Vysoká škola Báňská – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Projekt do předmětu Směrované a přepínané sítě

Nalezení, vytvoření a ověření nástroje na testování QoS a měření propustnosti

Vytvořil: Jiří Štěrba
Login: ste377

1. Úvod

Poslední dobou dochází v počítačových sítích k rozvoji služeb, jejichž funkčnost a dostupnost pro uživatele závisí na charakteristikách počítačové sítě. Například lze uvést služby VoIP, videokonference a on-line aplikace.

Co vše musíme sledovat pro dodržení kvality služeb (QoS – Quality of Services):

- **Volná kapacita sítě** - rozdíl mezi instalovanou kapacitou a zátěží. Je třeba sledovat nejen průměrné hodnoty, ale i jejich dynamické změny v čase.
- **Ztrátovost paketů** – uvádí se v procentech nebo počtem paketů. Jedná se o pakety, které nedorazí od zdroje k cíly.
- **Zpoždění** - doba potřebná k přenosu paketu od odesílatele k příjemci.
- **Rozkmit (jitter)** – rozdíl ve zpoždění jednotlivých paketů posílaných od zdroje k cíly. Tato vlastnost je v mnoha případech důležitější než absolutní hodnota zpoždění.

Následující hodnoty zpoždění , ztrátovosti paketů, rozkmitu a volné kapacity jsou vztaženy ke službě VoIP.

Zpoždění:	do 150 ms , max.50 ms pro použití faxu
Ztrátovost paketů :	< 1%
Rozkmit:	maximálně 20 ms ,max. 5 ms pro použití faxu
Volná kapacita sítě:	dle použitého kodeku je třeba počítat s volnou kapacitou minimálně 30/30 kbps pro jeden hovor při použití kodeku G.729 a až 90/90kbps pro jeden hovor při použití kodeku G.711. Pokud bude probíhat souběžně více hovorů musí být volná kapacita linky rovna násobku potřebné volné kapacity pro jeden hovor a počtu hovorů. Příklad : 3 hovory pomocí kodeku G 711 potřebují celkem 270 kbps , 3 x 90 kbps

2. Způsoby měření linek

Pokud potřebujeme zajistit kvalitu služeb v naší síti, a dochází –li v síti k zahlcení, nebo nemáme dostatečnou bandwidth, měli bychom na základě měření implementovat QoS mechanismus, nebo dokoupit bandwidth.

Mechanismus QoS se implementuje podle toho jaký typ provozu potřebujeme preferovat (VoIP, online aplikace).

Abychom mohli správně implementovat QoS mechanismy je dobré o lince vědět jaké má vlastnosti :

1. **Propustnost (Bandwidth)**

2. **Zpoždění (Latency)**

3. **Ztrátovost paketů (Packet loss)**

4. **Rozkmit (Jitter)**

Způsobů jak změřit tyto vlastnosti je hned několik. Záleží jen na tom jak přesné výsledky potřebujeme.

2.1 Webové nástroje na měření propustnosti, zpoždění, ztrátovosti paketů a rozkmitu

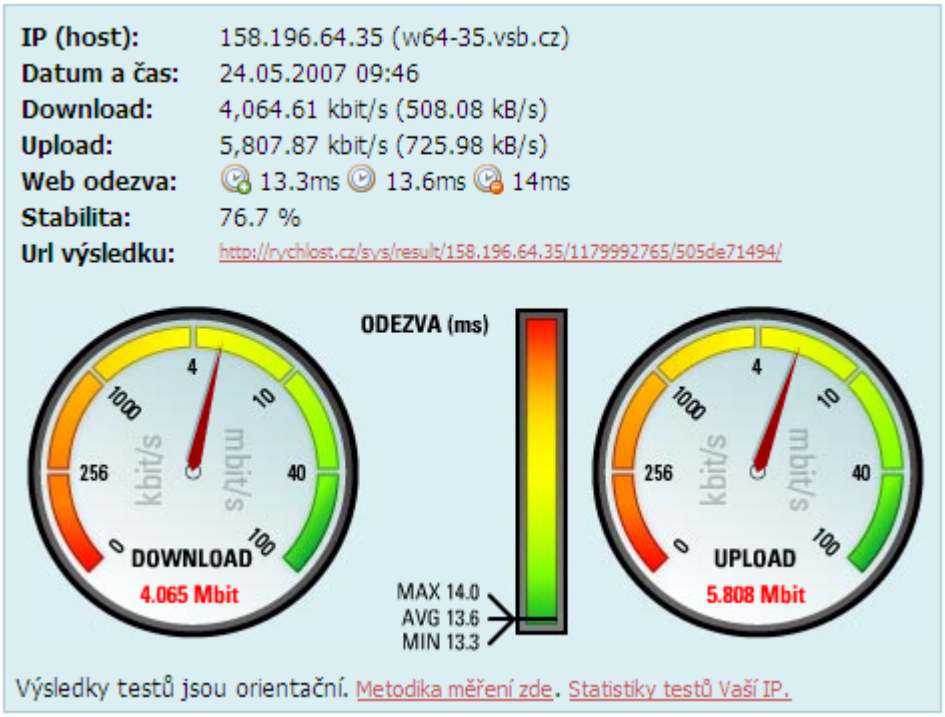
Pro měření je možné použít webových měřidel, která jsou například na stránkách www.rychlost.net .

Tento nástroj dokáže ověřit více vlastností linky, nejen její rychlost směrem k uživateli ale také od uživatele a odhalit tak, zda se jedná o symetrickou či asymetrickou linku. Dále je patrná velikost odezvy. V tomto případě je odezva získána pomocí nástroje ping a jak uvádí i autor celého testovacího nástroje na stránkách www.rychlost.net má charakter pouze orientační.

Princip měření na www.rychlost.net je následující:

1. po spuštění testu začne prohlížeč stahovat testovací soubor o velikosti 100kB. V případě, že je tento soubor stažen za více jak 5 sekund, je test úspěšně dokončen a uveden ve statistice. V opačném případě je vypočítána nová velikost testovacího souboru, který bude, dle prvního testu, stažen za déle jak 5 sekund. Maximální velikost testovacího souboru je 5000 kB, v tomto případě je test platný i v případě kratšího testu než 5 sekund.
2. Test uploadu je prováděn obdobně. K testu jsou použita data získaná při testu downloadu s horním limitem 1500 kB.
3. Test odezvy slouží k přibližnému určení odezvy (tzv. ping) klienta proti serveru. Tento test je však vzhledem k použité technologii velmi orientační.

Výhodou nástrojů tohoto typu je, že nejsou závislé na operačním systému ani na typu prohlížeče, který je používán. Ale jejich velkou nevýhodou je nepřesné měření těchto vlastností způsobené i zatížením linky na které jsou fyzicky umístěny stanice.



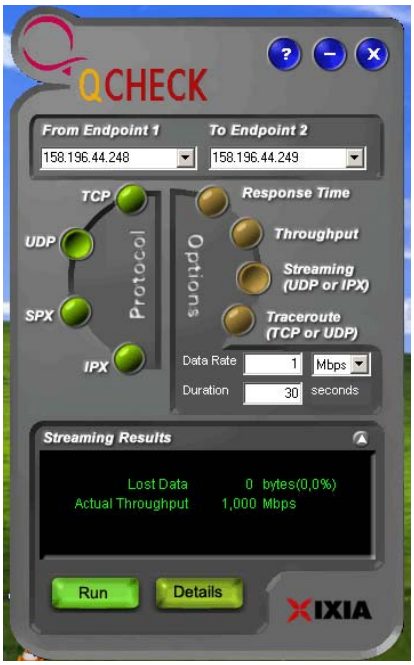
2.1 Nástroje na měření propustnosti, zpoždění a ztrátovosti paketů a rozkmitu v operačních systémech Windows

Pro měření parametrů linky (rozkmit, propustnost, zpoždění …) existuje velká řada nástrojů jak placených tak neplacených. Nástroje, které jsou stažitelné zdarma zastupuje Qcheck od společnosti IXIA, která je výrobcem i hardwarových nástrojů na ověřování rozkmitu, propustnosti.

Nástroj Qcheck se skládá ze dvou částí.

První částí je server – koncový bod (performance endpoint), který zajišťuje vlastní provádění testů. Testy se provádí ze serveru na server (mají P2P architekturu) a to na protokolu TCP, UDP což jsou protokoly 4 vrstvy IP a pro protokoly 3 vrstvy IPX a SPX. Server je implementován jak pro OS Windows tak pro OS Linux .

Druhou částí je klient v grafickém provedení. Popis klienta a obrázek je uveden níže Nevýhodou klienta je ta, že je implementován pouze pro OS Windows a neumožňuje zadat upřesňující parametry testů (např. číslo portu na kterém je test realizován).



Popis:

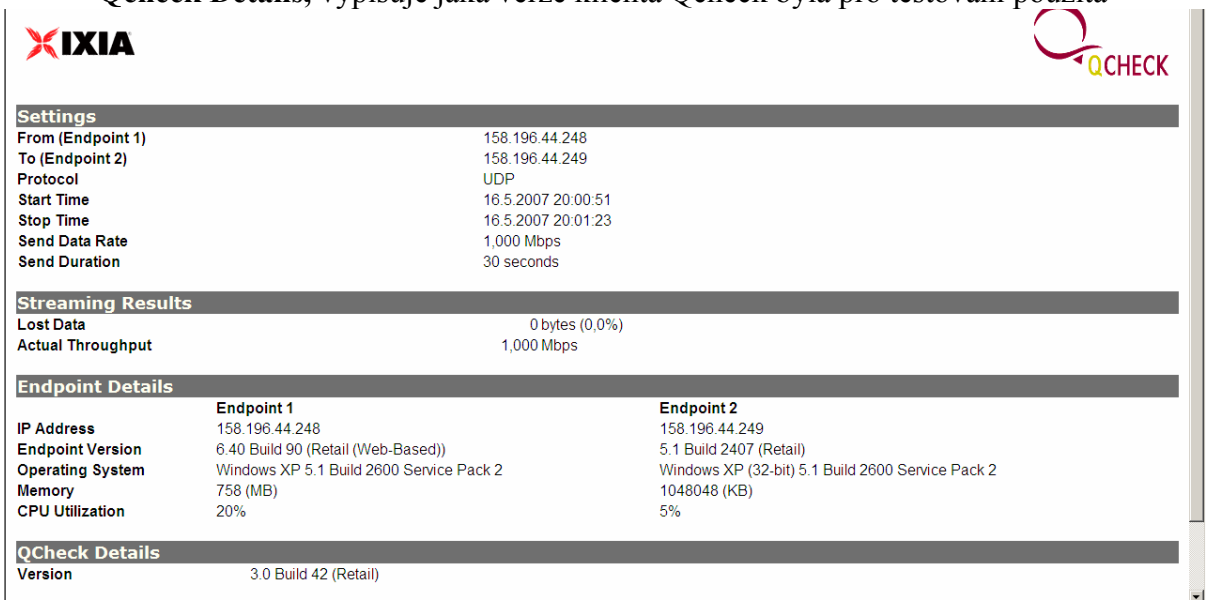
Ovládání klienta je prováděno plně intuitivně pomocí myši.

1. V prvním poli From Endpoint 1 zadáte adresu, nebo DNS jméno serveru z kterého chcete provádět měření (tento nemusí být zpuštěn na počítači v kterém je nainstalován klient)
2. V poli To Endpoint 2 zadáte adresu druhého serveru, oproti kterému chcete provést test, stejným způsobem jako v prvním poli.
3. Pomocí myši vyberte typ protokolu (UDP, TCP, IPX, SPX) - na obrázku vybrán UDP
4. Pomocí myši vyberte o jaký typ trestu máte zájem (Response Time – odezva, Throughput – propustnost, Streaming – propustnost, Traceroute - zobrazí se všechny směrovače v cestě k cíly. Jde vlastně o vytyčení trasy paketu.) – na obrázku vybrán Streaming
5. poté doplníte další parametry testu v tomto případě jak velkou propustnost (Data Rate) stream využije a jak dlouho bude test trvat(Duration)
6. Stisknete zelené tlačítko Run
7. v okně Streaming Resuslts se objeví výsledek testu. V tomto případě je propustnost (Actual Throughput) dodržena, v jiném případě může být menší. Také nedošlo ke ztrátě dat (Lost Data)

Pokud takto zobrazené výsledky nejsou dostačující stačí kliknou myší na tlačítko **Details**, poté se otevře v prohlížeči webová stránka s detailním výpisem testu vč. systému na kterém běží jak první tak druhý server.
Na výpisu níže, je vidět detailní výpis výsledku testu.Ve výpisu jsou čtyři základní sekce.
Settings, kde jsou vypsány vstupní parametry testu (Endpointy, protokol, čas spuštění, čas ukončení , Data Rate, Duration – doba trvání)
Streaming Results, jsou zde zobrazeny výsledky testu (Lost Data – ztracená data během testu, Actual Throughput – propustnost, která byla při testu dosažena)

Endpoint Details , zobrazuje informace o koncových bodech mezi kterými byl test prováděn. Zobrazuje IP adresu koncových bodů, použitá verze serveru koncového bodu, instalovaný OS, velikost operační paměti a na kolik procent byl při testu využit CPU. Informace o jaký typ CPU nezobrazuje.

Qcheck Details, vypisuje jaká verze klienta Qcheck byla pro testování použita



IXIA

QCHECK

Settings	
From (Endpoint 1)	158.196.44.248
To (Endpoint 2)	158.196.44.249
Protocol	UDP
Start Time	16.5.2007 20:00:51
Stop Time	16.5.2007 20:01:23
Send Data Rate	1,000 Mbps
Send Duration	30 seconds

Streaming Results	
Lost Data	0 bytes (0,0%)
Actual Throughput	1,000 Mbps

Endpoint Details	Endpoint 1	Endpoint 2
IP Address	158.196.44.248	158.196.44.249
Endpoint Version	6.40 Build 90 (Retail (Web-Based))	5.1 Build 2407 (Retail)
Operating System	Windows XP 5.1 Build 2600 Service Pack 2	Windows XP (32-bit) 5.1 Build 2600 Service Pack 2
Memory	758 (MB)	1048048 (KB)
CPU Utilization	20%	5%

QCheck Details	
Version	3.0 Build 42 (Retail)

2.2 Nástroje na měření propustnosti, zpoždění a ztrátovosti paketů a rozkmitu v operačních systémech Linux/Unix

Nástrojů na měření propustnosti, zpoždění a dalších parametru linky, které jsou pod OS Linux dostupné zdarma, je velké množství.

Jedním z nejkomplexněji pojatých nástrojů je NPToolkit CD od asociace INTERNET2. Toto Bootable CD je založeno na Bootable Knoppix Linux (tyto vycházejí z Debian Linuxu) a jeho image stejně jako jednotlivé testovací nástroje, na CD jich je obsaženo 5, jsou volně ke stažení na adrese e2epi.internet2.edu/network-performance-toolkit.html.

Dalším zástupcem je nástroj Netperf (Network performace), tento pochází z dílny Hewlett-Packard Company a je volně ke stažení na stránkách www.netperf.org, kde je ke stažení i manuál.

2.2.1 NPToolkit CD

NPToolkit CD je CD s Bootable Knoppix Linux, na které jsou implementovány testovací nástroje. Veškerá konfigurace těchto nástrojů probíhá po nabootování pomocí automaticky spuštěného skriptu .

Tento skript nabízí osm možností v menu:

1. **Setup USB Drive** - provede konfiguraci USB disku (definuje cestu k disku a data na disku nechá beze změny) a ten poté slouží k automatickému uložení konfigurace nástrojů. Tyto konfigurace pak slouží při dalším bootování a jsou automaticky zaváděny.
2. **bwctl** - slouží ke konfiguraci nástroje Bandwith Test Controller, což je nástroj na testování propustnosti linky
3. **ndt –** slouží ke konfiguraci Network Diagnostic Tool**,** konfigurace tohoto nástroje probíhá pomocí po sobě následujících otázek, které je pro správný běh nutné vyplnit.

Tento nástroj v sobě zahrnuje jak možnost provádět testy pomocí CLI tak pomocí webového rozhraní.

4. **npad –** provede konfiguraci nástroje Network Path and Aplication Diagnostic
5. **ntp –** provede uložení konfigurace NTP z ramdisku na Flash disk
6. **owamp –** slouží ke konfigurace nástroje One Way Ping, ten slouží k zjištění jednostranného zpoždění
7. **Static IP** – slouží k nastavení statické ip adresy, v případě že v sítí nefunguje DHCP
0. **Exit** - ukončí konfigurační skript a spustí login skript (uživatelské jméno Knoppix, heslo není nastaveno)

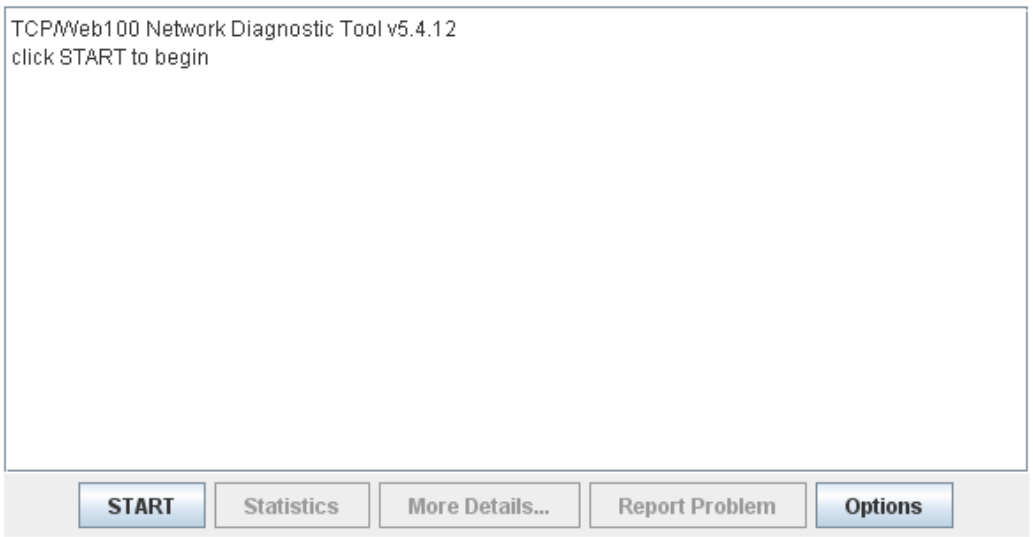
Většina konfigurací spočívá pouze v automatickém zkopírování již přednastavených konfigurací na Flash disk a do ramdisku, kde běží OS. Některé konfigurace potřebují doplňkové informace, jako je Vaše doménové jméno, nebo Váš email , na které se Vás postupně ptají pomocí automatického průvodce nastavením, který se spustí po zvolení jedné z voleb. Tyto parametry ale nejsou povinné.

Network Diagnostic Tool

Network Diagnostic Tool (NDT) je testovací nástroj založen na platformě klient-server a poskytuje klientům PC možnost zjistit propustnost linky a diagnostikovat potíže v síti. Přesněji poskytuje test propustnosti sítě pomocí protokolu TCP mezi počítačem a NDT serverem. Postup testování je následující : zaprvé začnou se posílat data od uživatele k serveru a to po dobu 10 s, poté je test opakován v opačném směru tj, od serveru k uživateli, také po dobu 10 s. Jelikož jádro linuxu na CD je rozšířeno o balíčky Web 100, tak zachycuje detailní statistiky o TCP datových tocích. Tyto data jsou poté analyzována a vyhodnocena aby bylo možné zobrazit jakých výsledků propustnosti bylo dosaženo.

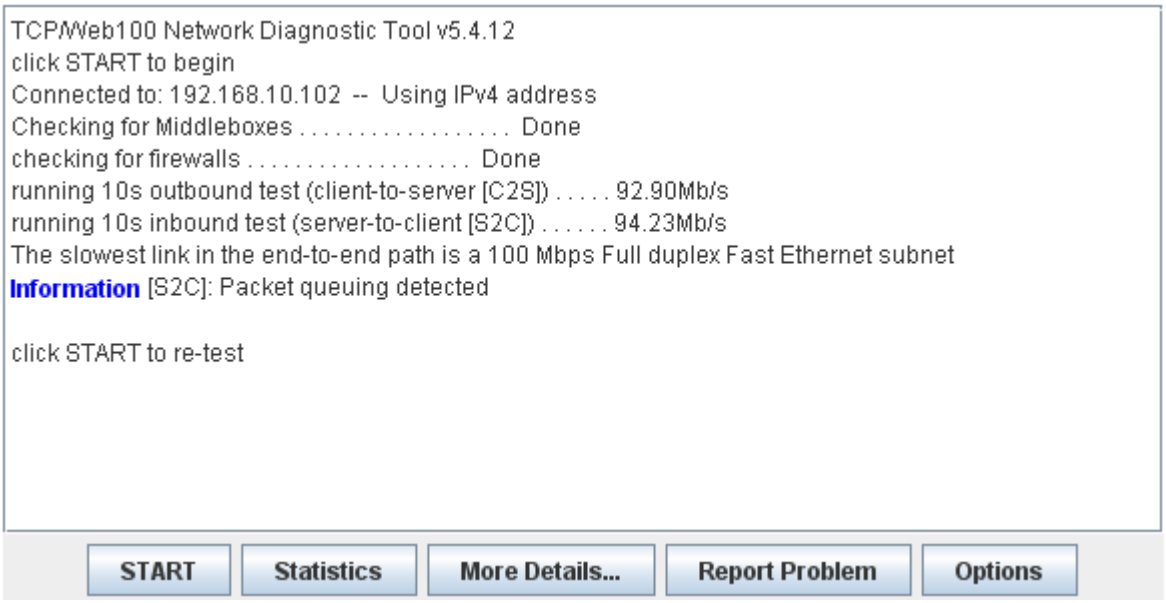
Obrázek ukazuje okno appletu na webových stránkách serveru. Tyto jsou standartě dostupné na portu 7123.

Příklad URL: http://192.168.10.102:7123



V appletu jsou po spuštění dvě možnosti – START – spustí test a Options – je možné nastavit má li test preferovat IPv6 adresu pokud jsou v síti používány jak IPv4 tak IPv6 adresy.

Po spuštění testu jsou na obrazovku postupně vypisovány jednotlivé kroky a výsledky ve zkráceném tvaru .



Po ukončení testu se aktivují tlačítka Statistics, More Details.. a Report Problem

Report problem – vytvoří soubor, který obsahuje informace o testu, který mužete pomocí emailu zaslat komukoliv si jen budete přát.

More Details… - zobrazí okno se všemi zaznamenávanými hodnotami WEB 100 jádra

WEB100 Kernel Variables:
Client: localhost/127.0.0.1
CurMSS: 1260
X_Rcvbuf: 33554432
X_Sndbuf: 33554432
AckPktsIn: 52102
AckPktsOut: 0
BytesRetrans: 0
CongAvoid: 0
CongestionOverCount: 0
CongestionSignals: 0
CountRTT: 52041
CurCwnd: 66780
CurRTO: 208
CurRwinRcvd: 65535
CurRwinSent: 5840
PktsIn: 52102
PktsOut: 97284
PktsRetrans: 0

Jedná se o ukázku jen několika pár hodnot. Je zde například informace o velikosti bufferu, kolik přišlo potvrzení o doručení paketu kolik bylo paketů přijato (PktsIn), odesláno (PktsOut) a přeposláno (PktsRetrans), např. z důvodu chyby.

Statistic - vypisuje kompletní Statistiku testu.
Detailní výpis statistiky :

WEB100 Enabled Statistics:
Checking for Middleboxes . . . . . Done
checking for firewalls . . . . . Done
running 10s outbound test (client-to-server [C2S]) 92.90Mb/s
running 10s inbound test (server-to-client [S2C]) 94.23Mb/s

------ Client System Details ------
OS data: Name = Windows XP, Architecture = x86, Version = 5.1
Java data: Vendor = Sun Microsystems Inc., Version = 1.6.0_01

------ Web100 Detailed Analysis ------
100 Mbps FastEthernet link found.
Link set to Full Duplex mode
No network congestion discovered.
Good network cable(s) found
Normal duplex operation found.

Web100 reports the Round trip time = 5.62 msec; the Packet size = 1260 Bytes; and
No packet loss - but packets arrived out-of-order 0.12% of the time
S2C throughput test: Packet queuing detected: 11.64%
This connection is receiver limited 98.28% of the time.
This connection is sender limited 1.61% of the time.

Web100 reports TCP negotiated the optional Performance Settings to:
RFC 2018 Selective Acknowledgment: ON
RFC 896 Nagle Algorithm: ON
RFC 3168 Explicit Congestion Notification: OFF
RFC 1323 Time Stamping: OFF
RFC 1323 Window Scaling: ON

Server '192.168.10.102' is not behind a firewall. [Connection to the ephemeral port was successful]
Client is not behind a firewall. [Connection to the ephemeral port was successful]
Information: Network Middlebox is modifying MSS variable
Server IP addresses are preserved End-to-End
Client IP addresses are preserved End-to-End

Statistika popisuje jak výsledky testu propustnosti , tak i informace o klientovi který test spustil a detailní analýzu , která dává informace o tom zda není vadný kabel, jaký duplex mode je v dané síti použit, zdali se klient nachází za firewallem či nikoliv.

NDT CLI

NDT CLI, tento nástroj umožňuje provádět i diagnostiku z příkazové řádky pomocí svého Client Line Interface, tento se spouští příkazem:

web100ctl –n (jméno serveru) – parametry.

Jako parametry je možné zadat :

-d vypisuje debut informace, například informace o použitých portech
-l tento parametr slouží pro výpis více detailů daného testu , je možné jej zařadit až 2 krát, v tomoto případě je výpis úplný
-4 použije výhradně IP adresu verze 4
-6 použije výhradně IP adresu verze 6

Příklad:

web100clt –n 192.168.10.102 –l –l

Testing network path for configuration and performance problems -- Using IPv4 address
Checking for Middleboxes . . . . . Done
checking for firewalls . . . . . Done
running 10s outbound test (client to server) . . . . . 93.95 Mb/s
running 10s inbound test (server to client) . . . . . 94.14 Mb/s
The slowest link in the end-to-end path is a 100 Mbps Full duplex Fast Ethernet subnet
Information: Other network traffic is congesting the link
Information [S2C]: Packet queuing detected: 11.94% (local buffers)
Server '192.168.10.102' is not behind a firewall. [Connection to the ephemeral port was successful]
Client is not behind a firewall. [Connection to the ephemeral port was successful]

------ Web100 Detailed Analysis ------

Web100 reports the Round trip time = 70.82 msec;the Packet size = 1448 Bytes; and
No packet loss was observed.
This connection is sender limited 1.64% of the time.
This connection is network limited 97.38% of the time.

Web100 reports TCP negotiated the optional Performance Settings to:
RFC 2018 Selective Acknowledgment: ON
RFC 896 Nagle Algorithm: ON
RFC 3168 Explicit Congestion Notification: OFF
RFC 1323 Time Stamping: ON
RFC 1323 Window Scaling: ON; Scaling Factors - Server=10, Client=10
The theoretical network limit is 45.52 Mbps
The NDT server has a 32768 KByte buffer which limits the throughput to 3615.05 Mbps
Your PC/Workstation has a 2684 KByte buffer which limits the throughput to 296.11 Mbps
The network based flow control limits the throughput to 157.10 Mbps

Client Data reports link is ' 5', Client Acks report link is ' 5'
Server Data reports link is ' 5', Server Acks report link is ' 5'
Packet size is preserved End-to-End
Server IP addresses are preserved End-to-End

Client IP addresses are preserved End-to-End
CurMSS: 1448
X_Rcvbuf: 33554432
X_Sndbuf: 33554432
AckPktsIn: 42723
AckPktsOut: 0
BytesRetrans: 0
CongAvoid: 40702

Výpis proměnných je daleko detailnější, zde je jen jeho zkrácená verze. Kompletní výpisy jsou připojeny jako příloha.

Jak je patrné z tohoto výpisu, tak aplikace v příkazové řádce poskytuje stejné informace jako applet. U appletu si detailní výpisy je možné zvolit kliknutím na příslušné tlačítko, v případě klienta v příkazové řádce je to zřetězením parametru –l.

One-way Ping (OWPING)

One Way Ping je implementován na protokolu One-way Active Measurement Protocol (OWAMP), který je popsán v RFC 4656. Jedná se o klient- server nástroj, který slouží k určení jednocestného zpoždění a jeho rozkmitu.

Pokud budeme spouštět test jednocestného pingu tak jej musíme spouštět oproti server, který běží na druhé straně. Spuštění vlastního testu se provádí z příkazové řádky pomocí příkazu :

owping [atributy] clientadr serveradr - clientadr není vyžadována automaticky se vezme adresa rozhraní, na kterém test provádíme

Příklad :
owping –c 199 localhost 192.168.10.1

výsledkem tohoto testu je následující výpis :

```
# owping -c 199 localhost 192.168.10.1
owping: FILE=time.c, LINE=106, NTP: Status UNSYNC (clock offset issues likely)
Approximately 22.8 seconds until results available

--- owping statistics from [192.168.10.1]:32776 to [localhost]:32777 ---
SID: 7f000001ca013e2fda09bb6a2f40536b
199 sent, 0 lost (0.000%), 0 duplicates
one-way delay min/median/max = 0.0229/0.1/0.814 ms, (unsync)
one-way jitter = 0.1 ms (P95-P50)
TTL not reported
no reordering

--- owping statistics from [localhost]:32779 to [192.168.10.1]:32778 ---
SID: c0a80a01ca013e2fdb225b74a7dd01ae
199 sent, 0 lost (0.000%), 0 duplicates
one-way delay min/median/max = 0.0219/0.1/12 ms, (unsync)
one-way jitter = 0.1 ms (P95-P50)
TTL not reported
no reordering
```

Test otestuje zpoždění v jednom směru (pokud je na stroji, ze kterého se test provádí, nainstalován také server OWAMP tak se provede automaticky i test ve druhém směru jak je uvedeno zde). Zobrazí odkud kam byl test realizován, zajímavá hodnota je i kolik bylo posláno paketů a kolik jich bylo duplikováno nebo ztraceno. Také zobrazí min, max, a mediánovou hodnotu odezvy a vypočítá i rozkmit jak je patrné z výstupu . Hodnota parametru –c dosahuje maximální hodnoty 199 a určuje počet posílaných pingů během test, pro hodnotu 200 již owping nefunguje.

Pokud je u příkazu použit atribut :

-H PHB je možné zadat značení paketů TOS bity dle RFC 2836

-D DSCP je možné zadat značení paketů TOS bity dle RFC 2474

Na CD NPToolkit jsou i další zajímavé testovací aplikace, jako Thrulay network capacity tester. Tato aplikace provádí test maximální propustnosti v reálném čase, s možností nastavení periody výpisu výsledků(např. 1s). Tuto aplikaci je možné použít pro online sledování zatížení linky a dostupné propustnosti na ní v časovém úseku. Samozřejmě tato aplikace umožňuje přidávat do paketů bity pro rozlišení služby v síti, a tím zjišťovat jak se daný typ provozu v síti chová (je-li používána implementace QOS, tak je možné ověřit zda funguje dle předpokladů.

Veškeré testovací nástroje obsažené na CD mají implementovánu i podporu pro IPv6. Tato podpora je plně automatická, tzn. Pokud má stanice na které aplikace běží přidělenu jak IPv6 tak IPv4 adresu tak testy použijí automaticky IPv6 adresu. Samozřejmostí je, že pomocí parametru se dá tato podpora vypnout a striktně používat jen IPv4.

2.2.1 Netperf

Netperf je testovací nástroj založený na platformě klient - server, který muže být používám pro zjišťování mnohých vlastností sítí . Primárně je ale zaměřen na testování velký přenosů dat (propustnost) přes sít a na testy request/response (žádost/odezva). Při těchto testech dokáže využívat protokolů protokolů TCP a UDP a dalších.

Tento nástroj vytvořil a je dále spravován IND Network Performace Team společnosti Hewlett Packard. Jeho výhodou je, že umí provádět testy jak pomocí IPv4 tak i pro IPv6. Typ použité adresy se volí jako atribut při zadání testu.

TCP_ STREAM test je jedním ze základních testů Netperfu. Jde o test propustnosti linky při použití protokolu TCP. Jeho použití je velice jednoduché , jak uvádí následující příklad.

```
netperf -H 192.168.10.1

     TCP STREAM TEST from 0.0.0.0 (0.0.0.0) port 0 AF_INET to
192.168.10.1 port 0 AF_INET
     Recv   Send    Send
     Socket Socket  Message  Elapsed
     Size   Size    Size     Time     Throughput
     bytes  bytes   bytes    secs.    10^6bits/sec

      32768  16384  16384    10.00      80.42
```

Z výstupu testu je patrné, z jaké adresy (adresa 0.0.00 reprezentuje localhost) a na jakou byl test proveden. Dále se dozvídáme informaci velikosti jak vysíláných zpráv, době trvání testu i velikosti propustnosti (zde 80.42 MBit, je zajímavé , že pro stejnou linku udává NTD propustnost 92.4 Mbit. Tento test byl na lince provádět opakovaně a vždy se stejným výsledkem).

U toho testu byl použit jediný parametr a to je –H , který udává adresu serveru.

UDP_STREAM test je obdobný test, jako předchozí, ale měří propustnost sítě s využitím protokolu UDP

netperf -t UDP_STREAM -H 192.168.10.1 -- -m 32768

```
     UDP UNIDIRECTIONAL SEND TEST from 0.0.0.0 (0.0.0.0) port 0 AF_INET to
192.168.10.1 (192.168.10.1) port 0 AF_INET
     Socket  Message  Elapsed      Messages
     Size    Size     Time         Okay Errors   Throughput
     bytes   bytes    secs            #      #   10^6bits/sec

     124928   32768   10.00      105672      0    2770.20
     135168           10.00      104844           2748.50
```

Ve výpisu výsledku vidíme jak velké zprávy byly posílány i propustnost (2,7 Gbit, což je chybu měření jelikož v PC byla instalována pouze 1Gbit síťová). Při spuštění tohoto testu byly použity následující parametry:

-t – určuje o jaký test se jedná , pokud se neudá tak je přednastavena na TCP_STREAM
-H – adresa serveru
-- -m - udává jak velké má být odchozí zpráva (zde 32 Kbyte)

TCP_RR test, slouží k ověření toho, jak rychle dojde k navázání spojení tzn. měří čas potřebný k navázání spojení mezi serverem a klientem. Jde o velice důležitou vlastnost sítě, po které jsou provozovány on-line aplikace.

```
netperf -t TCP_RR -H 192.168.10.1
 TCP REQUEST/RESPONSE TEST from 0.0.0.0 (0.0.0.0) port 0 AF_INET to
192.168.10.1 (192.168.10.1) port 0 AF_INET
     Local /Remote
     Socket Size   Request  Resp.   Elapsed  Trans.
     Send   Recv   Size     Size    Time     Rate
     bytes  Bytes  bytes    bytes   secs.    per sec

     16384  87380  1        1       10.00    29150.15
     16384  87380
```

Ve výpisu výsledku testu je patrná velikost posílaných zpráv (žádostí a potvrzení spojení) zde je to 1 byte. Poté velikost vstupního a výstupního bufferu a počet vytvořených spojení za 1s (Trans. Rate per sec)

3. Závěr

Problematika měření QoS není jednoduchou záležitostí a velice závisí na tom , jaký typ provozu bude chtít měřit a následně preferovat.

Nástrojů na měření QoS je nepřeberné množství a se všemi se není možné seznámit znát jejich syntaxi. Nejvíce informací o nástrojích pro měření QoS je možné nalézt na internetových fórech, nebo na stránkách producentů těchto nástrojů. Nástroje prezentované v této práci jsou pouhým průřezem všech typů nástrojů, které se dají na Internetu najít a jsou volně ke stažení. Nejsou a ani zde nemohou být popsány všechny možné varianty jak je možné tyto nástroje použít.Veškeré ostatní možnosti použití jsou k nalezení buď na webových stránkách producentů těchto nástrojů viz. „Použitá literatura“, nebo v manuálových stránkách.

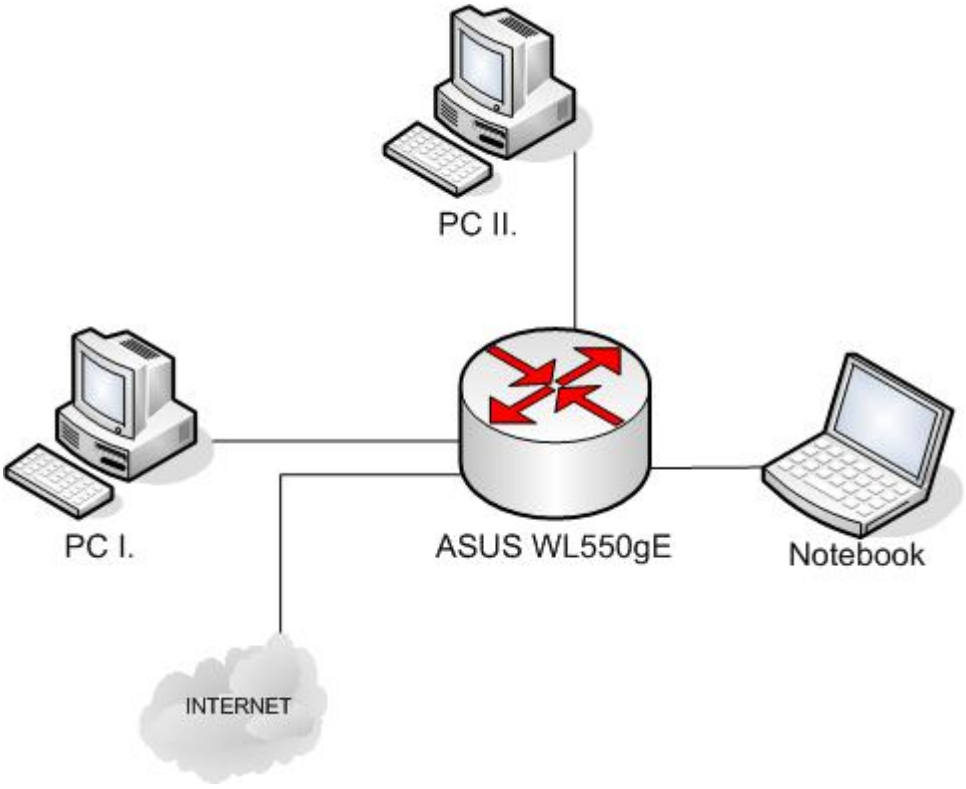
Veškeré testy byly prováděny na síti Ethernet 100 Mbit, s jedním routerem .

Počítače použité pro testování byly byly :

I. Notebook Fujitsu Siemens AMILO PRO V 3505,
OS WINDOWS XP SP2 + Linux ,
CPU: INTEL CORE DUO T2250,
760 MB RAM ,
1 Gbit síťová karta čip Marvell

II. Stolní PC I.
OS WINDOWS XP SP2, Knoppix Linux CD
CPU: AMD K8 SEMPRON 2400 +,
512 MB RAM,
100Mbit síťová karta čip Realtek

III. Stolní PC II.
OS LINUX SUSE 10.1,
CPU:AMD K7 950 MHz,
512 MB RAM,
100 Mbit sítová karta čip Realtek


PC II.
PC I.
ASUS WL550gE
Notebook
INTERNET

Přílohy :

NPToolKit CD

CD1 - Qcheck aplikace a endpoint pod OS Windows i Linux, konfigurace NPToolKit CD , které byla použita v této práci.

Kompletní výpis příkazu web100clt –n 192.168.10.102 –l – l

Kompletní výpis příkazu web100clt –n 192.168.10.102 –l

Kompletní výpis příkazu web100clt –n 192.168.10.102

Použitá literatura:

[1] Internet2. Manual Page: **One-way Ping (OWAMP)** [online].
Dostupný na WWW: <http://e2epi.internet2.edu/owamp/owampd.man.html>.
[2] Internet2. Manual Page: **Thrulay, network capacity tester** [online].
Dostupný na WWW: <http://e2epi.internet2.edu/thrulay/thrulay.man.html>.
[3] Internet2. **Network diagnostic tool** [online].
Dostupný na WWW: <http://e2epi.internet2.edu/ndt/>.
[4] Rick Jones. **Netperf manual** [online]. Dostupný na WWW:
<http://www.netperf.org/svn/netperf2/tags/netperf-2.4.3/doc/netperf.html>.
[5] IXIA . **Qcheck - Network Performance Measurement** [online]. Dostupný na WWW: http://www.ixiacom.com/products/display?skey=qcheck>.

Kompletní výpis příkazu web100clt –n 192.168.10.102 –l – l

Testing network path for configuration and performance problems -- Using IPv4 address
Checking for Middleboxes . . . . . Done
checking for firewalls . . . . . Done
running 10s outbound test (client to server) . . . . . 93.95 Mb/s
running 10s inbound test (server to client) . . . . . 94.14 Mb/s
The slowest link in the end-to-end path is a 100 Mbps Full duplex Fast Ethernet subnet
Information: Other network traffic is congesting the link
Information [S2C]: Packet queuing detected: 11.94% (local buffers)
Server '192.168.10.102' is not behind a firewall. [Connection to the ephemeral port was successful]
Client is not behind a firewall. [Connection to the ephemeral port was successful]

------ Web100 Detailed Analysis ------

Web100 reports the Round trip time = 70.82 msec;the Packet size = 1448 Bytes; and No packet loss was observed.
This connection is sender limited 1.64% of the time.
This connection is network limited 97.38% of the time.

Web100 reports TCP negotiated the optional Performance Settings to:
RFC 2018 Selective Acknowledgment: ON
RFC 896 Nagle Algorithm: ON
RFC 3168 Explicit Congestion Notification: OFF
RFC 1323 Time Stamping: ON
RFC 1323 Window Scaling: ON; Scaling Factors - Server=10, Client=10
The theoretical network limit is 45.52 Mbps
The NDT server has a 32768 KByte buffer which limits the throughput to 3615.05 Mbps
Your PC/Workstation has a 2684 KByte buffer which limits the throughput to 296.11 Mbps
The network based flow control limits the throughput to 157.10 Mbps

Client Data reports link is ' 5', Client Acks report link is ' 5'
Server Data reports link is ' 5', Server Acks report link is ' 5'
Packet size is preserved End-to-End
Server IP addresses are preserved End-to-End
Client IP addresses are preserved End-to-End
CurMSS: 1448
X_Rcvbuf: 33554432
X_Sndbuf: 33554432
AckPktsIn: 42723
AckPktsOut: 0
BytesRetrans: 0
CongAvoid: 40702
CongestionOverCount: 0
CongestionSignals: 1
CountRTT: 42724
CurCwnd: 935408

CurRTO: 280
CurRwinRcvd: 2748416
CurRwinSent: 6144
CurSsthresh: 729792
DSACKDups: 0
DataBytesIn: 0
DataBytesOut: 126027920
DataPktsIn: 0
DataPktsOut: 85154
DupAcksIn: 0
ECNEnabled: 0
FastRetran: 0
MaxCwnd: 1458136
MaxMSS: 1448
MaxRTO: 324
MaxRTT: 124
MaxRwinRcvd: 2748416
MaxRwinSent: 6144
MaxSsthresh: 729792
MinMSS: 1428
MinRTO: 204
MinRTT: 0
MinRwinRcvd: 6144
MinRwinSent: 5792
NagleEnabled: 1
OtherReductions: 0
PktsIn: 42723
PktsOut: 85154
PktsRetrans: 0
RcvWinScale: 10
SACKEnabled: 3
SACKsRcvd: 0
SendStall: 1
SlowStart: 1007
SampleRTT: 80
SmoothedRTT: 80
SndWinScale: 10
SndLimTimeRwin: 103460
SndLimTimeCwnd: 10295775
SndLimTimeSender: 173127
SndLimTransRwin: 9
SndLimTransCwnd: 11
SndLimTransSender: 2
SndLimBytesRwin: 1243200
SndLimBytesCwnd: 124780280
SndLimBytesSender: 4440
SubsequentTimeouts: 0
SumRTT: 3025504
Timeouts: 0
TimestampsEnabled: 1

WinScaleRcvd: 10
WinScaleSent: 10
DupAcksOut: 0
StartTimeUsec: 342722
Duration: 10572388
c2sData: 5
c2sAck: 5
s2cData: 5
s2cAck: 5
half_duplex: 0
link: 0
congestion: 1
bad_cable: 0
mismatch: 0
spd: 95.36
bw: 45.52
loss: 0.000011743
avgrtt: 70.82
waitsec: 0.00
timesec: 10.00
order: 0.0000
rwintime: 0.0098
sendtime: 0.0164
cwndtime: 0.9738
rwin: 20.9688
swin: 256.0000
cwin: 11.1247
rttsec: 0.070815
Sndbuf: 33554432
aspd: 0.00000

CWND-Limited: 44399.00

Kompletní výpis příkazu web100clt –n 192.168.10.102 –l

Testing network path for configuration and performance problems -- Using IPv4 address
Checking for Middleboxes . . . . . Done
checking for firewalls . . . . . Done
running 10s outbound test (client to server) . . . . . 93.95 Mb/s
running 10s inbound test (server to client) . . . . . 94.14 Mb/s
The slowest link in the end-to-end path is a 100 Mbps Full duplex Fast Ethernet subnet
Information: Other network traffic is congesting the link
Information [S2C]: Packet queuing detected: 11.94% (local buffers)
Server '192.168.10.102' is not behind a firewall. [Connection to the ephemeral port was successful]
Client is not behind a firewall. [Connection to the ephemeral port was successful]

------ Web100 Detailed Analysis ------

Web100 reports the Round trip time = 70.87 msec;the Packet size = 1448 Bytes; and No packet loss was observed.
This connection is sender limited 1.64% of the time.
This connection is network limited 97.29% of the time.

Web100 reports TCP negotiated the optional Performance Settings to:
RFC 2018 Selective Acknowledgment: ON
RFC 896 Nagle Algorithm: ON
RFC 3168 Explicit Congestion Notification: OFF
RFC 1323 Time Stamping: ON
RFC 1323 Window Scaling: ON; Scaling Factors - Server=10, Client=10
The theoretical network limit is 45.49 Mbps
The NDT server has a 32768 KByte buffer which limits the throughput to 3612.50 Mbps
Your PC/Workstation has a 2551 KByte buffer which limits the throughput to 281.23 Mbps
The network based flow control limits the throughput to 156.98 Mbps

Client Data reports link is ' 5', Client Acks report link is ' 5'
Server Data reports link is ' 5', Server Acks report link is ' 5'
Packet size is preserved End-to-End
Server IP addresses are preserved End-to-End
Client IP addresses are preserved End-to-End

Kompletní výpis příkazu web100clt –n 192.168.10.102

Testing network path for configuration and performance problems -- Using IPv4 address
Checking for Middleboxes . . . . . Done
checking for firewalls . . . . . Done
running 10s outbound test (client to server) . . . . . 93.95 Mb/s
running 10s inbound test (server to client) . . . . . 94.14 Mb/s
The slowest link in the end-to-end path is a 100 Mbps Full duplex Fast Ethernet subnet
Information: Other network traffic is congesting the link
Information [S2C]: Packet queuing detected: 11.93% (local buffers)
Server '192.168.10.102' is not behind a firewall. [Connection to the ephemeral port was successful]
Client is not behind a firewall. [Connection to the ephemeral port was successful]
Packet size is preserved End-to-End
Server IP addresses are preserved End-to-End
Client IP addresses are preserved End-to-End