VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

MĚŘENÍ KOMUNIKAČNÍHO ZPOŽDĚNÍ V IP SÍTÍCH

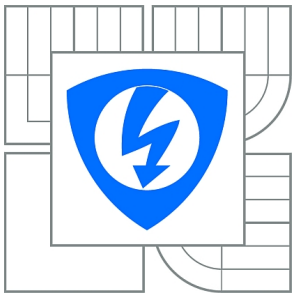
BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE VÍT BEDNÁŘ
AUTHOR

BRNO 2015

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

MĚŘENÍ KOMUNIKAČNÍHO ZPOŽDĚNÍ V IP SÍTÍCH

MEASUREMENT OF COMMUNICATION LATENCY IN IP NETWORKS

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

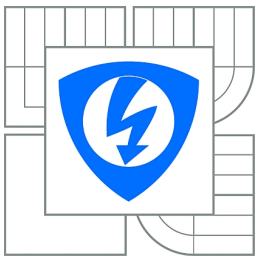
AUTOR PRÁCE — VÍT BEDNÁŘ

AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. DAN KOMOSNÝ, Ph.D.

SUPERVISOR

BRNO 2015



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student:	Vít Bednář	***ID:***	155140
Ročník:	3	***Akademický rok:***	2014/2015

NÁZEV TÉMATU:

Měření komunikačního zpoždění v IP sítích

POKYNY PRO VYPRACOVÁNÍ:

Nastudujte problematiku komunikačního zpoždění při přenosu dat v Internetu. Vytvořte seznam stanic a k těmto stanicím změřte komunikační zpoždění pomocí zvolených nástrojů. Srovnejte rozdíly v naměřených hodnotách pomocí různých nástrojů. Vytvořte webovou stránku, která bude umožňovat měření komunikačního zpoždění na zadané IP adresy.

DOPORUČENÁ LITERATURA:

[1] PUŽMANOVÁ, R. TCP/IP v kostce. 1. vyd. České Budějovice : Kopp, 2004. 607 s. ISBN 80-7232-236-2.
[2] COOPER, M. Advanced Bash-Scripting Guide. Lulu.com, 2010. ISBN: 978-1435752191.
[3] Linux Dokumentační projekt. Computer Press, 2008. ISBN: 978-80-251-1525-1.

Termín zadání:	9.2.2015	***Termín odevzdání:***	2.6.2015

Vedoucí práce: doc. Ing. Dan Komosný, Ph.D.
Konzultanti bakalářské práce:

doc. Ing. Jiří Mišurec, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

ABSTRAKT

Práce se zabývá měřením komunikačního zpoždění v sítích. Posupně je rozebrán vznik jednotlivých druhů zpoždění při přenosu v sítích. Dále pak jsou popsány nástroje, kterými je možné měřit zpoždění a následně je navrhnuta a zhotovená webová stránka. Pomocí této stránky je změřeno zpoždění na vybrané IP adresy.

KLÍČOVÁ SLOVA

Zpoždění, latence, ping, Arping, Hping

ABSTRACT

The aim of this thesis is the network communication delay measurement. The different delay reasons in network transfer are dealt successively as well as measuring tools are described. As the result a gauging web page is designed, programed and in conclusion, specified IP addresses access delay is measured.

KEYWORDS

Delay, latency, ping, Arping, hping

BEDNÁŘ, Vít *Měření komunikačního zpoždění v IP sítích*: bakalářská práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2015. 50 s. Vedoucí práce byl doc. Ing. Dan Komosný, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Měření komunikačního zpoždění v IP sítích“ jsem vypracoval(a) samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor(ka) uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil(a) autorská práva třetích osob, zejména jsem nezasáhl(a) nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom(a) následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autora(-ky)

PODĚKOVÁNÍ

Velmi děkuji vedoucímu mé semestrální práce doc. Ing. Danu Komosnému, Ph.D., za účinnou metodickou, pedagogickou a odbornou pomoc při zpracování mé bakalářské práce.

Brno ....

podpis autora(-ky)

Faculty of Electrical Engineering
and Communication
Brno University of Technology
Purkynova 118, CZ-61200 Brno
Czech Republic
http://www.six.feec.vutbr.cz

PODĚKOVÁNÍ

Výzkum popsaný v této bakalářské práci byl realizován v laboratořích podpořených z projektu SIX; registrační číslo CZ.1.05/2.1.00/03.0072, operační program Výzkum a vývoj pro inovace.

Brno . . . . . .

. . . . . .
podpis autora(-ky)

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

OP Výzkum a vývoj
pro inovace

OBSAH

1 Úvod **11**

2 Zpoždění v internetu **12**
2.1 Vznik zpoždění 12
2.2 Typy zpoždění 12
2.2.1 Zpoždění v koncových uzlech 13
2.2.2 Zpoždění na mezilehlých zařízeních 14
2.2.3 Zpoždění na přenosových linkách 14

3 Nástroje pro měření zpoždění **15**
3.1 Protokoly využívané pro měření zpoždění 15
3.1.1 Protokol ICMP 15
3.1.2 Protokol ARP 16
3.1.3 Protokol TCP 19
3.1.4 Protokol UDP 23
3.2 PING 24
3.3 ARPING 26
3.4 HPING 27

4 Zhotovený program pro měření latence **29**
4.1 Popis funkce programu pro měření latence 29
4.1.1 Vývojový diagram 30
4.1.2 Popis kódu 30
4.2 Vykonávání příkazů s právy uživatele Root 34
4.3 Úprava programu pro automatizované měření 34
4.4 Program pro měření latence přes webové rozhraní 35

5 Analýza výsledků **37**
5.1 Porovnání změřeného zpoždění získaných různými metodami 37
5.2 Měření zpoždění v průběhu jednoho dne 39

6 Závěr **44**

Literatura **45**

Seznam symbolů, veličin a zkratek **47**

Seznam příloh **48**

A Seznam IP adres **49**

B Obsah přiloženého CD **50**

SEZNAM OBRÁZKŮ

2.1 Zdroje zpoždění a místo vzniku [1]. 12
2.2 Síťový model TCP/IP a ISO/OSI. 13
3.1 Zdrojová stanice i cílová v lokální síti. 18
3.2 Zdrojová i cílová stanice v jiné síti. 19
3.3 ARP tabulka. 20
3.4 Průběh komunikace ARP protokolu. 20
3.5 Navazování spojení TCP. 22
3.6 ukončení spojení TCP. 23
3.7 Funkce Ping. 25
3.8 Příklad programu ping. 26
3.9 Příklad použití ARPING. 27
3.10 Příklad použití progamu Hping 28
4.1 Webová stránka 30
4.2 Vývojový diagram 31
4.3 Ukázka kódu: provedení měření pomocí programu Ping 32
4.4 Ukázka kódu: Provedení měření pomocí programu ARPING 33
4.5 Ukázka kódu: Provedení měření pomocí programu HPING - TCP ACK 33
4.6 Ukázka kódu: Provedení měření pomocí programu HPING - TCP FIN 33
4.7 Ukázka kódu: Provedení měření pomocí programu HPING - TCP SYN 34
4.8 Ukázka kódu: Provedení měření pomocí programu HPING - UDP . . 34
4.9 Ukázka kódu: provádění automatického měření 35
4.10 Ukázka kódu: provádění měření v projektu 36
5.1 Úspěšnost meření 37
5.2 Průměrné zpoždění různých metod 38
5.3 Zpoždění pomocí ping za 24 hodin 39
5.4 Průměrné hodnoty zpoždění pomocí TCP s příznakem ACK 40
5.5 Průměrné hodnoty zpoždění pomocí TCP s příznakem SYN 41
5.6 Průměrné hodnoty zpoždění pomocí UDP 42
5.7 Zpoždění za 24 na ceskatelevize.cz 42
5.8 Zpoždění pomocí všech metod za 24 hodin 43

SEZNAM TABULEK

3.1 Vybrané typy ICMP zpráv [12]. 15
3.2 Formát zprávy Echo request a Echo reply. 16
3.3 Formát zprávy paketu protokolu ARP 16
3.4 Segment TCP. 21
3.5 Datagram protokolu UDP 23
5.1 Průměrní zpoždění 38
5.2 Rozdíl průměrných hodnot jednotlivých metod měření 39
5.3 Srovnání PING a ARPING 39
5.4 Směřodatná odchylka pro měření během jednoho dne 41
A.1 Seznam IP adres pro měření 49

1 ÚVOD

Počítačové sítě jsou dnes velmi rozšířené a téměř každý se s nimi setkal. Většina uživatelů sítě si nedokáže představit, co vše se musí vykonat, než se jim potřebná data doručí, či začne fungovat nějaká internetová služba. Mezi hlavní kvalitativní parametr počítačových sítí patří zpoždění (latence), jež ovlivňuje kvalitu služeb a rychlost připojení. Pojem zpoždění je v počítačových sítích čas, který stráví zpráva na cestě k cíli. Jak velké zpoždění bude, ovlivňuje řada vlastností přenosové sítě, je však vždy snaha o to, aby jeho velikost byla co nejmenší.

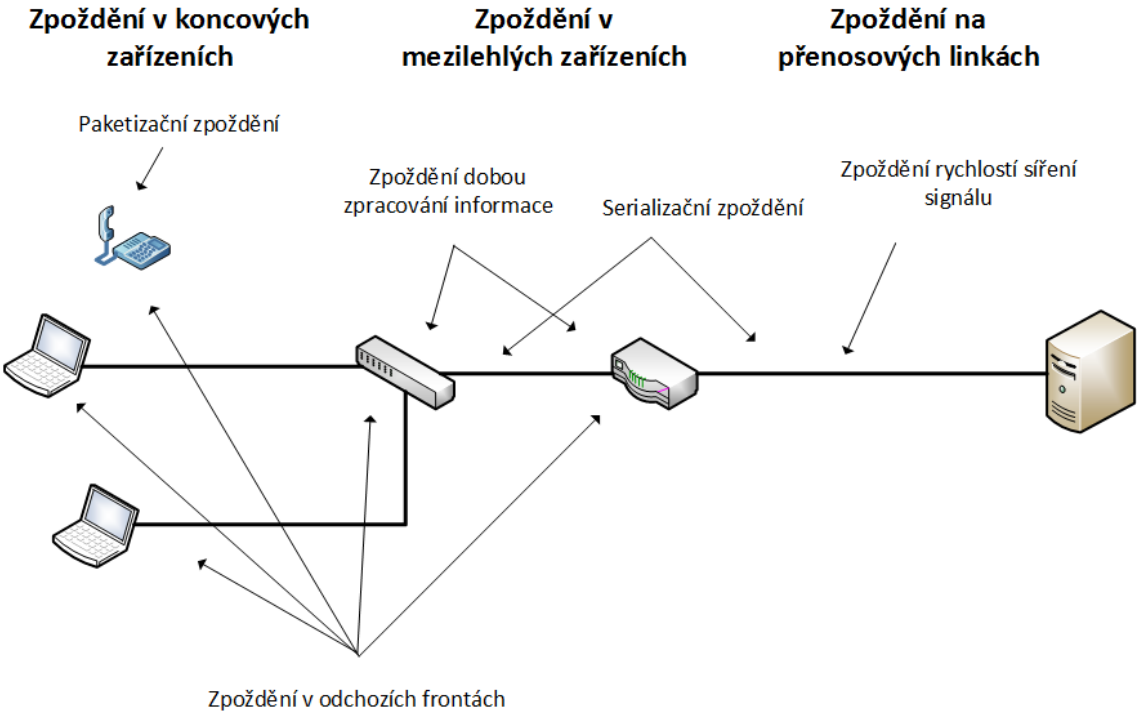
Tato práce se zabývá principem vzniku zpoždění na koncových zařízeních, na přenosových uzlech, na mezilehlých zařízeních a přenosových linkách. Tyto druhy jsou teoreticky rozebrány a zhodnocen jejich podíl na celkovém zpoždění. Dále jsou popsány principy nástrojů určené k měření zpoždění, v kap. 3.2 PING, v kap. 3.3 ARPING a Hping v kap. 3.4. Navržený a zhotovený program využívá zmíněných nástrojů pro měření zpoždění. Pomocí tohoto programu lze měřit zpoždění na různé stanice s využitím různých nástrojů, také lze provádět automatizované měření v časových intervalech.

Prakticky je provedeno několik měření z nichž první je popsáno v kap. 5.1 a zabývá se rozdíly úspěšnosti měření jednotlivých nástrojů a velikosti změřeného zpoždění. V dalším měření popsané v kap. 5.2 je zkoumána změna zpoždění na vybrané stanice v průběhu pracovního dne.

2 ZPOŽDĚNÍ V INTERNETU

2.1 Vznik zpoždění

Zpoždění je obecně čas, který potřebuje nějaká zpráva na to, aby se dostala od zdroje, který zprávu vygeneroval až k příjemci zprávy. V počítačových sítích je to doba od vyslání dat (datové zprávy) k přijmu dat na cílové stanici. Často se v počítačových sítích používá místo výrazu zpoždění výrazu latence. Velikost zpoždění závisí na vlastnostech sítě. Zpoždění vznikající na jednotlivých částech komunikačního řetězce má různý charakter, velikost i vliv na celkové zpoždění. Proto je vhodné vědět, kde k jakému zpoždění na přenosové cestě dochází a co ho způsobuje [1].



Obr. 2.1: Zdroje zpoždění a místo vzniku [1].

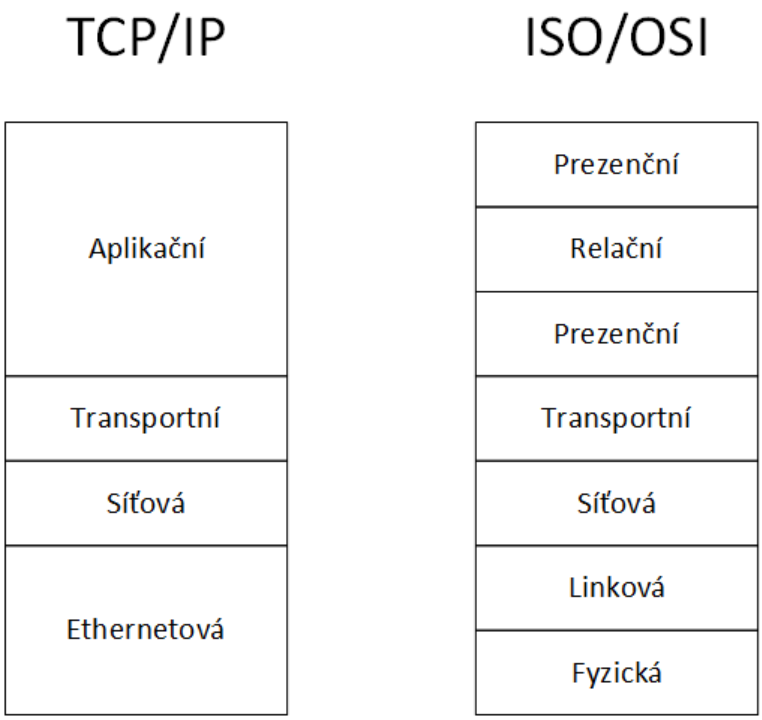
2.2 Typy zpoždění

Zpoždění lze rozdělit na deterministické a stochastické zpoždění. Deterministické zpoždění lze vypočítat, jedná se o minimální čas potřebný k přenosu zprávy. Stochastické zpoždění se mění a je závislé na aktuálním stavu sítě např. zatížení (nelze vypočítat) [6].

Velikost celkového zpoždění je dána součtem dílčích zpoždění, jež vznikají od vygenerování zprávy až po její doručení. Důležité je také vědět, jak se tyto dílčí zpoždění podílejí na výsledné velikosti zpoždění. Vlivy jednotlivých zpoždění jsou popsány dále.

2.2.1 Zpoždění v koncových uzlech

Jako koncové zařízení chápeme zdroj nebo příjemce zprávy, jejich typickým příkladem jsou osobní počítače, servery a poslední dobou příjemci zvuku a videa (VoIP telefony, Smart TV, další chytrá zařízení). Zařízení (aplikace) předpřipraví data k odeslání, data postupují vrstvami ISO/OSI, v IP sítích vrstvami TCP/IP. Model ISO/OSI a TCP/IP je uveden na obr. 2.2. Na síťové vrstvě jsou data označena svoji zdrojovou a cílovou IP adresou a jsou zabalena do paketu, na ethernetové vrstvě se zapouzdří paket do rámce či buňky a vyšle se bit po bitu na přenosovou linku. Přijímací stanice provede stejný postup v opačném pořadí. V dalších částech budeme uvažovat zpoždění, které vzniklo jen na 3. a nižší vrstvě ISO/OSI modelu.



Obr. 2.2: Síťový model TCP/IP a ISO/OSI.

2.2.2 Zpoždění na mezilehlých zařízeních

Mezilehlé zařízení je aktivní síťové zařízení sloužící k rozličným úkolům na cestě mezi zdrojovou a cílovou stanicí. Mezi nejdůležitější úkoly patří směrování a přepínání, čili přeposílání datových jednotek na nejkratší, či nejvýhodnější cestu k cíli. Aktivní síťová zařízení pracují na různých vrstvách TCP/IP modelu. Na ethernetové vrstvě pracují HUBy a switche (přepínače), na síťové pracují routery (směrovače). Některé switche mohou pracovat i na síťové vrstvě TCP/IP modelu [3].

Zpoždění způsobené prvky na ethernetové vrstvě je zanedbatelné 1–10 µs. Zpoždění způsobené přepínači je několikanásobně vyšší, přibližně je to asi 10-100 µs [5].

Na zpoždění v mezilehlých uzlech se podílí i doba strávená ve stupních a výstupních frontách. Doba zpoždění ve vstupní frontě ovlivňuje příchozí rychlost linky a velikost paketu. Čas, který zařízení potřebuje k přenosu datové jednotky (paketu, rámce, bitu) ze vstupu na výstup, závisí na výkonu daného prvku a zatížení sítě. Při velkém zatížení prvků může být zpoždění rovno několikanásobku oproti zpoždění na nezatíženém prvku, zvláště pak na směrovačích. Přesné hodnoty tohoto zpoždění způsobené těmito prvky lze zjistit z dat uváděných výrobcem nebo měřením daného zařízení.

2.2.3 Zpoždění na přenosových linkách

Přenosové linky ovlivňují výsledné zpoždění rychlostí šíření signálu v médiu a také svojí délkou. Je závislé na fyzické poloze jednotlivých stanic. Linky mezi stanicemi nejsou zpravidla vedeny nejkratší možnou trasou, ale kopírují jiné stavby, jakou jsou např. dálnice, železnice a dálkové vedení elektrické energie. Na celkovou vzdálenost má vliv i cenová politika směrování. Datové jednotky se vždy nešíří nejkratší možnou cestou, z důvodu rozložení zátěže může být zvolena i delší cesta.

V optických kabelech, ze kterých se převážně skládají páteřní sítě i část přístupových sítí, se signál šíří téměř 2/3 rychlostí světla (c = 299 792 458 m/s). To dává v přepočtu rychlost šíření signálu v optickém médiu 194 895 km/s. V metalickém médiu se signál šíří 3/4 rychlostí světla [5].

3 NÁSTROJE PRO MĚŘENÍ ZPOŽDĚNÍ

Existuje několik nástrojů, pomocí kterých lze měřit zpoždění mezi stanicemi v IP sítích. Nejznámější a nejvíce užívaný je nástroj PING, dále pak byl zvolen program HPING a ARPING. Většina z nich pracuje jen v příkazové řádce. Existuje ale řada nástaveb jak online http://ping.eu/ping/ tak programy s grafickým prostředím např.: r4G3 Pinger.

Z důvodu toho, že pro měření zpoždění se využívá kromě ICMP protokolu i protokol ARP, TCP a UDP, jsou v následujících kapitolách tyto protokoly popsány.

3.1 Protokoly využívané pro měření zpoždění

3.1.1 Protokol ICMP

Protokol ICMP (*Internet Control Message Protocol – protokol služebních hlášení*) je servisní protokol a nepřenáší žádná uživatelská data. Umožňuje signalizaci mimořádných událostí v síti a testování dostupnosti. Přenáší informace o chybách v datagramech, zjišťování doplňujících informací a také k ověření komunikace mezi stanicemi.

Zprávy protokolu ICMP se dělí na dvě skupiny. První slouží k zasílání chyb o nějakém nestandardním stavu při doručování IP datagramů (*error-reporting messages*). Druhá skupina je určena k dotazování, typicky k testování konektivity (*query messages*).

Vybrané zprávy ICMP protokolu:

Hlášení chyb

Typ	**Zpráva**
3	nedoručitelný IP datagram (destination unreachable)
4	snížení rychlosti odesílání (source quench)
5	přesměrování (redirection)
11	vypršení doby života (time exceeded)
12	problém s parametry (parameter problem)

Dotazování

Typ	**Zpráva**
8	žádost na odpověď (echo request)
0	odpověď na žádost o odezvu (echo reply)
13	požadavek na časové razítko (timestamp request)
14	odpověď na časové razítko (timestamp reply)

Tab. 3.1: Vybrané typy ICMP zpráv [12].

V Tab. 3.2 je uveden formát zprávy ECHO request a Echo reply.

Tab. 3.2: Formát zprávy Echo request a Echo reply.

Počet bitů:

8	8	16
Typ = 8 (echo request) nebo 0 (echo reply)	**Kód** = 0	**Kontrolní součet**
Identifikátor		**Pořadové číslo**
Volitelná data		

3.1.2 Protokol ARP

Transformaci adresy vyšší úrovně na adresy nižší úrovně, tedy nalezení fyzické adresy MAC k IP adrese řeší protokol ARP. Tuto transformaci řeší pomocí tabulky dočasných záznamů (cache).

Základní vlastnosti ARP

- slouží k nalezení neznámé fyzické (MAC) adresy v lokální sítí, pokud je známa IP adresa, obecně na základě adresy třetí úrovně zjištění adresy druhé úrovně.

- informace o odpovídajících adresách jsou uloženy v tabulkách, jsou zde uloženy pouze na několik minut, podle potřeby se obnovují nebo jsou vymazány na základě probíhajících změn v síti

Počet bitů:

8	8	16
Typ přenosového media		**Typ protokolu**
Délka adresy MAC	**Délka síťové adresy**	**Kód zprávy 1=REQ 2=RESP**
Zdrojová MAC		
Zdrojová síťová adresa		
Cílová adresa MAC		
Cílová síťová adresa		

Tab. 3.3: Formát zprávy paketu protokolu ARP

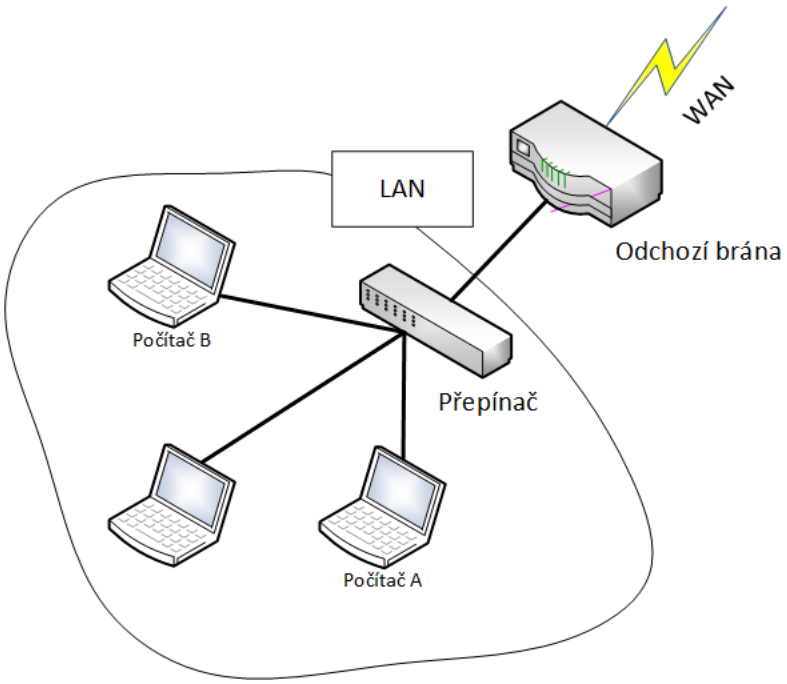
V tabulce 3.3 je uveden formát ARP paketu [12].

- **Typ přenosového media** (*Hardware type*) - 16 bitů indikuje typ použitého media resp. spojové technologie např. pro Ethernet je hodnota 0x0001, ATM má 0x0010.
- **Typ protokolu** (*Protocol type*) - 16 bitů indukuje typ vyššího protokolu v rámci něhož se logická adresa používá, pro IP je hodnota 0x8000.
- **Délka fyzické adresy MAC** (*(Hardware length)*) - 8 bitů, délka fyzické adresy v bajtech, pro Ethernet 0x06.
- **Délka síťové adresy**(*Protocol length*) - 8 bitů, délka logické adresy taktéž v bajtech, pro IPv4 adresu 0x04.
- **Kód zprávy** (*Operation*) - 16 bitů specifikuje operaci, kterou odesílatel provedl - 0x0001 pro žádost a 0x0002 pro odpověď.
- **Zdrojová / hledaná MAC** (*Sender / target hardware address*) - obsahuje fyzickou adresu zdroje / hledanou, délka je specifikována v poli *délka fyzické adresy.*
- **Zdrojová / hledaná síťová adresa** (*Sender / target logical address*) - obsahuje síťovou adresu zdroje / hledanou, délka je specifikována v poli *délka síťové adresy* [12].

Princip funkce ARP protokolu - jeden síťový segment

V jednom síťovém segmentu máme dva počítače. Zdrojová stanice - počítač A a cílová stanice - počítač B viz obr. 3.1. Předpokládáme, že počítače mohou mezi sebou komunikovat přímo. Každý má fyzikou adresu MAC_A a MAC_B a síťovou adresu IP_A a IP_B. Jestliže dostane síťová vrstva počítače A požadavek od transportní vrstvy přenést data na adresu počítače B tedy B_IP, musí být schopna zajistit převod z IP_B na MAC_B.

Počítač A nejprve prozkoumá svoji arp tabulku, kde jsou uloženy záznamy fyzických a síťových adres (arp cache). Pokud v ní nenajde odpovídající záznam, musí použít protokol ARP. Počítač A tedy vyšle žádost protokolu ARP s informacemi o zdrojové fyzické a síťové adrese (MAC_A a IP_A) a hledanou síťovou adresou (IP_B) a směruje je všem stanicím v lokání síti (tzv broadcast). Všechny stanice zprávy přijmou, ale odpoví pouze stanice s hledanou IP adresou tedy v našem případě stanice s B_IP (počítač B). Počítač B odpoví zprávou *reply*, do které vyplní pole hledané fyzické adresy MAC_B a pošle na adresu zdrojové adresy (MAC_A). Počítač B si zkontroluje vlastní ARP tabulku zda ji nedoplnit o dvojici adres získaných v žádosti ARP (MAC_A a IP_A)



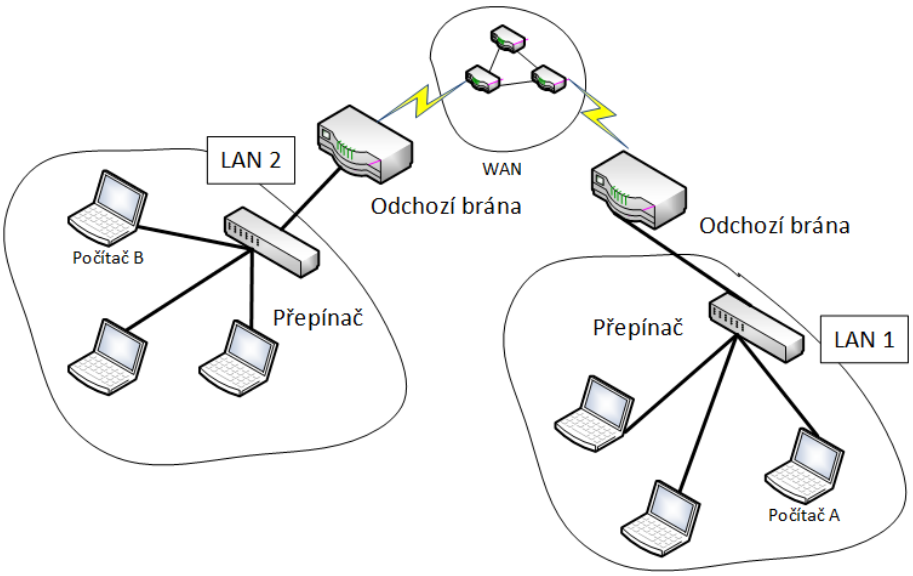
Obr. 3.1: Zdrojová stanice i cílová v lokální síti.

Princip funkce ARP protokolu - dva síťové segmenty

Stejný případ jako v předchozím příkladu, s tím rozdílem že stanice nejsou v jednom síťovém segmentu. Pokud se hledaná cílová stanice nenachází v lokální síti, je zaslán rámec na fyzickou adresu výchozí brány (*default gateway*). Pokud počítač A nezná adresu výchozí brány zjistí ji stejným způsoben jako v předešlém příkladu (pomocí protokolu ARP). Výchozí brána odešle paket směrem do sítě, kde se nachází cílová adresa IP_B.

ARP tabulka

Jak bylo zmíněno protokol ARP využívá ke své funkci tabulku, v ní jsou dvojce adres - IP adresa a fyzická adresa. Na obr. 3.3 je uveden příklad takovéto tabulky. Pokud bude chtít stanice poslat paket na adresu např. 192.168.1.1, v tabulce najde odpovídající záznam a doplní cílovou adresu v rámci tj. bc-c8-10-4f-ee-1d. V posledním sloupci je uveden způsob jakým byl záznam získán. Pokud je uvedeno dynamicky, znamená to, že k vytvoření záznamu byl použit ARP protokol. Adresy od 5. řádku jsou speciální tj. 5.-8. řádek multicastové adresy a na posledním řádku je broadcastová adresa.



Obr. 3.2: Zdrojová i cílová stanice v jiné síti.

3.1.3 Protokol TCP

Transmission Control Protocol (TCP) je transportní protokol pracující se spojením. Poskytuje logické spojení mezi aplikacemi, tedy poskytuje spolehlivý přenos dat. TCP využívají ke své funkci aplikační protokoly vyžadující spolehlivou transportní službu a nevadí jim větší režie přenosu, jako jsou například FTP, TELNET, SMTP. TCP přijímá od vyšších vrstev souvislý tok bytů (byte stream), který rozděluje do segmentů.

Vlastnosti TCP

- **Spolehlivá transportní služba** - kladné potvrzení přijatých dat a opětovné poslání špatně doručených.
- **Služba se spojením** - před přenosem je navázáno spojení a po ukončení je rozvázáno.
- **Efektivní využití přenosových kanálů** - při vysílání se využívá vyrovnávacích kanálů.
- **Komunikace proces - proces** - pomocí portů.

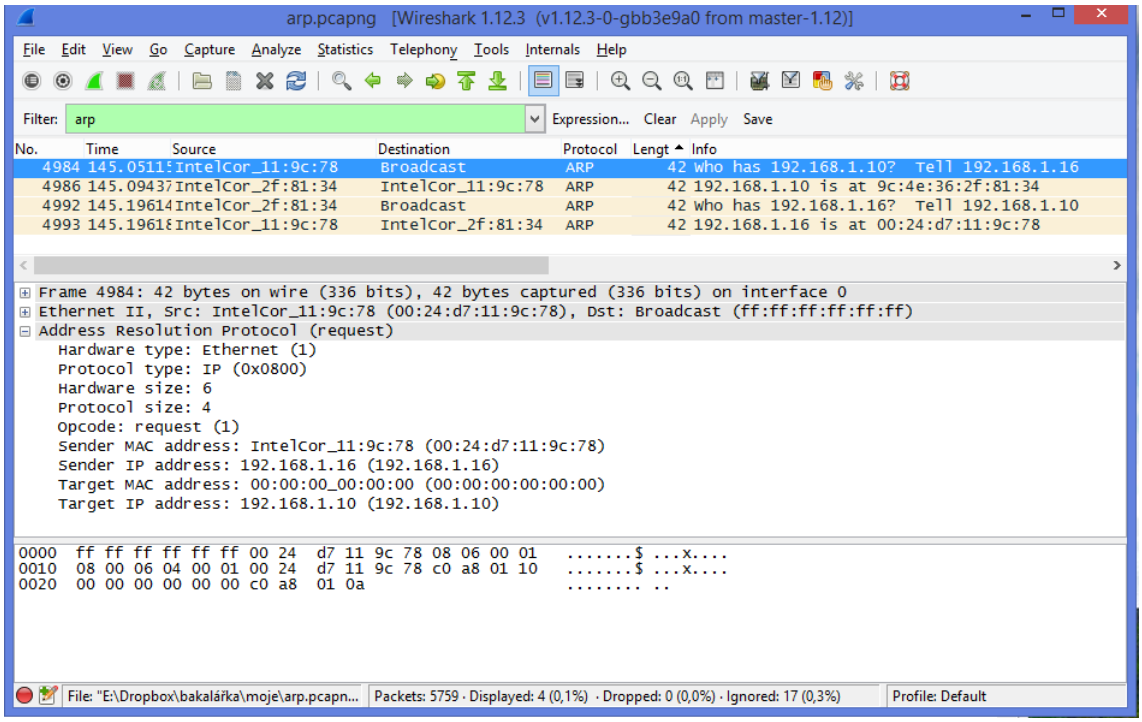
Záhlaví segmentu TCP obr. 3.4 obsahuje následující pole:

- Zdrojový port (*source port*) – identifikuje zdrojový aplikační proces.
- Cílový port (*destination port*) - identifikuje cílový aplikační proces.
- Pořadové číslo (*sequence number – SEQ*)– pořadové číslo prvního z odesílaných bajtů v daném segmentu .

```
C:\Users\vít>arp -a

Interface: 192.168.1.16 --- 0x4
  Internet Address      Physical Address      Type
  192.168.1.1           bc-c8-10-4f-ee-1d     dynamic
  192.168.1.10          9c-4e-36-2f-81-34     dynamic
  192.168.1.14          68-5d-43-44-36-7b     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  224.0.0.253           01-00-5e-00-00-fd     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Obr. 3.3: ARP tabulka.



Obr. 3.4: Průběh komunikace ARP protokolu.

Počet bitů:

4	6	6	8	8
Zdrojový port			**Cílový port**	
Pořadové číslo				
Číslo potvrzeni				
Délka hlavičky	**Rezervováno**	**Příznakové bity**	**Šířka okna**	
Kontrolní součet			**Označení urgentních dat**	
Volitelné možnosti				**Výplň**
Data				

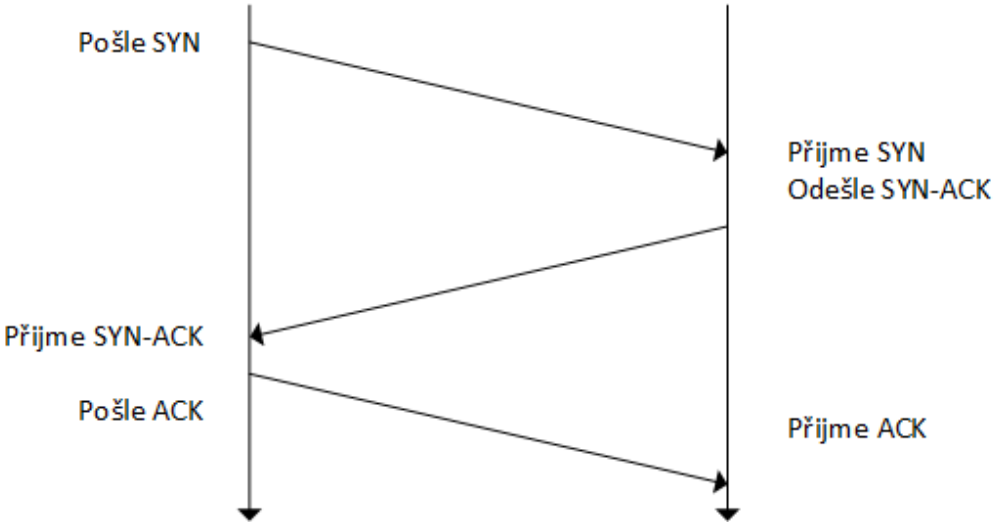
Tab. 3.4: Segment TCP.

- Číslo potvrzení (*acknowledgment number*) – specifikuje pořadové číslo dat, které očekává jako následující.
- Délka záhlaví - délka celého záhlaví v násobku 32 bitů.
- Příznakové bity - Funkce řízení, mohou být různě kombinovány.
  - URG – označuje urgentní data.
  - ACK – označuje platnost pole s číslem potvrzení.
  - PSH – označuje segment, který přenáší data.
  - RST – požaduje okamžité ukončení spojení.
  - SYN – žádost o navázání spojení, odesílatel začíná novou sekvenci číslování.
  - FIN – žádost o ukončení spojení - odesílatel ukončil přenos dat.
- Šířka okna (*window size*)– velikost okna (maximální počet bajtů, které může vysílač poslat aniž by čekal na potvrzení od přijímače.
- Kontrolní součet (*TCP checksum*).
- Označení urgentních dat (*urgent pointer*) - jen když je nastaven příznak URG.
- Volitelné možnosti (*options*).

Navazování spojení a přenos dat

Před každým přenosem podporovaným protokolem TCP musí předcházet povinná výměna tří segmentů v rámci fáze navazování spojení – mechanizmus trojitého potřásání rukou (three way handshaking). Příklad navazování spojení a počátku komunikace obr. 3.5:

1. klient vysílá: SYN ISN = 50
2. server vysílá: SYN ISN= 99, ACK = 51
3. klient vysílá: ACK = 100
4. klient vysílá: byty 51-100
5. server vysílá: ACK = 101
6. klient vysílá: byty 101-150



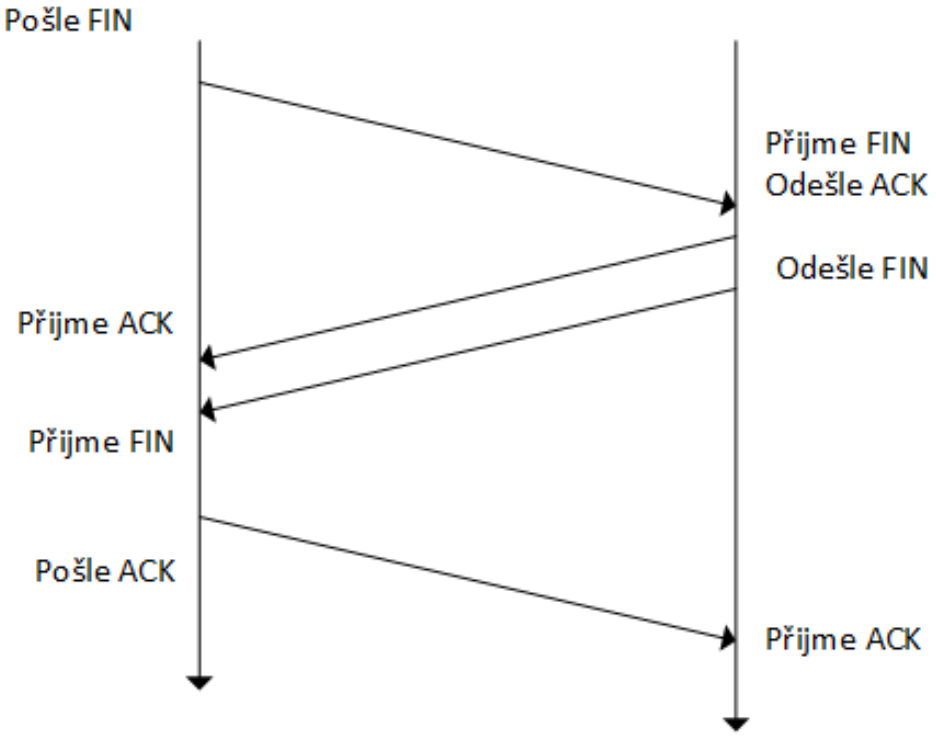
Obr. 3.5: Navazování spojení TCP.

Ukončení spojení

Musí být provedeno z obou stran. Nastaví se příznak FIN, ten musí být druhou stranou potvrzen jako jakýkoliv jiný segment.

Klient žádá o ukončení spojení obr. 3.6:

1. klient vysílá: FIN ISN = x
2. server vysílá: ACK = x+1 a FIN ISN = y
3. klient vysílá: ACK = y+1
4. server příjme: ACK = y+1



Obr. 3.6: ukončení spojení TCP.

3.1.4 Protokol UDP

User Datagram Protocol (UDP) je jednoduchý transportní protokol. Poskytuje nespolehlivou transportní službu bez spojení. UDP využívají aplikační protokoly SNMP a DHCP atd. Aplikační program využívající UDP musí převzít kontrolu chyb, duplicity zpoždění, dodání mimo pořadí nebo ztrátu konektivity. UDP podporuje vysílání na všeobecnou (broadcast) adresu IP a na skupinové adresy (multicast).

Počet bitů	
16	16
Zdrojový port	**Cílový port**
Délka	**Kontrolní součet**
Data	

Tab. 3.5: Datagram protokolu UDP

- Zdrojový port – identifikuje zdrojový aplikační proces
- Cílový port - identifikuje cílový aplikační proces
- Délka – označuje délku celého segmentu v násobcích 32
- Kontrolní součet – provádí zabezpečení přes celý segment

Vlastnosti protokolu UDP

- **Komunikace proces-proces** - pomocí socketových adres, resp. zejména portů.
- **Přenos dat bez spojení** - každý datagram je přenášen jako samostatná jednotka
- **Žádné řízení toku dat** - Vysílač může zahltit příjemce či síť. Nejsou mechanizmy na řešení těchto problémů kromě kontrolního součtu

3.2 PING

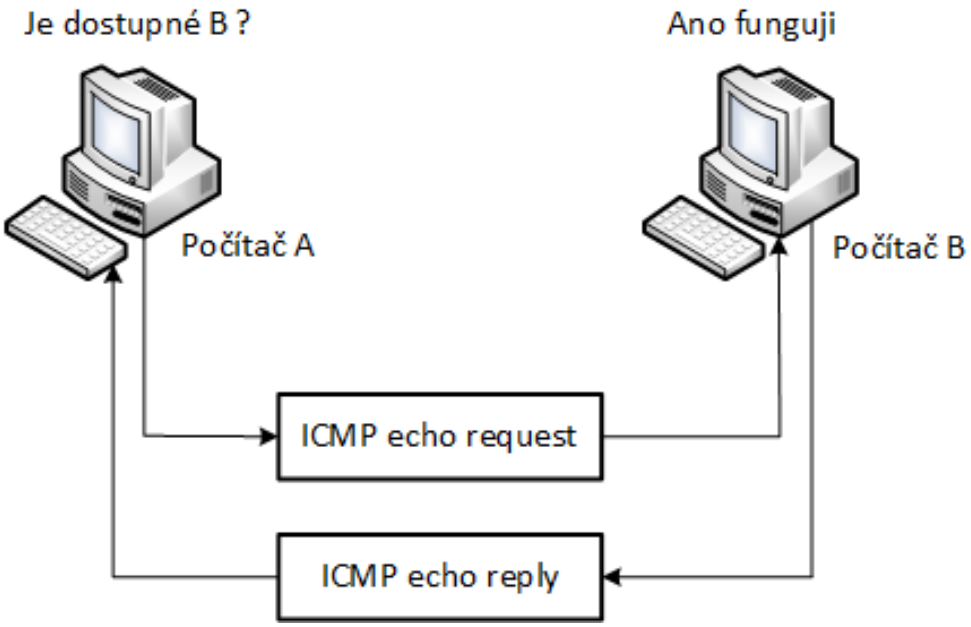
Ping (Packet Internet Groper) využívá ke své funkci ICMP protokol popsaný v kap. 3.1.1 k zjištění dostupnosti cílové stanice sítě a změření zpoždění na tuto stanici. Ping pracuje na nejnižší možné vrstvě a je implementován v operačním systému. Na základě vyslání zprávy ICMP typu echo reguest s IP adresou cílové stanice očekává od cíle potvrzení o funkčnosti a dosažitelnosti stanice, typ zprávy ICMP Echo reply obr. 3.7.

Parametry zprávy ICMP echo reply:

Kód	**Význam**
1	Network unreachable = síť je nedostupná.
2	Host unreachable = stanice je nedosažitelná.
3	Protocol unreachable = port je nedosažitelný.
4	Fragmentation needed and DF set = pokud je nutno paket fragmentovat, ale příznak Don't Fragment je nastaven.
5	Source failed = odesílatelem požadované směrování selhalo.
6	Destination network unknown = cílová síť není známa.
7	Destination host unknown = cílový počítač není znám.

Je třeba rozlišovat mezi typy dostupnosti nebo nedostupnosti cíle.

- Nedostupná síť - informace od směrovače na cestě k cíli, ohlašuje problémy se směrováním v síti.
- Nedostupná stanice - informace od posledního směrovače na cestě k cíli, ohlašuje problémy s doručením datagramu.
- Nedostupný port - informace od cílové stanice, která je funkční, ale dotazovaný port není dostupný.



Obr. 3.7: Funkce Ping.

Zpoždění změřené pomocí PING zahrnuje v sobě výše zmíněné druhy zpoždění. Zprávy ping nabírají také zpoždění při každém průchodu směrovačem ve vstupních a výstupních frontách, kde nejsou zpracovávány prioritně spíše naopak. Některé firewally mohou zprávy ICMP protokolu blokovat a proto není vhodné je používat na rozsáhlých sítích pro zjištění zátěže. Ping nelze ztotožnit s rychlostí reakce na konkrétní aplikace [10].

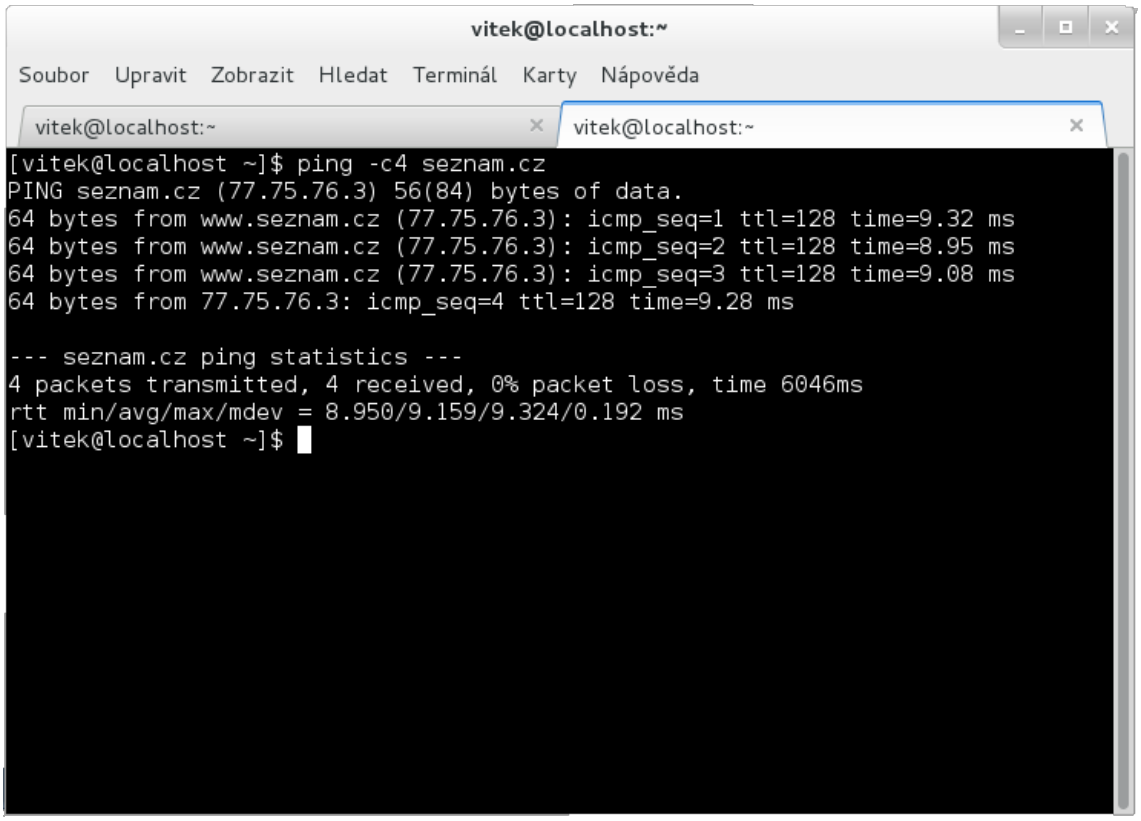
Ukázka funkce programu PING

Program Ping se spouští z příkazového řádku. V MS Windows program PING pošle implicitně 4 ICMP dotazy a poté vypíše statistiku úspěšnosti. OS Linux vysílá ICMP dotazy a přijímá odpovědi, dokud není zastaven uživatelem [6] . V obou OS je možné tyto hodnoty měnit a použít dalších parametrů.

Zde jsou popsány základní funkce v prostředí LINUX:

ping [volby] **IP adresa**,

–a	provede rozlišení adresy na jméno
–n	počet provede příslušný počet pokusů o odpověď
–l	velikost vyrovnávací paměti k odesílání
–f	nastavuje příznak Nefragmentovat (don´t fragment)
–i	nastavuje TTL (Time To Live - maximální počet průchodů přes směrovač)
–w	zajišťuje prodloužení doby vypršení čekání na odpověď (timeout)



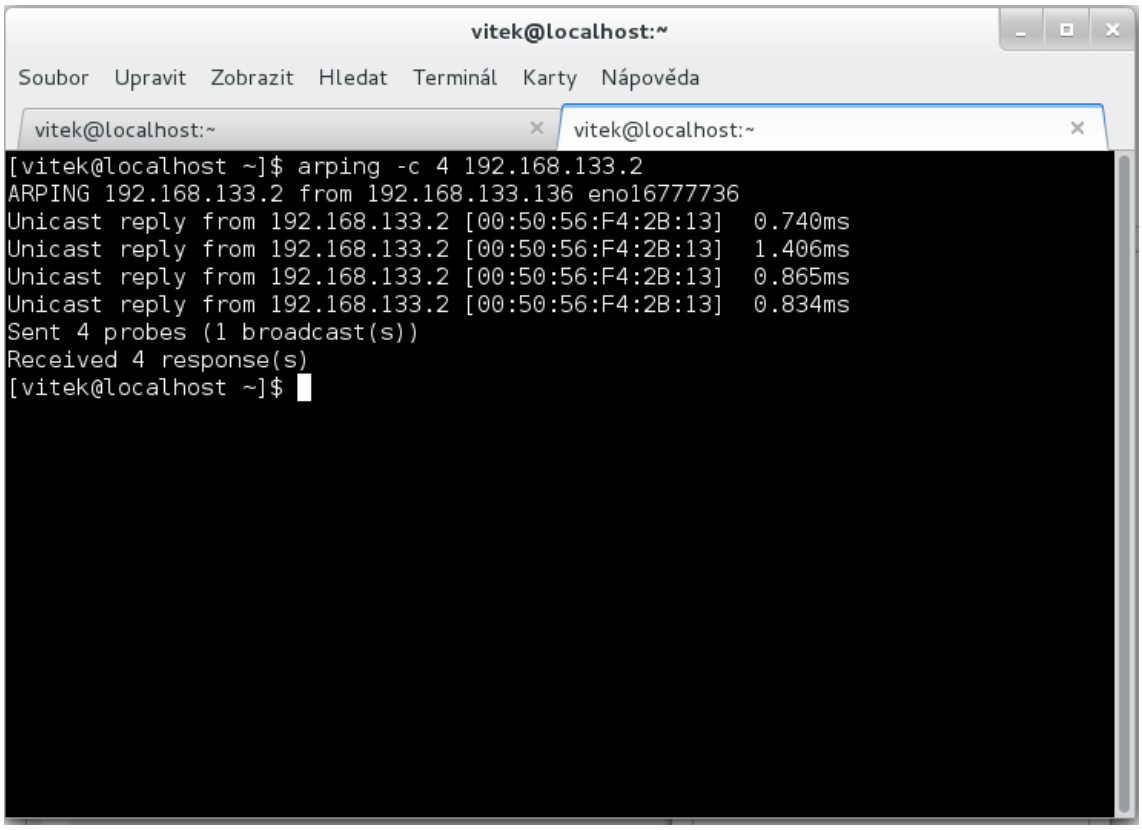
Obr. 3.8: Příklad programu ping.

3.3 ARPING

Jak bylo zmíněno výše, program PING nelze využít vždy. Některé firewall mohou ICMP pakety vyslané programem PING ignorovat nebo přímo zahazovat. Dalším problémem může být, že některá koncová zařízení v daném síťovém segmentu nemusí mít přidělenu IP adresu. Z těchto důvodu lze využít program ARPING využívající protokol ARP. Nevýhodou je, že umožňuje měřit zpoždění pouze na lokálním síťovém segmentu. Program ARPING umožňuje měřit zpoždění na zadanou IP adresu či adresu MAC.

Příklad použití ARPING

Program vyšle ARP dotaz s cílovou síťovou adresou IP či fyzickou adresou MAC a očekává odpověď. Typický příklad použití ARPING je na obr. 7. kde jsou vyslány



Obr. 3.9: Příklad použití ARPING.

celkem 4 dotazy na adresu 192.168.133.136. Po odeslání a přijetí program vypíše úspěšnost přijetí odpovědí na dotazy ARP.

Níže jsou uvedeny nejčastěji používané parametry nastavení ARPING

-b všechny ARP dotazy budou zasílány formou broadcast
–c 4 provede právě čtyři žádosti na zadanou adresu a skončí
–l vybere rozhraní, ze kterého se má příkaz provést
-s MAC – Nastaví zdrojovou MAC adresu

Parametry nastavení se mohou v různých verzích programu mírně lišit [3].

3.4 HPING

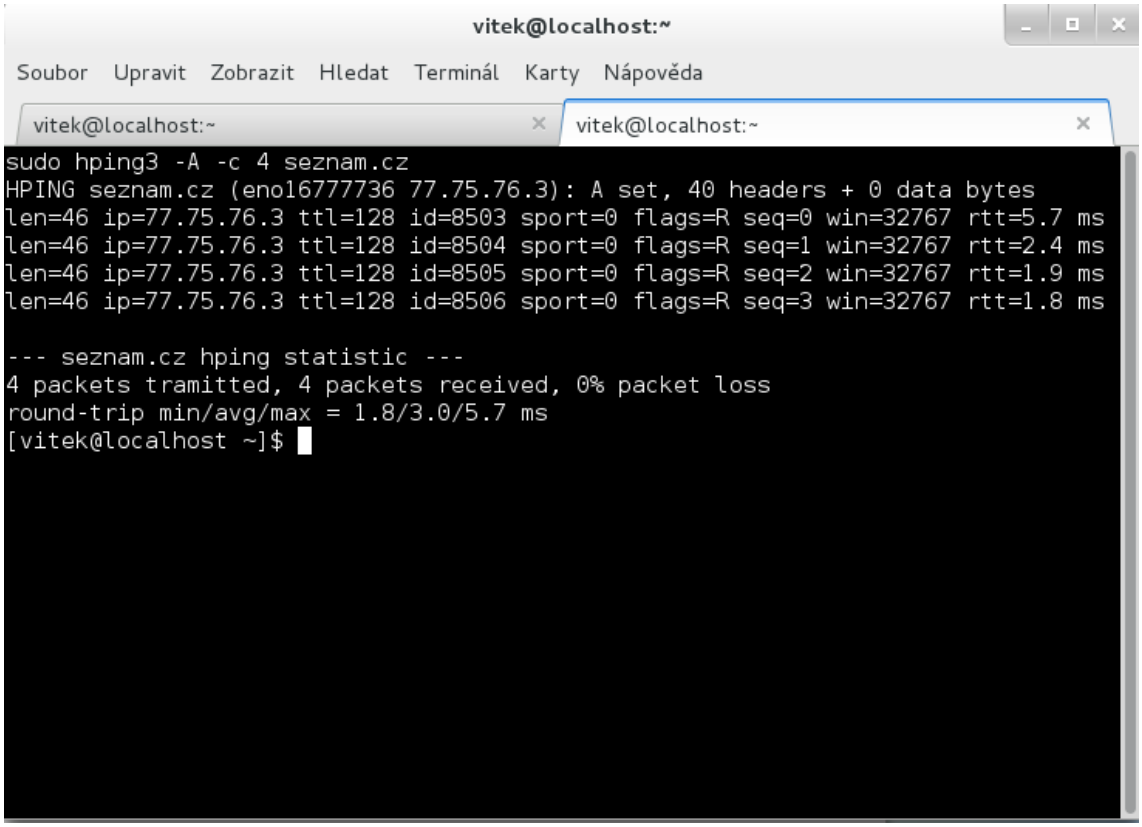
Hping je volně šiřitelný generátor a analyzátor TCP/IP paketů, který byl inspirován programem Ping. Podporuje protokoly TCP, UDP a ICMP. Může pracovat jako traceroute či jako PING. Pole záhlaví lze nastavovat pomocí parametrů [8].

Hping primárně slouží k testování firewall, pokročilé skenování portů a všeobecně k testování sítě.

Příklad použití HPING

HPING umožnuje nastavovat řídící příznaky TCP paketu

- -F – nastaví příznak FIN
- -S - nastaví příznak SYN
- -R - nastaví příznak RST
- -A - nastaví příznak ACK
- -U – nastaví příznak URG
- -1 - posílá ICMP zprávy
- -2 – posílá UDP pakety



Obr. 3.10: Příklad použití progamu Hping

Na obr. 3.10 Hping vysílá 4 TCP pakety s příznakem ACK na adresu seznam.cz. Program následně přijímá potvrzení a měří zpoždění od vyslání k přijetí zprávy. Na konci vypíše statistiku úspěšnosti a minimální, průměrné a maximální zpoždění.

4 ZHOTOVENÝ PROGRAM PRO MĚŘENÍ LATENCE

Protože výše uvedené programy pracují pouze v příkazové řádce, byla dle zadaní navrhnuta a zhotovena webová stránka. S využitím výše zmíněných nástrojů umožňuje webová stránka měřit zpoždění pomocí ICMP protokolu, ARP protokolu, TCP protokolu s možností zvolit příznaky řízení (*ACK, SYN, FIN*) a pomocí protokolu UDP.

Jelikož program HPING potřebuje ke své správné funkci práva uživatele root, proto bylo od původního plánu umístit hlavní stránku na školní server upuštěno a stránka v současnosti běží na minipočítači Raspberry PI 2. Na tomto zařízení je nainstalován systém Linux distribuce Rasbian (odnož distribuce DEBIAN), ta je uzpůsobena pro běh na tomto zařízení. V tomto systému je nainstalován webový server Apache2 a PHP server. Toto řešení nedisponuje velkým výkonem, je ale energeticky úsporné a pro účely této aplikace zcela dostačující.

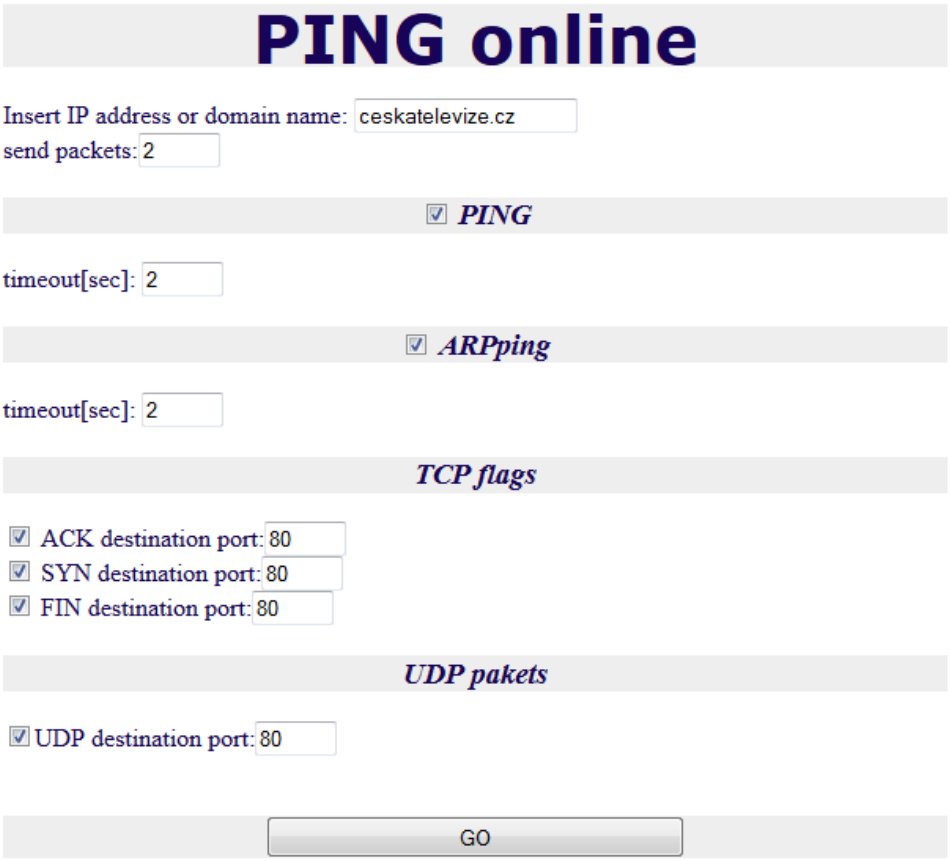
Webová stránka je napsána v jazyce PHP. PHP je skriptovací jazyk pro tvorbu dynamického obsahu webových stránek. Jazyk PHP provede skript přímo na straně serveru a klientovi je odeslán pouze výsledek provedeného skriptu na rozdíl od javascriptu. To lze s výhodou použít pro měření zpoždění na uživatelem zadanou IP adresu.

V rámci bakalářské práce byli vytvořeny celkem tři programy. Jeden program je umístěn na vlastním serveru a slouží pro porovnání různých metod měření. Další program slouží pro zjištění změny zpoždění během jednoho pracovního dne a poslední program je umístěn na školním serveru na adrese http://geolocation.utko.feec.vutbr.cz /xbedna54/, je součástí projektu, který se zabývá geolokací, na tomto projektu se podílejí studenti pod vedením doc. Ing. Dana Komosného, Ph.D, Tento program slouží pro měření zpoždění pouze nástrojem PING.

4.1 Popis funkce programu pro měření latence

Po načtení webové stránky obr. 4.1 se předvyplní IP adresa uživatele, který se připojil. Uživatel následně zadá IP adresu nebo doménové jméno např. centrum.cz, vyplní kolik dotazů se má poslat, následně si vybere jakým způsobem chce měřit zpoždění. Má na výběr měřit pomocí ICMP protokolu programem PING, kde lze nastavit dobu čekání na odpověď - timeout, dále pomocí protokolu ARP program ARPING (ten ale z principu své funkce pracuje pouze v lokální síti), dále pak pomocí protokolu TCP kde si muže zvolit příznaky řízení TCP spojení (ACK,SYN,FIN). Nakonec pomocí protokolu UDP. U protokolu TCP a UDP je možnost zvolit si cílový port.

Po kliknutí na tlačítko GO se postupně provedou jednotlivá měření. Poté se změřené zpoždění vypíše do tabulky a vypočte se průměrné zpoždění. Při neúspěšném měření se do tabulky vypíše *not available*.

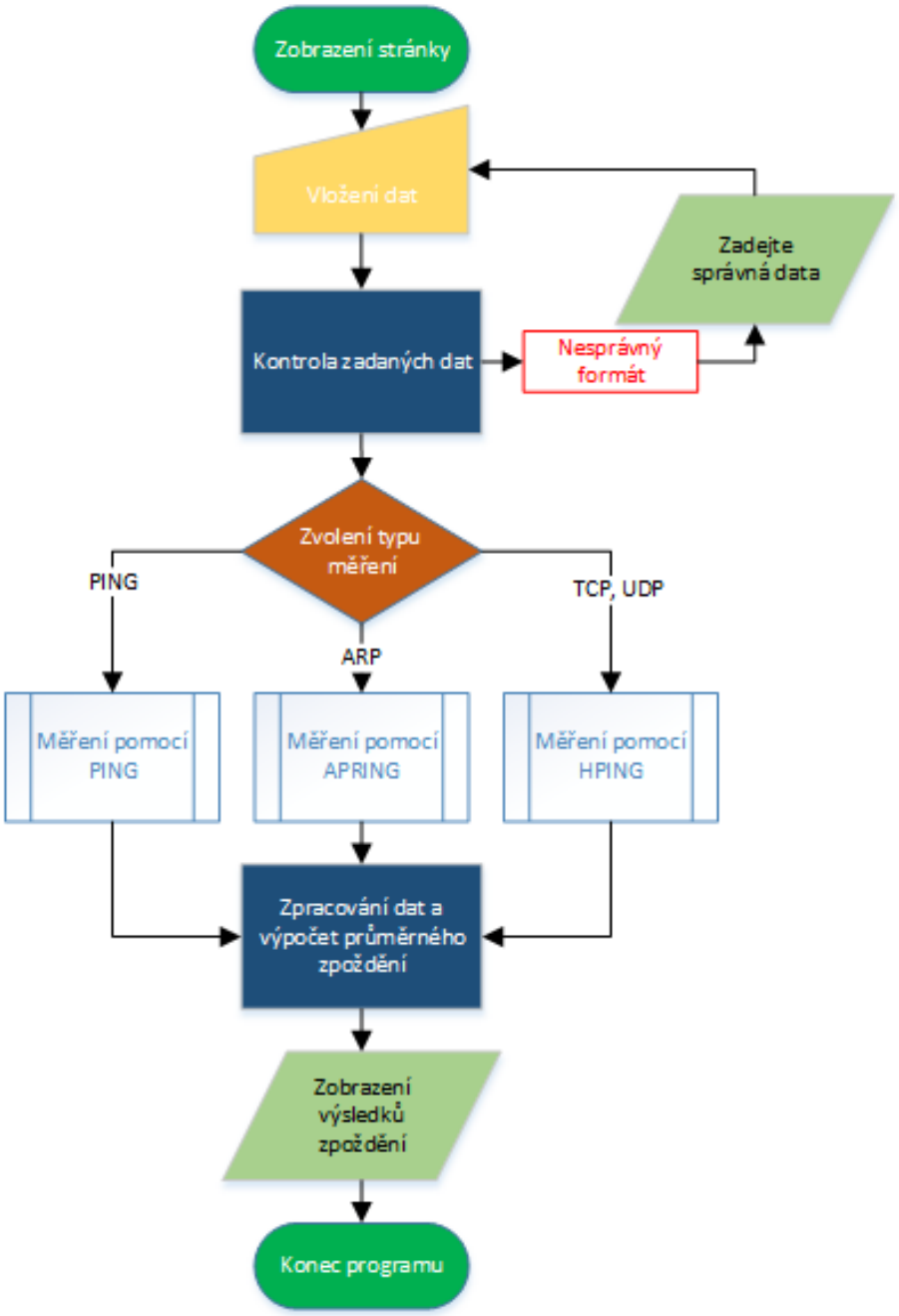


Obr. 4.1: Webová stránka

4.1.1 Vývojový diagram

4.1.2 Popis kódu

Do systému bylo nejdříve potřeba doinstalovat potřebné nástroje. Po načtení stránky se zjistí adresa klienta, který se připojuje a předvyplní se do formuláře. Po vyplnění stránky uživatelem se nejprve ověří správnost IP adresy či doménového jména pokud nevyhovuje vypíše hlášku *You must insert valid IP address or domain name!!*. Potom se podle uživatelem zvolených parametrů měření spouští jednotlivá měření.



Obr. 4.2: Vývojový diagram

Měření pomocí nástroje PING

Spuštění programu Ping se provádí jako u dalších programů PHP funkcí *shell_exe*. Ve vývojovém digramu je znázorněn blokem *Měření pomocí PING*. Protože po provedení příkazu by se nám do proměnné *ping* uložil celý standardní výstup z programu ping, provedeme pomocí dalších příkazů vyseparování pouze průměrné hodnoty zpoždění. Viz obr 4.3. Znak | nám zajistí předání výstupu programu ping na vstup dalšího programu. Příkaz *tail -n 1* vypíše pouze poslední řádek, awk '{print $4}' vytiskne čtvrté pole v řádku, příkaz *cut -d '/'* rozdělí výstup podle zpětného lomítka a parametrem *-f 2* vypíšeme druhý v pořadí. Nakonec vypíšeme průměrnou hodnotu do tabulky.

```
$pocet =$_POST['pocet'];;
$ping = "ping -W ".$timeout_ping." -c ".$pocet."  ".$cmd." |
tail -n 1 | awk '{print $4}' | cut -d '/' -f 2";

if(isset($_POST["1"])){
$output_ping = chop(shell_exec($ping));
if (($output_ping) == ""){

            $output_ping = 'not available';
      }
      else {
            $zpozdeni=$output_ping;
            $prvku=$prvku + 1;}
      $data = $data.$output_ping."\t";
      echo('<tr><td>' ."PING".'</td>'.'<td>'.$output_ping.'</
      td>'.'</tr>');
```

Obr. 4.3: Ukázka kódu: provedení měření pomocí programu Ping

Měření pomocí nástroje ARPING

Spuštění programu Arping a následná úprava výstupu programu je obdobná jako u programu Ping. Ve vývojovém digramu blok *Měření pomocí ARPING*. U tohoto programu je ještě nutné zvolit rozhraní parametrem -I v tomto případě eth0. Dále se program musí spouštět správy uživatele root viz. kap. 4.2.

```
$arpping = "spust arping -I eth0 -w ".$timeout_arp." -c
".$pocet." ".$cmd." | head -n ".    ($pocet + 1)." | tail -n
".$pocet." | awk '{print $6}' | cut -d '=' -f 2 | awk '{total +=
$1; count++ } END { print total/count}'";
```

Obr. 4.4: Ukázka kódu: Provedení měření pomocí programu ARPING

Měření pomocí nástroje HPING

Program Hping se spouští několikrát s rozdílnými parametry podle toho zda je zvolen TCP protokol a příznaky ACK, FIN, SYN nebo UDP protokol. Blok *blok Měření pomocí HPING*. Po provedení měření opět obdobným způsobem získáme průměrnou hodnotu zpoždění a vypíšeme ji do tabulky. Ukázky kódu jsou uvedeny na obr. 4.5, 4.6, 4.7, 4.8

```
$hping1 = "spust hping3  -A  -c ".$pocet."  ".$cmd." -p
".$dportACK." 2>&1 >/dev/null | tail -n 1 | awk '{print $4}' |
cut -d '/' -f 2";
```

Obr. 4.5: Ukázka kódu: Provedení měření pomocí programu HPING - TCP ACK

```
$hping1 = "spust hping3  -F  -c ".$pocet."  ".$cmd." -p
".$dportFYN." 2>&1 >/dev/null | tail -n 1 | awk '{print
$4}' | cut -d '/' -f 2";
```

Obr. 4.6: Ukázka kódu: Provedení měření pomocí programu HPING - TCP FIN

```
$hping1 = "spust hping3  -S  -c ".$pocet."  ".$cmd." -p
".$dportSYN." 2>&1 >/dev/null | tail -n 1 | awk '{print $4}' | cut -
d '/' -f 2";
```

Obr. 4.7: Ukázka kódu: Provedení měření pomocí programu HPING - TCP SYN

```
$hping1 = "spust hping3  -2  -c ".$pocet."  ".$cmd." -p
".$dportUDP." 2>&1 >/dev/null | tail -n 1 | awk '{print $4}' | cut
-d '/' -f 2";
```

Obr. 4.8: Ukázka kódu: Provedení měření pomocí programu HPING - UDP

4.2 Vykonávání příkazů s právy uživatele Root

Pro spuštění aplikace s právy root pod běžným účtem je zapotřebí nejprve nastavit příznakový bit setuid, který zajistí, že spuštěný proces běží s právy vlastníka zmíněného spustitelného souboru, v tomto případě uživatele root. Z bezpečnostního hlediska jsou ignorovány setuid atributy u shellových skriptů. Příznaky se nastaví pomocí "chmod u+s SOUBOR ".

Jelikož po spuštění programu s nastaveným setuid bitem se změní pouze efektivní ID uživatele, tak je třeba, aby program provedl změnu i reálného ID uživatele. To se provede zavoláním funkce "setreuid(real_id, efektivni_id) ". Po provedení těchto kroků již program může spouštět aplikace pod právy vlastníka.

4.3 Úprava programu pro automatizované měření

V rámci bakalářské práce byl požadavek zjistit, zda se bude velikost zpoždění měnit během jednoho pracovního dne. Protože se jedná o relativně velký počet IP adres, na kterých by se mělo zpoždění měřit a ruční opisování změřených hodnot by zabralo hodně času, bylo zapotřebí vytvořit skript, který provede automatické měření v uživatelem zadaných intervalech a změřené hodnoty zapíše do souboru.

Popis programu pro automatické měření

Skript využívá výše zmíněné nástroje. Program postupně načítá IP adresy ze souboru IP.txt uloží do proměnné IP a provede postupně měření pomocí PING, TCP-ACK, TCP-SYN a UDP potom změřené hodnoty uloží do souboru autodata.txt. Měření probíhá opakovaně, dokud funkce feof nevrátí hodnotu false, tím se ukončí cyklus while a celé měření.

Automatické spuštění měření se provádí pomocí softwarového deamona CRON, který umožňuje spouštět různé programy, skripty v určitých časech nebo v intervalech. V našem případě byl interval spuštění měření stanoven na 30min.

```
$soubor = fopen("IP.txt", "r");                  //otevře soubor IP.txt

  $datum = Date("j/m/Y H:i:s", Time());          //zjistí aktuální čas

  $data_auto = $data_auto.$datum."\r";           //uloží aktulání čas
  $pakety = 4;                                   //počet odeslaných paketů

while (!feof ($soubor)) {
        $output_ping = "";
        $IP ="";
        $IP = fgets($soubor, 4096);
        $IP = chop($IP);
        $data_auto = $data_auto.$IP."\t";        //uložení IP adresy
        $ping = "ping -W 2 -c ".$pakety." ".$IP." | tail -n 1 | awk '{print $4}' | cut -d '/' -f 2";
        $data_auto = $data_auto.$output_ping."\t";          //uložení změřeného zpoždění
```

Obr. 4.9: Ukázka kódu: provádění automatického měření

4.4 Program pro měření latence přes webové rozhraní

V rámci projektu zabývající se geolokací, na kterém se podílí více studentů pod vedením doc. Ing. Dana Komosného, Ph.D, byl zhotoven modul pro tento projekt, který provádí měření zpoždění pomocí nástroje PING přes webové rozhraní na zadanou IP adresu a výsledná hodnota je předána formátem dat typu JSON.

Po získání IP adresy se ověří správnost formátu IP adresy. (Pro další rozvoj aplikace je zde i kontrola doménového jména.) Pokud nevyhoví zadaná IP adresa, cyklus vrátí do Json *format_error*. Poté se provede vlastní měření stejným způsobem, jak

```
else {
   $ping = "ping -c 2 -W 1 ".$ipaddress." | tail -n 1 | awk '{print $4}' | cut -d '/' -f 2";
   $output_ping = chop(shell_exec($ping));
         if ($output_ping == "")
                  $output_ping = "not avilable";
   $ret = array();
   $ret['adress'] = "$ipaddress";
   $ret['delay'] = "$output_ping";
   }
   echo json_encode($ret);
```

Obr. 4.10: Ukázka kódu: provádění měření v projektu

je popsáno v kap. 4.1.2 viz obr. 4.10. Do pole ipadress se uloží IP adresa a do pole delay se uloží změřené zpoždění a vytvoří se Json.

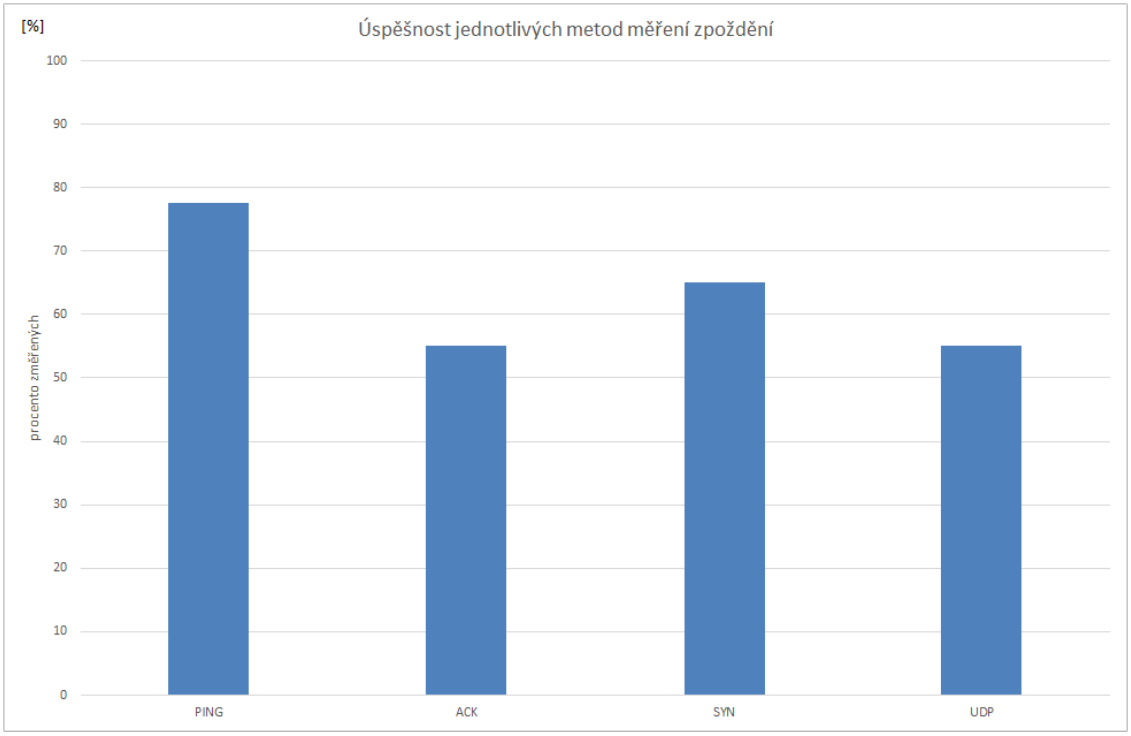
5 ANALÝZA VÝSLEDKŮ

Za pomocí kolegů pracujících pod stejným vedením bylo shromážděno celkem 63 veřejných IP adres. V rámci bakalářské práce bylo změřeno zpoždění na tyto adresy postupně všemi výše zmíněnými metodami tedy pomocí protokolu ICMP, ARP, TCP s příznaky ACK,SYN,FIN a UDP. Byly provedeny celkem dva druhy měření. Při měření se ani jednou nepodařilo změřit zpoždění s nastaveným příznakem FIN a proto není tento příznak ve výsledcích zahrnut.

5.1 Porovnání změřeného zpoždění získaných různými metodami

Účelem prvního měření bylo zjistit, zda se zpoždění změřené různými metodami navzájem liší a o kolik. Dále nás zajímalo jaká je úspěšnost každé metody měření.

Na grafu 5.1 je vidět úspěšnost jednotlivých způsobů měření. Nejúspěšnější metoda měření je PING s 77,5 %, pomocí protokolu ARP se nepovedlo ani jedno měření, což je dané tím, že pracuje pouze v lokální síti a neprojde přes router. Úspěšnost příznaku ACK byla 55% což je podobné jak u příznaku SYN 65%. 55% má také úspěšnost měření pomocí protokolu UDP.

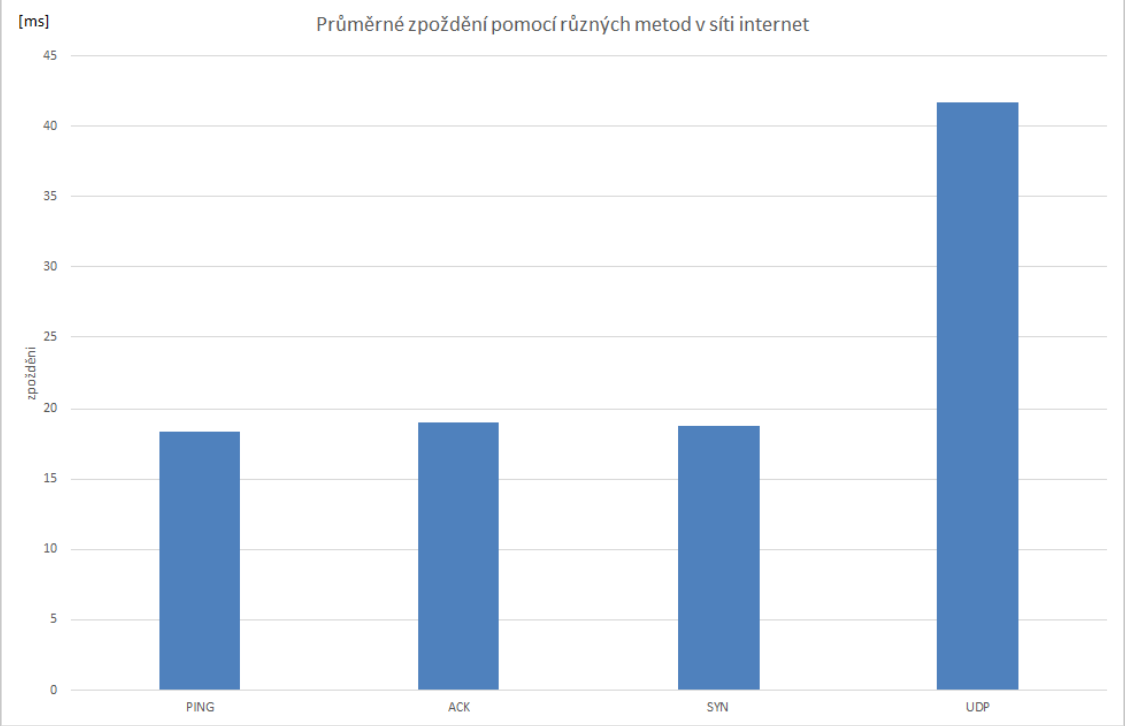


Obr. 5.1: Úspěšnost meření

V další části jsem zjišťoval, jak se bude měnit zpoždění zjištěné jednotlivými způsoby měření. Hodnoty zpoždění jsou uvedeny v tab. 5.1 respektive v tab. 5.2. Nejmenší průměrné zpoždění bylo zjištěno pomocí nástroje Ping 18,338 ms a největší překvapivě pomocí protokolu UDP tj. 41,700 ms.

Metoda	**PING**	**ACK**	**SYN**	**UDP**
Průměr [ms]	18,338	19,024	18,792	41,700
Median [ms]	17,132	17,100	16,60	31,20
Směrodatná odchylka [ms]	10,732	7,100	6.995	39,863

Tab. 5.1: Průměrní zpoždění



Obr. 5.2: Průměrné zpoždění různých metod

Jak je vidět v tab. 5.1 největší směrodatná odchylka byla zjištěna u meření pomocí UDP protokolu a to 39,836 ms, nejměnší pak u protokolu TCP s příznakem SYN a to 6,999 ms.

V tab. 5.2 je uveden rozdíl mezi jednotlivými metodami měření.

V tab. 5.3 je uveden rozdíl zpoždění pomocí nástroje Ping a ARPING, měření bylo prováděno v rámci lokální sítě, kde bylo umístěno celkem 7 stanic. Zpoždění pomocí ARPING je o 0,455 ms větší. To je způsobeno tím, že ARP protokol periodicky posílá broadcast a tím se zvyšuje jeho zpoždění.

Rozdíl	[ms]	Rozdíl	[ms]
ACK-PING	2,772	**SYN-ACK**	0,081
SYN-PING	2,906	**UDP-ACK**	19,706
UDP-PING	19,860	**UDP-SYN**	19,144

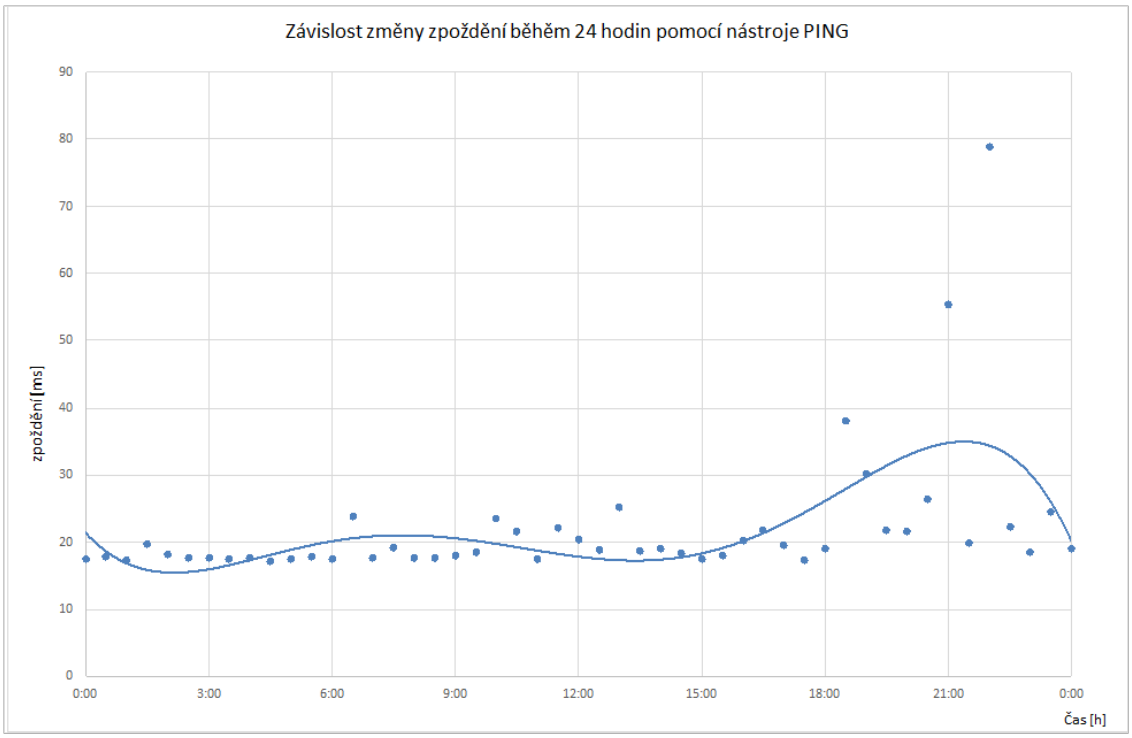
Tab. 5.2: Rozdíl průměrných hodnot jednotlivých metod měření

Nástroj	zpoždění [ms]
PING	1,133
ARPING	1,587

Tab. 5.3: Srovnání PING a ARPING

5.2 Měření zpoždění v průběhu jednoho dne

Účelem dalšího měření bylo zjistit, zda se mění zpoždění v průběhu pracovního dne. Pro tento účel byl vytvořen skript popsán v kap. 4.3. Zpoždění se měřilo na 63 IP adres pomocí PING, TCP s příznakem řízení ACK a SYN a pomocí protokolu UDP. Měření bylo prováděno v době od 0:00 v pátek 10. 4. 2015 do 0:00 v sobotu 11. 4. 2015 každých 30 minut. Změřená data byla následně zpracována do grafů.

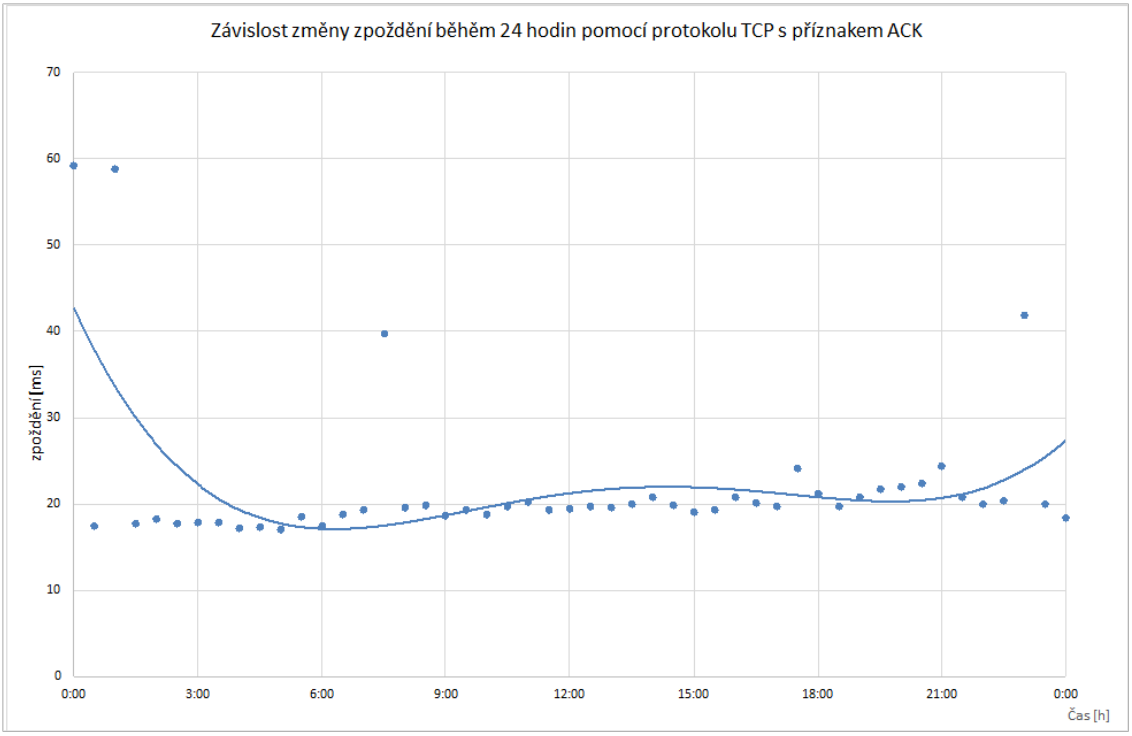


Obr. 5.3: Zpoždění pomocí ping za 24 hodin

V grafu 5.3 je uvedeno průměrné zpoždění pomocí nástroje PING. Je patrné, že

zpoždění se mírně navyšuje směrem k odpoledním a večerním hodinám. Minimální hodnota zpoždění byla 17,163 ms a to ve 4:30 hodin a nejvyšší hodnota byla naměřena ve 22:00 hodin a to 78,79 ms. Některé hodnoty vyznačné v grafu se značně liší od celkového průměru, proto byla vypočtena směrodatná odchylka uvedena v tab. 5.4.

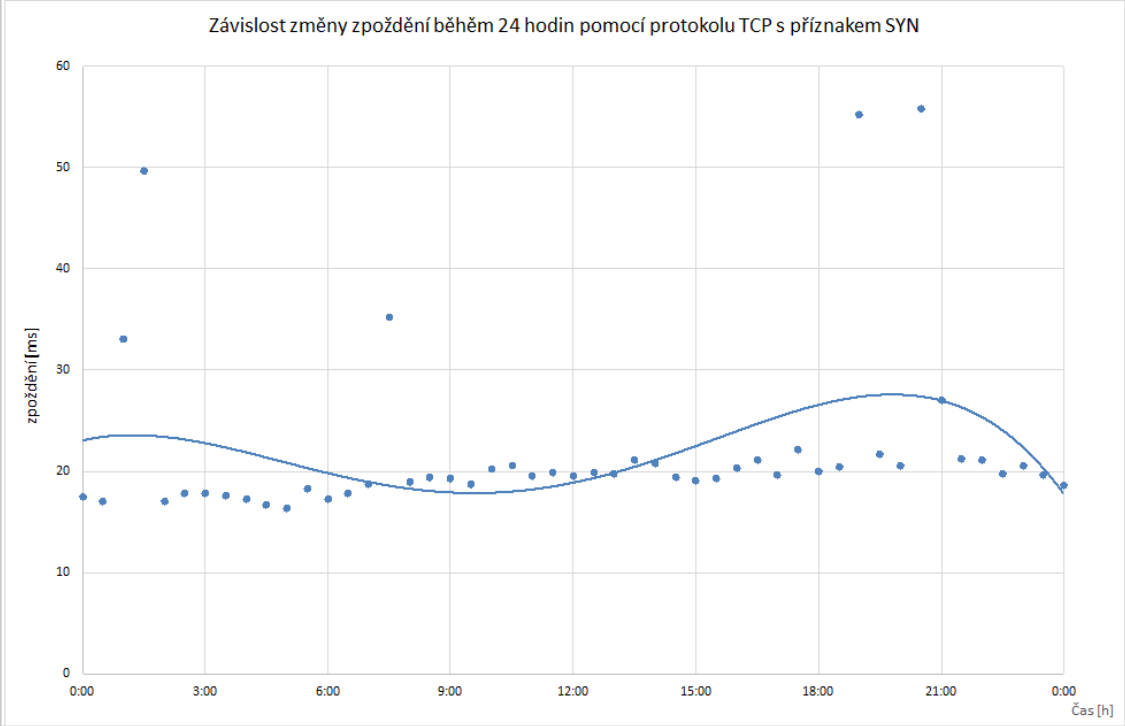
Dále bylo měření prováděno pomocí protokolu TCP s příznakem ACK. V grafu 5.4 jsou uvedeny průměrné hodnoty. Maximální průměrná hodnota byla naměřena v pátek v 0:00 a to 59.229 ms minimální naopak v 5:00 a to 17.117 ms. Od průměru se velmi liší i hodnota v čase 1:00. Tento rozdíl byl způsoben velkým zpožděním vždy na jednu IP adresu konkrétně v čase 0:00 na IP 109.81.188.208 (1032,1ms) a v 1:00 na IP 89.177.128.123 (1027,4ms). Z grafu je patrné, že zpoždění opět narůstá směrem k večerním a odpoledním hodinám. Směrodatná odchylka je uvedena taktéž v tab. 5.4..



Obr. 5.4: Průměrné hodnoty zpoždění pomocí TCP s příznakem ACK

Měření pomocí příznaku SYN je znázorněno v grafu 5.5. Zpoždění se příliš neliší od zpoždění změřeného pomocí příznaku ACK. Má stejný průběh a maximální hodnota byla ve 20:30 55,839 ms a minimální v 5:00 16,294 ms.

Poslední bylo provedeno měření pomocí UDP protokolu znázorněno v grafu 5.6. Jednotlivé hodnoty zpoždění se velice liší od průměrné hodnoty, maximální hodnota byla v 11:30 255,612 ms a minimální v 17:30 23,5 ms. Zpoždění opět narůstá k



Obr. 5.5: Průměrné hodnoty zpoždění pomocí TCP s příznakem SYN

odpolením a večerním hodinám.

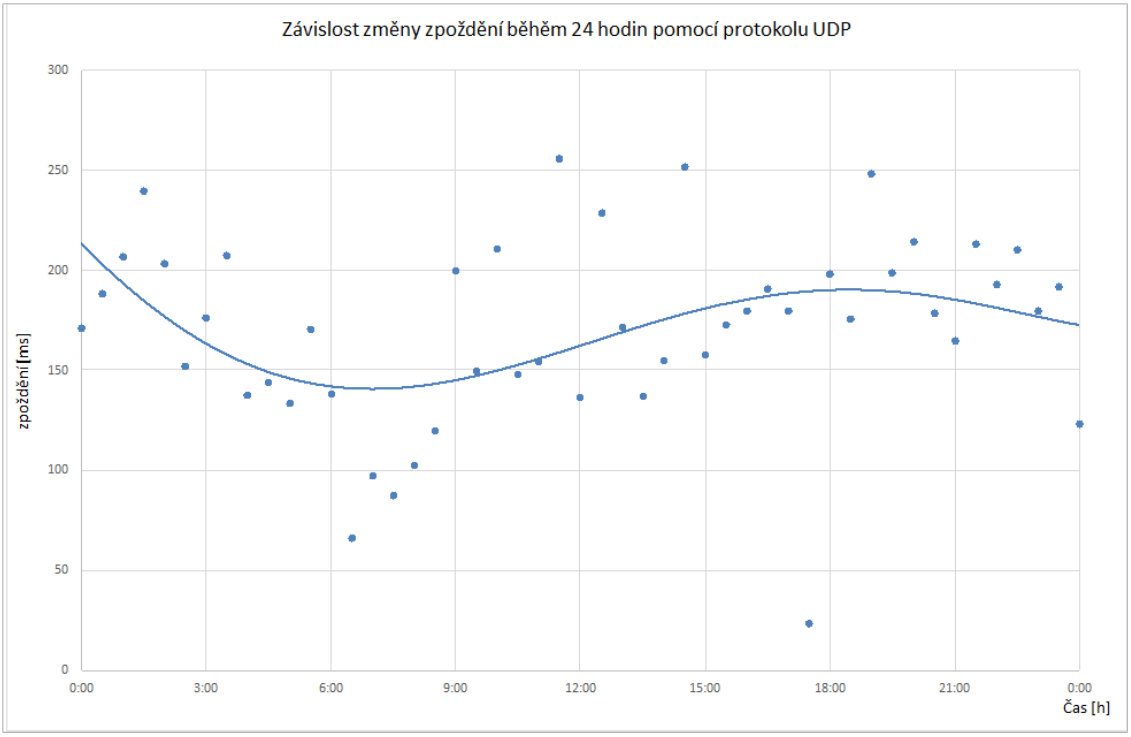
V tab. 5.4 je uvedena směrodatná odchylka pro každý způsob měření během pracovního dne.

Nástroj	**PING**	**ACK**	**SYN**	**UDP**
Směrodatná odchylka [ms]	10,421	8,925	8,834	46,934

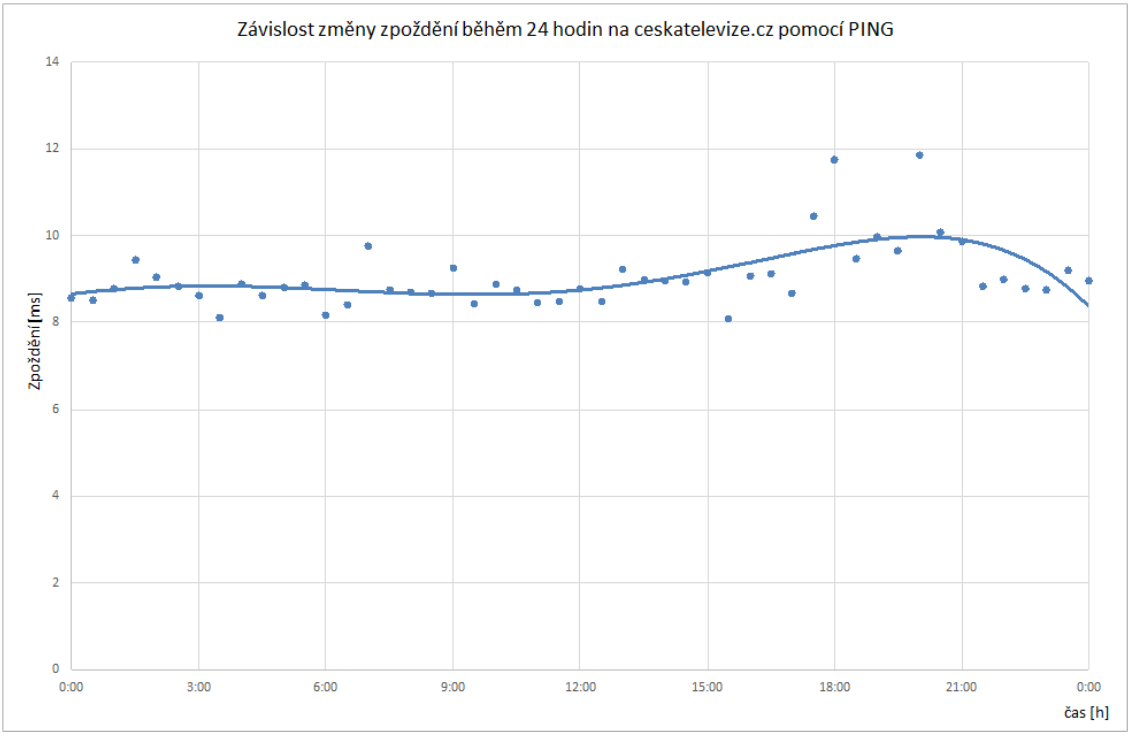
Tab. 5.4: Směřodatná odchylka pro měření během jednoho dne

Nakonec byl zpracován graf zpoždění v průběhu 24 hodin na server ceskatelevize.cz. Patrný nárůst zpoždění je od 17:30 a trvá do 21:30. V této době probíhá hlavní zpravodajská relace a večerní primetime.

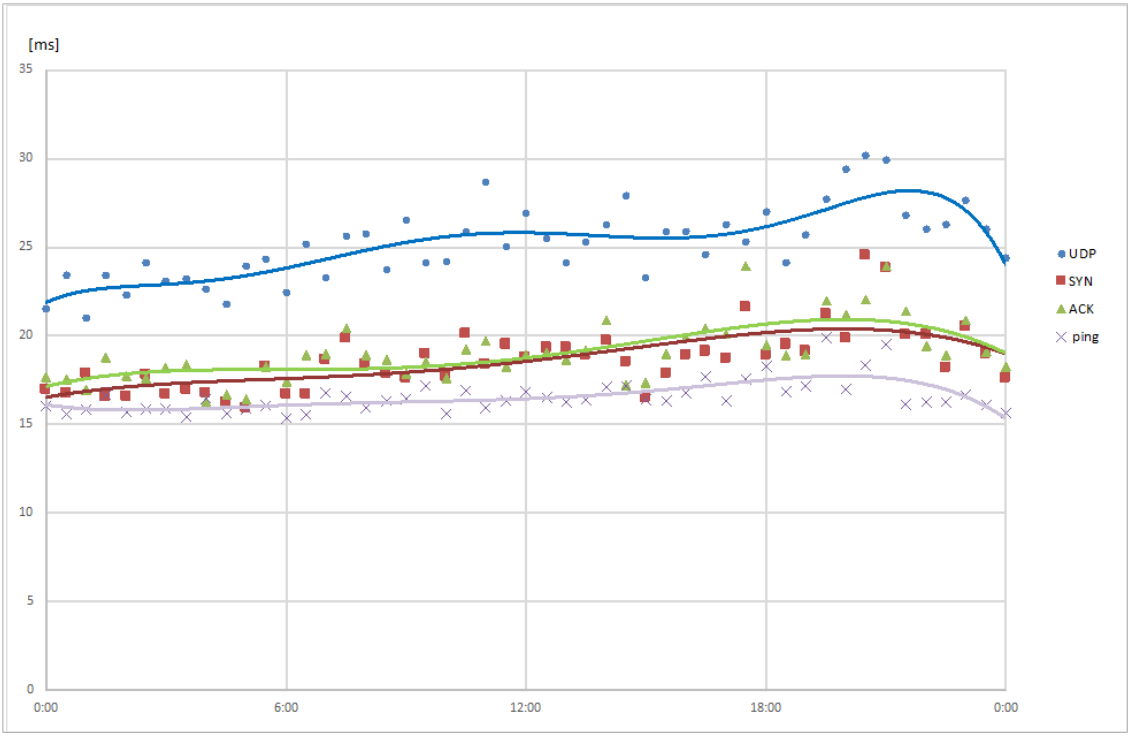
Graf 5.8 znázorňuje všechny metody měření v průběhu 24 hodin.



Obr. 5.6: Průměrné hodnoty zpoždění pomocí UDP



Obr. 5.7: Zpoždění za 24 na ceskatelevize.cz



Obr. 5.8: Zpoždění pomocí všech metod za 24 hodin

6 ZÁVĚR

V práci je prostudována teorie komunikačního zpoždění v sítích, v praktické je pak realizována webová stránka pro měření zpoždění a provedeno vlastní měření. V teoretické části se práce zabývá vznikem zpoždění v koncových zařízeních, na mezilehlých zařízeních a na přenosových linkách. Poté jsem se zaměřil na nástroje sloužící k měření zpoždění, konkretně na PING, ARPING a HPING, tyto nástroje jsou popsány v kapitole 3.

V praktické části jsem se zabýval navrhnutím a zhotovením webové stránky umožnující měření zpoždění. Webová stránka využívá výše zmíněné nástroje a umožňuje měřit zpoždění pomocí ICMP protokolu, TCP protokolu, možné nastavit příznaky řízení ACK, SYN, FIN a pomocí protokolu UDP. Stránka též umožňuje měřit zpoždění na vybrané stanice v různých časových intervalech.

Poslední část práce tvoří samotné měření zpoždění. Bylo provedeno několik měření. První měření popsané v kapitole 5.1 se zabývá rozdíly jednotlivých způsobů měření. Prvním kritériem v tomto měření byla úspěšnost. Nejúspěšnější v tomto směru bylo měření pomocí PING s 77,5 % úspěšně změřeného zpoždění na IP adresy. Dalším kritériem pak bylo samotné porovnání velikosti zpoždění. Nejmenšího zpoždění dosáhl PING a to v průměru 18,338 ms, největšího pak měření pomocí UDP protokolu 41,700 ms. Poslední měření zpoždění bylo prováděno periodicky každých 30 min po dobu 24 hodin a je popsáno v kapitole 5.2. Průběhy jednotlivých měření resp, velikost zpoždění se k večerním a odpoledním hodinám zvyšuje.

LITERATURA

[1] Bednar, JAKUB *Velikost zpoždění aktivních prvků sítě* Brno, 2010 BAKALÁŘSKÁ PRÁCE. VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ.

[2] Tutorial: Hping2 Basics *The Ethical Hacker Network: Free Online Magazine for the Security Profesional* [online]. 3. sprna 2006 [cit. 2015-04-07]. Dostupné z: <https://www.ethicalhacker.net/columns/gates/tutorial-hping2-basics>

[3] Síťové nástroje v Linuxu, 4. část. BOHDAN MILAR, Bohdan Milar. *Linuxexpress* [online]. 25. červenec 2005 [cit. 2015-04-07]. Dostupné z: <http://www.linuxexpres.cz/praxe/sitove-nastroje-v-linuxu-4-cast>

[4] KLAŠKA, Luboš. *Základní kvalitativní parametry sítě (1) - latency (zpoždění)* [online]. 2006 [cit. 2014-12-07]. Dostupné z: <http://www.svetsiti.cz/clanek.asp?cid=Zakladni-kvalitativni-parametry-site-1-latency-zpozdeni-6122006>

[5] BALEJ, Jiří a Dan KOMOSNÝ. Zdroje zpoždění při komunikaci v Internetu. *Zdroje zpoždění při komunikaci v Internetu* [online]. 2010, č. 1 [cit. 2014-12-07]. Dostupné z: <http://www.elektrorevue.cz/cz/clanky/komunikacni-technologie/15/zdroje-zpozdeni-pri-komunikaci-v-internetu/>

[6] BALEJ, Jiří. *Simulace zpoždění při přenosu dat mezi stanicemi v IP sítích: Simulation of data transmission latency between nodes in IP networks* . Brno: Vysoké učení technické, Fakulta elektrotechniky a komunikačních technologií, 2010. 1 elektronický optický disk [CD-ROM / DVD]. Diplomová práce. Vysoké učení technické v Brně (VUT). Vedoucí práce doc. Ing. DAN KOMOSNÝ, Ph.D.

[7] Horák, Michael *Určení polohy stanic v síti Internet pomocí přenosového zpoždění* . Brno: Vysoké učení technické, Fakulta elektrotechniky a komunikačních technologií, 2013. . Diplomová práce. Vysoké učení technické v Brně (VUT). Vedoucí práce doc. Ing. DAN KOMOSNÝ, Ph.D

[8] ZEZULKA, CSC, Prof. Ing. František a Ing. Ondřej HYNČICA. *Průmyslový Ethernet II: Referenční model ISO/OSI.* [online]. [cit. 2014-12-07]. Dostupné z:<http://www.odbornecasopisy.cz/prumyslovy-ethernet-ii:-referencni-model-iso-osi-34209.html>

[9] *Základní kvalitativní parametry sítě (1) - latency (zpoždění).* KLAŠKA, Luboš. Svět sítí [online]. 6. prosince 2006 [cit. 2015-04-07]. Dostupné z: <http://www.svetsiti.cz/clanek.asp?cid=Zakladni-kvalitativni-parametry-site-1-latency-zpozdeni-6122006>

[10] PUŽMANOVÁ, Rita. *TCP/IP v kostce. 2. upr. a rozš. vyd.* České Budějovice: Kopp, 2009, 619 s. ISBN 978-80-7232-388-3.

[11] ČÍKA, P. *Multimediální služby.*. Brno: Vysoké učení technické v Brně, 2012. ISBN: 978-80-214-4443- 0. (cs)

[12] JEŘÁBEK, J. *Komunikační technologie.* Brno: Vysoké učení technické v Brně, 2013. s. 1-172. ISBN: 978-80-214-4713-4. (cs)

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

VoIP	Voice over Internet Protocol
IP	Internet Protocol — internetový protokol
ISO/OSI	referenční síťový model
TCP/IP	Transmission Control Protocol/Internet Protocol - soustava protoklů
ICMP	Internet Control Message Protocol
ARP	Address Resolution Protocol
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
MAC	Media Access Control
LAN	Local Area Network - lokální síť
FTP	File Transfer Protocol
TELNET	Telecommunication Network
PHP	Hypertext Preprocessor
SMTP	Simple Mail Transfer Protocol

SEZNAM PŘÍLOH

A Seznam IP adres **49**

B Obsah přiloženého CD **50**

A SEZNAM IP ADRES

212.47.2.209	77.75.76.3	77.75.77.220	46.255.224.60	194.228.3.66
185.17.119.33	5.198.129.128	213.155.40.147	213.155.38.86	37.221.245.255
213.226.234.137	213.194.217.12	83.208.46.175	83.208.46.178	90.177.237.150
109.81.188.208	88.102.7.222	86.61.137.186	93.190.63.238	80.188.106.243
37.221.245.246	78.98.78.190	212.79.109.151	90.183.224.254	194.79.52.192
212.47.2.209	158.194.230.90	195.113.124.185	195.178.88.109	78.174.89.152
130.193.9.54	83.208.47.160	109.81.185.196	90.178.14.109	37.44.19.46
46.149.119.235	78.98.254.205	89.177.131.77	90.181.107.50	90.181.85.184
193.84.36.129	46.13.152.128	79.127.136.85	82.144.144.107	89.203.220.170
178.188.51.90	78.102.208.117	78.108.107.72	88.103.133.158	92.60.207.159
46.28.105.127	89.177.128.123	212.4.138.51	94.113.161.251	193.165.149.233
88.101.79.76	92.60.207.159	92.60.207.125	88.101.79.76	213.211.37.153
90.177.161.25	90.177.205.165	31.31.228.5		

Tab. A.1: Seznam IP adres pro měření

B OBSAH PŘILOŽENÉHO CD

Na přiloženém CD se nacházejí tyto soubory

- BP_xbedna54.pdf - elektronická verze práce
- Složka ROOT - program pro spouštění aplikací pod právy ROOT
- Složka WEB - programy pro měření latence