
- Vyčkání na ukončení běhu vlákna

4.3 TCP socket open test

- Vytvoření nové instance třídy java.net.Socket (*třída pro provádění TCP operací na straně klienta, používá nativní kód pro komunikaci se síťovými knihovnami v operačním systému*) (16)
- Vytvoření nové instance třídy java.net.SocketAddress s parametry IP adresy vzdáleného hosta a čísla portu
- Otestování připojení k socketu pomocí metody connect() s parametry instance třídy java.net.SocketAddress a timeoutu připojení v milisekundách.
- Po úspěšném připojení je socket uzavřen metodou close()
- Pokud připojení není úspěšné, metoda connect() vrátí výjimku IOexception

4.4 Stažení a uložení souboru z URL adresy

- Vytvoření nové instance třídy java.net.URL s adresou stahovaného souboru *(třída pro definici URL adresy, umožňuje zahrnout informace o hostname, port, protokol, cestu a další parametry)* (16)
- Vytvoření nového objektu třídy BufferedInputStream, který získává data z otevřeného síťového spojení z konkrétní URL adresy
- Vytvoření nového objektu třídy FileOutputStream *(podtřída třídy OutputStream pro zápis dat do souboru)* (16)
- Vytvoření nového objektu třídy ByteArrayOutputStream (zapisuje data do rozšiřovatelného pole byte[])
- Záznam časového údaje t1
- Stažení dat z URL adresy do vyrovnávací paměti (bufferu)
- Záznam časového údaje t2
- Zápis dat z vyrovnávací paměti do souboru pomocí metody write třídy FileOutputStream
- Uzavření používaných síťových spojení se vzdáleným serverem
- Metody zápisu nebo čtení dat vrací výjimku IOException, pokud není proces úspěšný a dojde k chybě

4.5 Nahrání souboru pomocí webového formuláře (HTTP POST)

- Vytvoření nové instance třídy java.net.URLConnection s otevřením připojením k URL adrese pro upload souboru
- *Vytvoření nového objektu třídy FileInputStream, který zajišťuje načítání dat ze souboru* (16)
- Sestavení webového požadavku HTTP POST pro nahrání souboru ve formě „multipart/form-data“
- Vytvoření nového objektu třídy OutputStream, který nahraje data do webového formuláře
- Odeslání první části webového požadavku do objektu třídy OutputStream
- Odeslání souboru do objektu třídy OutputStream
- Odeslání druhé části webového požadavku do objektu třídy OutputStream
- Záznam časového údaje t1
- Spuštění procesu zápisu objektu třídy OutputStream
- Vytvoření nového objektu třídy InputStream
- Spuštění procesu načítání dat z objektu třídy InputStream do vyrovnávací paměti
- Záznam časového údaje t2

4.6 Řešené problémy při implementaci a programování

Předávání zpráv po dokončení testů

Z důvodu nutnosti spouštět jednotlivé testy v nových vláknech aplikace bylo třeba využít třídy IntentService pro spouštění asynchronních úloh a pro přijímání a odesílání informací o provedeném testu do hlavní aplikační třídy.

Generování souborů pro upload test

Jako jednoduchý a pro výkon mobilního zařízení nenáročný způsob generování náhodných souborů o různých velikostech se zdá být použití utility „dd /dev/urandom“. V aplikaci je použita pro generování souborů pro test rychlosti uploadu.

Zatížení internetového připojení při testování rychlosti

Při testování mobilní aplikace bylo zjištěno nedostatečné vytížení internetové konektivity při stahování pouze jednoho souboru. Bylo tedy nutné použít spouštění více vláken stahování a nahrávání souborů zároveň a odchycení jejich výsledků pomocí ExecutorService.

Automatické přepínání frekvenčních pásem Wifi v OS Android

Operační systém Android disponuje funkcí pro automatické přepínání mezi frekvenčními pásmy Wi-Fi (2,4 GHz a 5 GHz). Z toho důvodu je v aplikaci zobrazeno aktuálně využívané frekvenční pásmo pro snazší orientaci při měření.

4.7 Návrh algoritmu pro vyhodnocení stavu připojení

Tento algoritmus přijímá výsledky dílčích testů, porovnává je a na základě výsledků určí stav síťového připojení. Tato podkapitola popisuje princip a funkcionalitu algoritmu.

4.7.1 Analýza přítomnosti síťového připojení

Pro možnost práce s jakoukoliv aplikací, vyžadující připojení k Internetu, je nutné aktivní síťové připojení. V mobilních telefonech je možnost použít buď Wi-Fi připojení nebo mobilní datový signál operátora.

4.7.2 Analýza síly signálu Wi-Fi

Pro reprezentaci síly signálu se používá jednotka RSSI [dBm] (Received Signal Strength Indication). *Tento údaj je důležité při měření brát v potaz, protože má dopad na výkon koncových bodů (klientů) připojených k síti. Ovlivňuje také maximální šířku pásma a zpoždění přenosu dat bezdrátových klientů. U Wi-Fi připojení se hodnoty RSSI pohybují v rozsahu –50 - –90 dBm, při použití 3G připojení v rozsahu –85 - –105 dBm.* (17)

Vše také záleží na použitém frekvenčním pásmu Wi-Fi (2,4 GHz nebo 5 GHz). Pásmo 5 GHz poskytuje vyšší výkon při potřebě vyšší propustnosti oproti 2,4 GHz. V případě slabého signálu je propustnost na podobných hodnotách, nicméně u 5 GHz pásma dochází k vyšší ztrátovosti.

Toto ukazuje i tabulka z reálného testování propustnosti:

Tabulka 3 - Závislost propustnosti na hodnotě RSSI a frekvenčním pásmu

RSSI	2,4 GHz	5GHz
–65 dBm	20 Mbps	30 Mbps
–85 dBm	2,5 Mbps	2,5 Mbps

Zdroj: (18)

Při praktickém testování vlivu hodnoty RSSI na RTT byly naměřeny tyto výsledky:

Tabulka 4 - Výsledky měření závislosti RTT na hodnotě RSSI

RSSI (dBm)	Latence 2,4 GHz (ms)	Latence 5 GHz (ms)
−44	15-18	12
−50	20-25	14
−65	30	20
−75	40-50	60
−85	100	160

Z těchto hodnot vyplývá, že pro zajištění velmi dobré kvality připojení je nutná minimální úroveň RSSI alespoň −70 dBm, pro zajištění dostatečné kvality alespoň −80 dBm.

4.7.3 Analýza stability připojení

Velice důležitým ukazatelem stability připojení je množství paketů přijatých od začátku testu. *Pomocí ICMP/TCP/UDP ping testu lze stabilitu zjistit z naměřených hodnot RTT (Round Trip Time). Odeslané pakety se mohou kdekoliv po cestě do cíle ztratit (mohou být zahozeny), poté je do měření zahrnutá také míra ztrátovosti.* (19)
Ztrátovost je vypočítána pomocí následujícího vzorce:

$$w = \frac{n - r}{n}$$

w = míra ztrátovosti

r = počet přijatých paketů

n = počet odeslaných paketů

Hodnota RTT je reprezentována časem (v milisekundách), který uplynul od odeslání paketu cílovému zařízení do přijetí odpovědi od tohoto zařízení. Tento čas je ovlivněn vzdáleností mezi dvěma zařízeními, hustotou síťového provozu a vytížením každého zařízení.

Pokud cílové zařízení neodpovídá na požadavek na odezvu, může to být kvůli těmto faktorům: Cílové zařízení je vypnuté nebo nedostupné v síti, nastala porucha části sítě mezi lokálním a cílovým zařízením, došlo k softwarové chybě na cílovém zařízení případně mohlo být toto zařízení nakonfigurováno z bezpečnostních důvodů tak, aby neodpovídalo na požadavky na odezvu. (20). Pokud tedy ICMP ping není funkční, ale

test pomocí jiných protokolů (TCP, UDP) ano, dochází zřejmě k blokaci ICMP provozu na firewallu.

Měření pomocí ICMP protokolu je často používáno k odhadu TCP a UDP síťového provozu a ICMP protokol je dobrým ukazatelem TCP a UDP latencí. *Avšak ICMP měření dosahuje vyšší míry ztrátovosti než TCP a UDP.* (19)

Akceptovatelná míra ztrátovosti a velikosti latencí se liší podle konkrétní aplikace. Mezi nejcitlivější z nich patří přenos hlasu (VoIP telefonie) – zde by latence neměly překročit hodnotu 150 ms. (21) Ztrátovost je v případě VoIP služeb také kritická. Výpadek pouhých 2 paketů za sebou způsobí drobné přerušení hovoru. Procentuální hodnota ztrátovosti by pak neměla překročit 1 %.

4.7.4 Analýza rychlosti připojení

Test rychlosti přenosu dat je důležitý z důvodu zvyšující se datové náročnosti dnešních aplikací. Nestačí mít tedy pouze stabilní síť s co nejmenším počtem výpadků, ale podstatná je i rychlost stahování a odesílání dat na vzdálený server. Z toho důvodu se často provádí měření rychlosti sítě. U mobilních zařízení jsou navíc dvě základní možnosti internetového připojení – Wi-Fi a mobilní datové připojení.

Dnešní zařízení s možností Wi-Fi připojení používají zpravidla varianty 802.11g (rychlost 54 Mbps), která byla vyvinuta kvůli zpětné kompatibilitě se standardem 802.11b (přenosová rychlost 11 Mbps), 802.11n (300 Mbps, 600 Mbps MIMO) a 802.11ac s maximální rychlostí do 1300 Mbps ve frekvenčním pásmu 5 GHz a 450 Mbps pro pásmo 2,4 GHz. (22)

Přehled všech variant Wi-Fi standardu 802.11 znázorňuje tabulka

Tabulka 5 - Přehled variant Wi-Fi standardu 802.11

Varianta	Frekvenční pásmo (GHz)	Počet kanálů
802.11a	5	42
802.11b	2,4	14
802.11g	2,4	14
802.11n	2,4 a 5	13
802.11ac	5	42
802.11ad	60	4

Zdroj: (23)

U mobilního datového přenosu jsou pro změnu rozlišovány varianty podle generace sítě (2G, 3G, 4G). *Generace 2G sítí (zkratka EDGE) disponuje přenosovou rychlostí maximálně 1 Mbps, standardně se však naměřené hodnoty pohybují okolo 500 kbps. Sítě třetí generace CDMA dokáží přenášet data rychlostí maximálně 4 Mbps a aktuální standard pro mobilní datové připojení, LTE (Long-Term Evolution), pracuje s rychlostmi až 300/75 Mbps (download/upload). Verze LTE Advanced zvyšuje tento limit až na 1000/500 Mbps.* (24)

Minimální vyžadovaná rychlost síťového přenosu se liší podle konkrétního použití. Mezi nejnáročnější aplikace se řadí streamovací služby pro on-line přenos videí v HD kvalitě. Ty vyžadují konkrétně okolo 5 Mbps. Dále například přehrávání videí na portálu YouTube.com potřebuje ke své funkčnosti rychlost cca 1 Mbps, telefonování pomocí aplikace Skype minimálně 0,1 Mbps pro obyčejné hovory a 0,3 Mbps pro videohovory (download i upload). (25)

4.7.5 Sumarizace výsledků a vyhodnocení

Modul periodicky (jednou za 5 vteřin) spustí všechny subtesty, shromáždí výsledky, vyhodnotí je a v uživatelském rozhraní zobrazí celkový stav připojení. Ten může nabývat tří hodnot (dobrý, zhoršený, špatný).

Ve stavu „dobrý“ jsou všechny testy v pořádku a síťové připojení nevykazuje v tuto chvíli žádné anomálie, které by mohly ohrozit jeho kvalitu a stabilitu. Druhý stav „zhoršený“ poukazuje na výskyt jevu zhoršené kvality. V případě, že tento stav nastane, měly by ostatní aplikace svá data synchronizovat, protože z této situace může dojít k přechodu do stavu „špatný“. Zde již většinou není připojení dostupné vůbec, případně jen s častými výpadky a vysokými odezvami, při kterých se spojení se vzdáleným serverem může přerušit.

Níže jsou popsány hodnoty výsledků testů, které se používají pro vyhodnocování celkového stavu síťového připojení:

Dostupnost síťového připojení

Stav „dobrý“

- Dostupné připojení Wi-Fi NEBO dostupné mobilní datové připojení

Stav „zhoršený“

- Není

Stav „špatný“

- Není dostupné žádné síťové připojení

Síla Wi-Fi signálu (RSSI hodnota)

Stav „dobrý“

- Hodnota RSSI > −70 dBm

Stav „zhoršený“

- Hodnota RSSI < −70 dBm

Stav „špatný“

- Hodnota RSSI < −80 dBm

Překlad DNS názvu

Stav „dobrý“

- DNS název vzdáleného serveru byl přeložen

Stav „zhoršený“

- Není

Stav „špatný“

- DNS název vzdáleného serveru nebyl přeložen

ICMP ping test

Stav „dobrý“

- Ztrátovost série pingů ICMP ≤ 25 % a ztrátovost předchozí série pingů ICMP ≤ 25 % A ZÁROVEŇ latence série pingů ICMP ≤ 120 ms a latence předchozí série pingů ICMP ≤ 120 ms

Stav „zhoršený“

- Ztrátovost série pingů ICMP ≥ 25 % a ztrátovost předchozí série pingů ICMP ≥ 25 % NEBO latence série pingů ICMP ≥ 120 ms a latence předchozí série pingů ICMP ≥ 120 ms

Stav „špatný“

- Ztrátovost ICMP = 100 % a ztrátovost TCP ≥ 50 %
- Ztrátovost série pingů ICMP ≥ 50 % a ztrátovost předchozí série pingů ICMP ≥ 50 % NEBO latence série pingů ICMP ≥ 150 ms a latence předchozí série pingů ICMP ≥ 150 ms

TCP ping test

Stav „dobrý“

- Ztrátovost série pingů TCP ≤ 25 % a ztrátovost předchozí série pingů TCP ≤ 25 % A ZÁROVEŇ latence série pingů TCP ≤ 120 ms a latence předchozí série pingů TCP ≤ 120 ms

Stav „zhoršený“

- Ztrátovost série pingů TCP ≥ 25 % a ztrátovost předchozí série pingů TCP ≥ 25 % NEBO latence série pingů TCP ≥ 120 ms a latence předchozí série pingů TCP ≥ 120 ms

Stav „špatný“

- Ztrátovost TCP = 100 % a ztrátovost ICMP ≥ 50 %
- Ztrátovost série pingů TCP ≥ 50 % a ztrátovost předchozí série pingů TCP ≥ 50 % NEBO latence série pingů TCP ≥ 150 ms a latence předchozí série pingů TCP ≥ 150 ms

Download speedtest

Stav „dobrý“

- Naměřená rychlost > 1000 kbps

Stav „zhoršený“

- Není

Stav „špatný“

- Naměřená rychlost < 1000 kbps

4.8 Testování

Tato kapitola popisuje postupy pro testování funkčnosti vytvořené aplikace, parametry použitých zařízení.

4.8.1 Testovací koncová zařízení

Pro testování mobilní aplikace byla použita koncová zařízení odlišného výkonu, z různých cenových kategorií a s operačním systémem Android v různých verzích (6.0, 7.0, 8.0).

Mobilní telefon Huawei P9 Lite

Operační systém: Android 7.0 Nougat

CPU: 4x 2,0 GHz + 4x 1,7 GHz

RAM: 2 GB

Kapacita interního úložiště: 16 GB

Podpora frekvenčních pásem Wi-Fi 2,4 GHz

Zdroj: (26)

Mobilní telefon Lenovo C2

Operační systém: Android 6.0 Marshmallow

CPU: 4x 1 GHz

RAM: 1 GB

Kapacita interního úložiště: 8 GB

Podpora frekvenčních pásem Wi-Fi 2,4 GHz

Zdroj: (27)

Mobilní telefon Honor View 10

Operační systém: Android 8.0 Oreo

CPU: 4x 2,36 GHz + 4x 1,8 GHz

RAM: 6 GB

Kapacita interního úložiště: 128 GB

Podpora frekvenčních pásem Wi-Fi 2,4 GHz a 5 GHz

Zdroj: (28)

Tablet Huawei MediaPad T3

Operační systém: Android 7.0 Nougat

CPU: 4x 1,4 GHz

RAM: 2 GB

Kapacita interního úložiště: 16 GB

Podpora frekvenčních pásem Wi-Fi 2,4 GHz a 5 GHz

Zdroj: (29)

4.8.2 Testovací síťová zařízení

Wi-Fi AP Ubiquiti Unifi AP-AC-LR

Maximální rychlost v pásmu 2,4 GHz: 450 Mbps

Maximální rychlost v pásmu 5 GHz: 867 Mbps

Maximální vysílací výkon v pásmu 2,4 GHz: 24 dBm

Maximální vysílací výkon v pásmu 5 GHz: 22 dBm

Vysílací část: Dual-band anténa, vysílací výkon 3 dBi

Zdroj: (30)

Router MikroTik RouterBoard RB941-2nD (hAP lite)

Operační systém: RouterOS L4

CPU: 650 MHz

RAM: 32 MB

Síťová rozhraní: 4x 10/100 Mbit Ethernet port, Wi-Fi 2,4 GHz, 802.11b/g/n

Zdroj: (31)

4.8.3 Postup testování

1) Různá kvalita Wi-Fi signálu (-20 dBm, -60 dBm, -85 dBm) v obou frekvenčních pásmech (2,4 GHz a 5 GHz)
2) Mobilní datové připojení (vynucené použití sítě 2G/3G/4G)
3) Uměle simulované výpadky připojení (ztrátovost 25 % a 50 %)
4) Omezená rychlost síťového připojení (omezeno technologií QoS na rychlosti 4/4 Mbps a 2/0,5 Mbps)
5) Srovnání rychlosti stahování/nahrávání v aplikaci a webového prohlížeče Google Chrome

Všechny uvedené situace jsou postupně simulovány na testovacích koncových zařízeních, s použitím síťových zařízení, uvedených v kapitole 2.11.2 a mobilním datovým připojením.

Je provedeno otestování při různé kvalitě Wi-Fi signálu (vynikající úroveň signálu, středně silný signál, slabý signál) v obou frekvenčních pásmech (**2,4 GHz** a **5 GHz**). Následně je testování opakováno při použití různých typů mobilního datového připojení (sítě 2G, 3G, 4G).

Dalším z testů je detekce ztrát paketů u síťového připojení. Tento jev je simulován routerem MikroTik, který provádí zahazování každého x-tého paketu a tím simuluje výpadky. Router MikroTik provádí u dalšího typu testu také umělé snížení rychlosti přenosu dat po síti pomocí nastavených QoS pravidel (nejprve na symetrickou rychlost **4/4 Mbps** a poté nesymetrickou rychlost **2/0,5 Mbps**).

Jako poslední test je provedeno porovnání výsledků testů rychlosti v aplikaci s rychlostí stahování a nahrávání dat pomocí mobilního prohlížeče Google Chrome.

5 Výsledky testování

Různá kvalita Wi-Fi signálu

Testování s internetovou konektivitou o rychlosti cca 60/60 Mbps

Hodnoty v tabulce jsou uváděny v jednotkách Mbps (download/upload).

Testy rychlosti přenosu dat – frekvenční pásmo 2,4 GHz

Tabulka 6 - Výsledky testu rychlosti přenosu dat (2,4 GHz)

Zařízení	-20 dBm	-60 dBm	-85 dBm
Huawei P9 lite	32,70/37,43	19,30/26,75	1,40/3,81
Lenovo C2	44,04/39,63	39,97/36,56	1,48/2,81
Honor View 10	48,25/47,22	51,86/49,54	2,48/1,59
Huawei MediaPad T3	41,42/42,21	24,01/30,85	1,80/3,06

Testy rychlosti přenosu dat – frekvenční pásmo 5 GHz

Tabulka 7 - Výsledky testu rychlosti přenosu dat (5 GHz)

Zařízení	-20 dBm	-60 dBm	-85 dBm
Huawei P9 lite	nepodporováno	nepodporováno	nepodporováno
Lenovo C2	nepodporováno	nepodporováno	nepodporováno
Honor View 10	62,57/58,39	51,97/36,54	1,80/4,76
Huawei MediaPad T3	59,76/62,21	57,4/60,02	3,47/7,25

Testy ICMP latencí – frekvenční pásmo 2,4 GHz

Tabulka 8 - Výsledky testu ICMP latencí (2,4 GHz)

Zařízení	-20 dBm	-60 dBm	-85 dBm
Lenovo C2	26	33	171
Huawei MediaPad T3	23	31	129

Testy ICMP latencí – frekvenční pásmo 5 GHz

Tabulka 9 - Výsledky testu ICMP latencí (5 GHz)

Zařízení	-20 dBm	-60 dBm	-85 dBm
Lenovo C2	nepodporováno	nepodporováno	nepodporováno
Huawei MediaPad T3	17	22	142

Testy mobilního datového připojení

Všechny testy mobilního datového připojení byly prováděny při maximální síle signálu mobilního operátora.

Testy rychlosti přenosu dat

Tabulka 10 - Výsledky testu rychlosti mobilního připojení

Zařízení	2G síť	3G síť	4G síť
Huawei P9 lite	0,22/0,07	3,01/0,67	22,88/7,02
Honor View 10	Nebyl dokončen	2,84/0,56	14,00/5,21

Testy ICMP latencí

Tabulka 11 - Výsledky testu ICMP latencí (mobilní připojení)

Zařízení	2G síť	3G síť	4G síť
Huawei P9 lite	314	157	34
Honor View 10	266	143	23

Testy TCP latencí

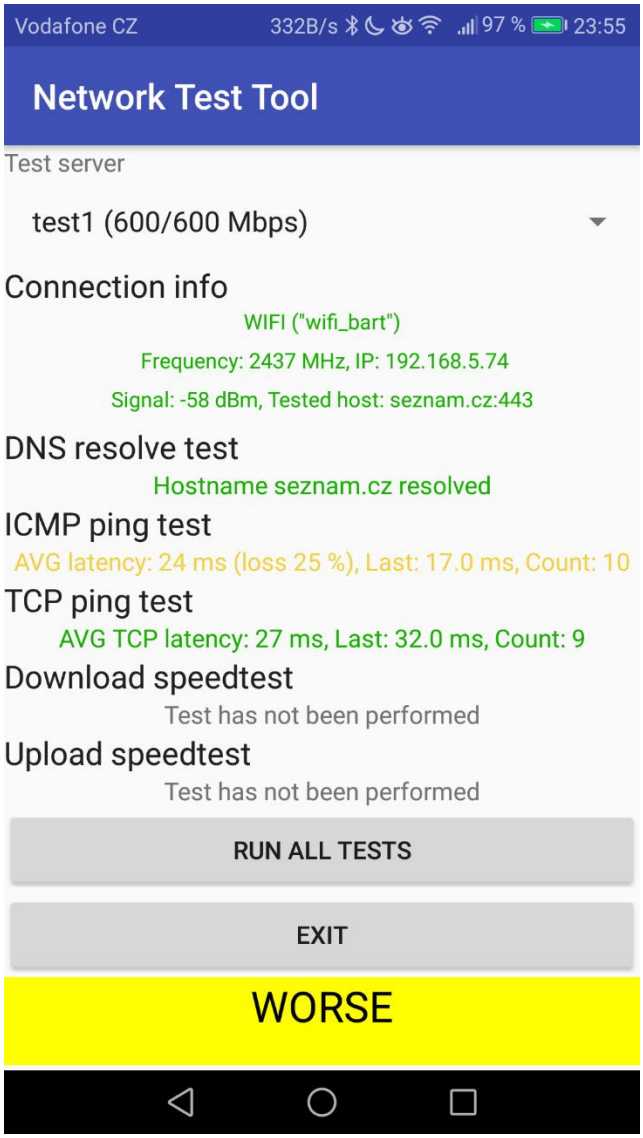
Tabulka 12 - Výsledky testu TCP latencí (mobilní připojení)

Zařízení	2G síť	3G síť	4G síť
Huawei P9 lite	1275	193	43
Honor View 10	654	175	37

Test ztrátovosti paketů

Síťový firewall je pro tento test nastaven tak, aby zahazoval nejprve každý 4. paket a poté každý 3. a 4. paket.

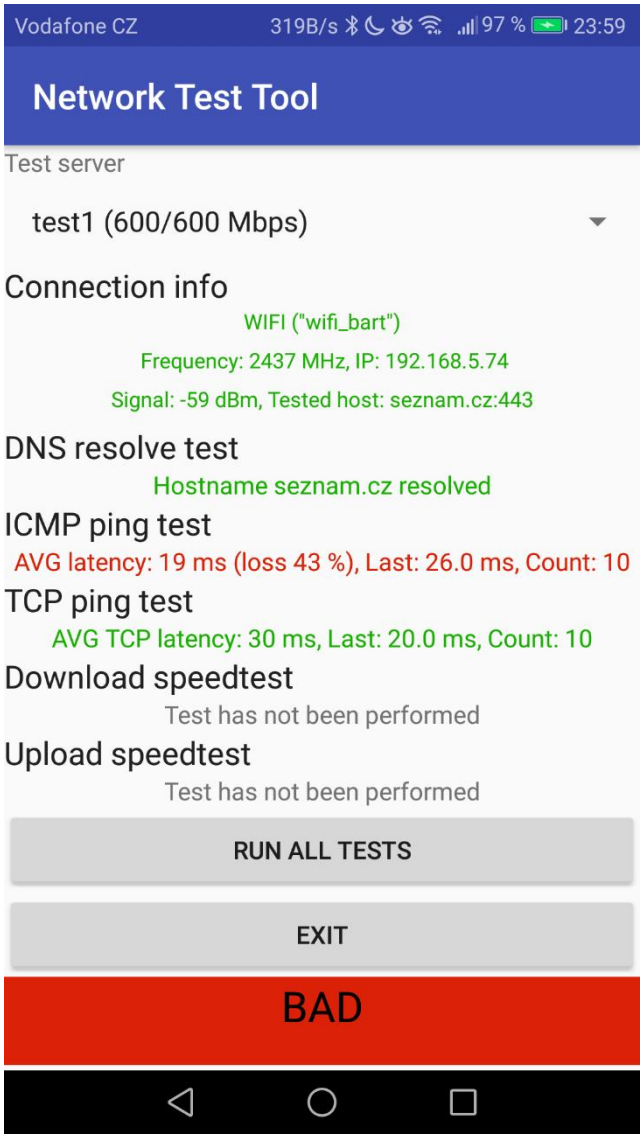
Zahazování každého 4. paketu (simulace ztrátovosti 25%)



Obrázek 21 - Výsledek testu ztrátovosti 25 % v mobilní aplikaci
Zdroj: Vlastní tvorba

Cílem tohoto testu bylo dokázat, že aplikace zobrazí varování při ztrátovosti o velikosti ≥ 25 % a zároveň ≤ 50 %. Je také kontrolováno, zda nedošlo k výpadku alespoň 2 paketů za sebou.

Zahazování každého 3. a 4. paketu (simulace ztrátovosti 50%)



Obrázek 22 - Výsledek testu ztrátovosti 50 % v mobilní aplikaci
Zdroj: Vlastní tvorba

Cílem tohoto testu bylo dokázat, že aplikace zobrazí chybu při ztrátovosti o velikosti ≥ 50 %. Dále zde došlo k výpadku 2 paketů za sebou (byl zahazován každý 3. a 4. paket).

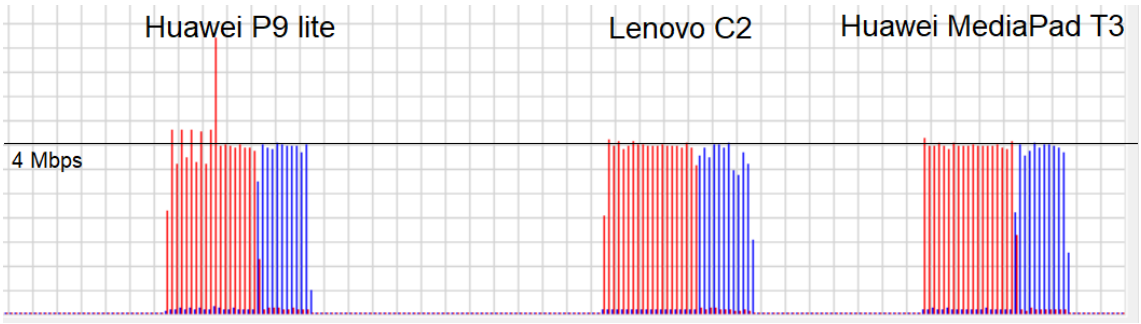
Simulace omezené rychlosti síťového připojení

Na routeru bylo před provedením tohoto testu nastaveno omezení maximální rychlosti pomocí technologie QoS na uvedené rychlosti (4/4 Mbps a 2/0,5 Mbps).

Omezení rychlosti na 4/4 Mbps

Tabulka 13 - Výsledky testu s omezením rychlosti 4/4 Mbps

Zařízení	Rychlost (download/upload)
Huawei P9 lite	3,83/3,76
Lenovo C2	3,82/3,77
Huawei MediaPad T3	3,97/3,81



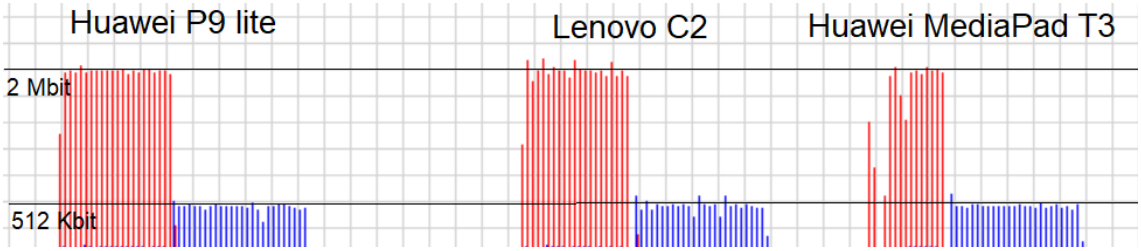
Obrázek 23 - Využití šířky pásma během testu

Zdroj: Nástroj Winbox

Omezení rychlosti na 2/0,5 Mbps

Tabulka 14 - Výsledky testu s omezením rychlosti 2/0,5 Mbps

Zařízení	Rychlost (download/upload)
Huawei P9 lite	1,89/0,52
Lenovo C2	1,94/0,53
Huawei MediaPad T3	1,94/0,57



Obrázek 24 - Využití šířky pásma během testu

Zdroj: Nástroj Winbox

Porovnání měření rychlostí připojení s mobilním prohlížečem

Stahování souboru

Velikost 65 536 kB

Čas stahování: 21,13 s

Výsledná rychlost: **24 812 kbps**

Naměřená hodnota pomocí mobilní aplikace: **26 324 kbps**

Nahrávání souboru

Velikost 65 536 kB

Čas nahrávání: 95.86 s

Výsledná rychlost: **5 469 kbps**

Naměřená hodnota pomocí mobilní aplikace: **5 597 kbps**

6 Závěr

Z výsledků získaných během měření je zřejmé, že kvalitu síťového připojení ovlivňuje více faktorů. Ty je nutné brát vždy v potaz, protože jeden faktor může mít vliv na jiné faktory a ovlivňuje celkovou kvalitu připojení.

Při využívání Wi-Fi připojení je nutné mít k dispozici kvalitní signál. V dnešní době rozmachu zařízení vybavených 5 GHz modulem Wi-Fi, stoupají i přenosové rychlosti, kterých lze s těmito zařízeními dosáhnout. Naproti tomu mobilní datové připojení sice poskytuje větší nezávislost a mobilitu, nicméně zde je kvalita znatelně horší – pro standardní aplikace s datově nenáročným provozem je dostačující připojení 4G (označované zkratkou LTE), kde lze dosáhnout přenosových rychlostí i cca 20/10 Mbps, závisí však na aktuální kvalitě signálu mobilního operátora. Připojení typu 3G a 2G se jeví pro použití s dnešními aplikacemi jako nevyhovující (nízké přenosová rychlosti, vysoké latence).

Negativně ovlivňují kvalitu připojení také výpadky, jež mohou způsobit rapidní pokles rychlosti přenosu a v horším případě až ztrátu spojení se vzdáleným serverem. Toto je problém zejména při slabším signálu Wi-Fi nebo pomalejších typech mobilního datového připojení, kde hrozí reálné riziko vzniku výpadků.

Další vývoj vytvořené mobilní aplikace Network Test Tool by měl zahrnovat vylepšení a modernizaci grafického uživatelského rozhraní, zlepšení interakce s uživatelem, zahrnutí dalších ovládacích prvků. Dále by měla být doplněna funkčnost serverové části měřícího systému přenosové rychlosti o náhodné generování názvů souborů (případně generování celých souborů) z důvodu zamezení možného použití mezipaměti lokálního proxy serveru na straně klienta a zkreslení výsledků měření.

Účelem této práce je objasnit základní teorii z oblasti počítačových sítí a síťových protokolů, vysvětlit problematiku měření sítě a ukázat možný návrh postupu pro tyto účely, včetně implementace přizpůsobené pro mobilní zařízení.

7 Použitá literatura

1. Alani, Mohammed M. *Guide to OSI and TCP/IP Models.* místo neznámé : Springer, 2014. 3319051520, 9783319051529.

2. Reviews, CTI. *Communication Networks: Computer science, Computer networking.* místo neznámé : Cram101 Textbook Reviews, 2016. 146723303X, 9781467233033.

3. Tarmo Anttalainen, Ville Jaaskelainen. *Introduction to Communication Networks.* místo neznámé : Artech House, 2014. 1608077624, 9781608077625.

4. Michael G. Solomon, David Kim, President and Chief Security Officer Security Evolutions Inc Fairfax Virginia David Kim, (In, Jeffrey L. Carrell. *Fundamentals of Communications and Networking.* místo neznámé : Jones & Bartlett Publishers, 2014. 1284060152, 9781284060157.

5. Sequeira, Anthony. *Interconnecting Cisco Network Devices, Part 1 (ICND1) Foundation Learning Guide.* místo neznámé : Cisco Press, 2013. 0133410234, 9780133410235.

6. Aboelela, Emad. *Network Simulation Experiments Manual.* místo neznámé : Elsevier, 2011. 0123852110.

7. Chwan-Hwa (John) Wu, J. David Irwin. *Introduction to Computer Networks and Cybersecurity.* místo neznámé : CRC Press, 2016. 1466572140, 9781466572140.

8. Stewart, James M. *CompTIA Security+ Review Guide: Exam SY0-401.* místo neznámé : John Wiley & Sons, 2014. 1118922905, 9781118922903.

9. Dean, Tamara. *Network+ Guide to Networks.* místo neznámé : Cengage Learning, 2009. 1423902459, 9781423902454.

10. Tebepah, Ibuomo R. WiMAX for Online Service Transmission. *International Journal of Networks and Communications.* 2017.

11. Garg, Vijay. *Wireless Communications & Networking.* místo neznámé : Elsevier, 2010. 0080549071.

12. Lewis, Wayne. *LAN switching and wireless.* místo neznámé : Cisco Press, 2008. 978-1-58713-207-0.

13. Grigorik, Ilya. *High Performance Browser Networking: What Every Web Developer Should Know about Networking and Web Performance.* místo neznámé : O'Reilly Media, Inc., 2013. 1449344747.

14. Granneman, Scott. *Linux Phrasebook.* místo neznámé : Addison-Wesley Professional, 2015. 9780133038590.

15. A Speed Test is a test to measure the access performance metrics. *LaroccaSolutions.* [Online] 1. Říjen 2016. [Citace: 09. 04 2018.] https://www.laroccasolutions.com/speed-test/.

16. Harold, Eliotte Rusty. *Java Network Programming, Fourth Edition.* 3. místo neznámé : O'Reilly Media, 2014. 978-1-449-35767-2.

17. *Low RSSI in WLANs: Impact on application-level performance.* Tauber, Markus. 2013. 978-1-4673-5288-8.

18. *Characterizing and Modeling the Impact of Wireless Signal Strength on Smartphone Battery Drain.* Ding, Ning. 2013.

19. Birrer, Stefan, Bustamante, Fabián a Chen, Yan. *Can we trust ICMP-based measurements?* 2004.

20. Sobell, Mark G. *A Practical Guide to Ubuntu Linux.* místo neznámé : Pearson Education, 2010. 9780132483933.

21. Wallace, Kevin. *CCNP Routing and Switching ROUTE 300-101 Official Cert Guide.* místo neznámé : Cisco Press, 2014. 9780133414271.

22. Wehrle, Klaus, Günes, Mesut a Gross, James. *Modeling and Tools for Network Simulation.* místo neznámé : Springer Science & Business Media, 2010. 9783642123313.

23. Hoy, Joseph. *Forensic Radio Survey Techniques for Cell Site Analysis.* místo neznámé : John Wiley & Sons, 2014. 9781118925751.

24. Buhagiar, Jon. *CompTIA Network+ Review Guide: Exam N10-007.* místo neznámé : John Wiley & Sons, 2018. 9781119432302.

25. Martin, Chris. What are good upload and download speed? *Tech Advisor from IDG.* [Online] IDG UK, 9. Srpen 2017. [Citace: 25. Duben 2018.] https://www.techadvisor.co.uk/feature/internet/what-are-good-upload-download-speeds-3662378/.

26. Co., HUAWEI Technologies. Huawei P9 Lite smartphone. *HUAWEI Global.* [Online] HUAWEI Technologies Co., 2018. [Citace: 24. Duben 2018.] https://consumer.huawei.com/en/phones/p9-lite/specs/.

27. Lenovo C2 - Android HD Smartphones. *Lenovo Official Nigeria Site.* [Online] Lenovo, 2018. [Citace: 25. Duben 2018.] https://www3.lenovo.com/ng/en/smart-devices/smartphones/c-series/K10a40/p/PPIPPIKK101.

28. Honor View 10. *Honor Official Store.* [Online] HUAWEI Device USA, 2018. [Citace: 23. Duben 2018.] https://store.hihonor.com/us/honor-view-10/specification.

29. HUAWEI MediaPad T3. *HUAWEI Global.* [Online] HUAWEI Technologies, 2018. [Citace: 25. Duben 2018.] https://consumer.huawei.com/en/tablets/mediapad-t3/specs/.

30. Ubiquiti Networks, Inc. Unifi AC AP Datasheet. *Ubiquiti Networks.* [Online] [Citace: 24. Duben 2018.] https://dl.ubnt.com/datasheets/unifi/UniFi_AC_APs_DS.pdf.

31. Mikrotik Routers and Wireless - Product: hAP lite. *Mikrotik Routers and Wireless.* [Online] MikroTik. [Citace: 24. Duben 2018.] https://mikrotik.com/product/RB941-2nD.

32. Christos N. Houmkozlis, George A. Rovithakis. *End-to-End Adaptive Congestion Control in TCP/IP Networks.* místo neznámé : CRC Press, 2017. 143984058X, 9781439840580.

8 Přílohy

1) Příloha 1 – ZIP soubor se zdrojovými kódy mobilní aplikace Network Test Tool a instalačním APK souborem této aplikace

Univerzita Hradec Králové
Fakulta informatiky a managementu

Zadání bakalářské práce

Autor:	**Tomáš Bartoníček**
Studium:	I1600839
Studijní program:	B1802 Aplikovaná informatika
Studijní obor:	Aplikovaná informatika
Název bakalářské práce:	**Modul pro testování propustnosti sítě**
Název bakalářské práce AJ:	Module for testing network throughput

Cíl, metody, literatura, předpoklady:

1) Úvod 2) Terminologie, metody měření sítě 3) Návrh vlastního řešení 4) Implementace, testování 5) Výsledky a závěr 6) Literatura Cíl práce: Cílem je nalezení vhodného postupu pro efektivní testování propustnosti sítě, postup implementovat a demonstrovat pomocí mobilní aplikace a prakticky ověřit.

1) LAN switching and wireless, Lewis Wayne, Cisco Press, 2008 2) Network monitoring, Lambert M. Surhone, Miriam T. Timpledon, Susan F. Marseken; Betascript Publishing, 2010 3) Network simulation experiments manual, Aboelela Emad, 2012 4) Modeling and tools for network simulation, Klaus Wehrle, Mesut Güneş, James Gross, 2010

Garantující pracoviště:	Katedra informatiky a kvantitativních metod, Fakulta informatiky a managementu
Vedoucí práce:	doc. Ing. Filip Malý, Ph.D.
Datum zadání závěrečné práce:	14.1.2015