Journal of the Technical University of Gabrovo, Vol. 53'2016 (91-96)

ИЗВЕСТИЯ
на Технически университет
Габрово

ИЗСЛЕДВАНЕ НА СЦЕНАРИИ ЗА ОСИГУРЯВАНЕ КАЧЕСТВО НА ОБСЛУЖВАНЕТО

STUDY SCENARIOS FOR QUALITY OF SERVICE

Мирослав Славов*
Технически университет - Габрово

Статията е постъпила на 08 февруари 2016 г.; след ревизия на 21 март 2016 г.; приета за отпечатване на 24 март 2016 г.

Abstract

This paper presents experimental results from study of typical scenarios for quality of service. The experiments show the impact of the major parameters, which influence the quality of service - packets lost, round trip time, jitter and packets delay. The paper shows the required devices configurations as well as statistics for discarded packets.

Keywords: Quality of Service; Cisco IOS; VoIP; HTTP; FTP.

ВЪВЕДЕНИЕ

Качеството на обслужване (quality of service - QoS) се отнася до няколко свързани аспекта на телефонията и компютърните мрежи, които позволяват предаването на трафик със специфични изисквания. В частност са разработени много технологии, които да позволят компютърните мрежи да станат толкова полезни колкото телефонните мрежи за глас, а също така да се поддържат и нови приложения с дори по-стриктни изисквания към услугите[2].

ИЗЛОЖЕНИЕ

Дефиниции в качество на обслужването [2]

В областта на компютърните мрежи и другите телекомуникационни мрежи, използващи комутация на пакети, управлението на трафика се отнася до контролни механизми за резервиране на ресурсите, а не толкова до постигане на качество на услугите. Качеството на обслужване е способността да се осигурят различни приоритети за различните приложения, потребители или потоци от данни или да се гарантира определено ниво на производителност на потоците от данни. Гарантирането на качество на обслужване е важно, особено за приложения, използващи поточна мултимедия в реално време, тъй като те изискват определена битова грешка и са чувствителни към закъсненията.

Мрежите или приложенията, използващи метода най-добър опит (best-effort) не поддържат качество на обслужването.

Качества на трафика

Ниска пропускателна способност

Поради различното натоварване от други потребители, споделящи общи мрежови ресурси, битовата скорост (максималната пропускателна способност), която се предоставя на определен поток от данни може да бъде прекалено ниска за мултимедийни услуги в реално време, ако всички потоци имат еднакви заложени приоритети.

Изхвърлени пакети

Маршрутизаторът може да не успее да достави някои пакети, ако данните в тях са повредени или ако те пристигнат когато буферите им са препълнени. Получаващото приложение може да поиска тази информация да бъде препредадена и по този начин да предизвика сериозни закъснения в общото предаване.

Грешки

Понякога пакетите са повредени поради шум и интерференция, особено в безжичните комуникации и при дълги медни проводници. Приемникът трябва да открие това и като в случая на загубените пакети, да поиска препредаване на информацията.

Латентност

В някои ситуации даден пакет може да пътува дълго време до местоназначението, тъй като е задържан в дълги опашки или е преминал по по-дълги пътища за да се избегне задръстване. Този параметър е различен от пропускателната способност, тъй като закъснението може да нараства във времето, дори при достатъчна пропускателната способност.

Вариации (jitter)

Пакетите от източника могат да достигат местоназначението с различни закъснения. Закъснението на пакетите варира в зависимост от позицията му в опашките на маршрутизаторите по пътя между източника и получателя. Тези промени в закъснението са познати като вариации и могат сериозно да повлияят на качеството на поточно аудио и/или видео

Доставка в неправилен ред

Когато набор от свързани пакети се маршрутизира през мрежа, различните пакети могат да преминат по различни пътища, всеки с различно закъснение. В резултат пакетите могат да пристигнат в приемника в различен ред от този, под който са били изпратени. Това е много важно за видео и VoIP потоци, където качеството значително се влияе и от латентността и от неправилния ред на пакетите.

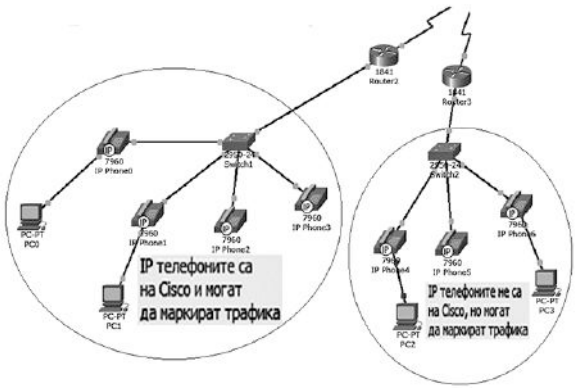
* *Тел.: 066 827 550; e-mail: miroslav_slavov@mail.bg*

Опитна постановка за изследване на качеството на обслужване [1]

На фиг. 1 са представени два фрагмента от проектираната опитна постановка. Разгледани са типични сценарии с IP телефони, които могат да маркират трафика и с такива, които нямат вградена тази функция. Това поражда известни разлики в конфигурацията на устройствата в сегментите.

И за двата сегмента е прието правилото, че IP телефоните ще маркират само гласовия трафик, а трафика за данни ще бъде маркиран в мрежовото устройство.

В избраната топология и двата комутатора извършват маркиране на трафика, а в маршрутизаторите се прилагат политиките по обработка и приоритизиране.



Фиг. 1. Сегмент от мрежата, включващ IP телефони от различни производители с възможност за маркиране на трафика

Първоначално трябва да се активира услугата качество на обслужване чрез следната команда:

SW1(config)#mls qos

В левия сегмент от мрежата телефоните са произведени от фирмата Cisco Systems, при което в конфигурацията се използва само една команда, за доверие в маркирания от тях трафик:

1. Приемане на трафика от телефоните:

interface range fa0/2 - fa0/24
mls qos trust device cisco-phone

Тази команда приема маркирания от телефоните трафик и му се доверява. Тя се изпълнява за всички интерфейси.

2. Маркиране на трафика:

```
class-map HTTP
 match protocol http
class-map FTP
 match protocol ftp
policy-map WEB
 class HTTP
  set ip dscp af21 (18)
 class FTP
  set ip dscp af22 (20)
```

Чрез командата class-map се създава клас, в който се определят видовете трафик. В случая се групират два типа трафик - уеб и трансфер на файлове. След като се групира трафика той трябва да бъде маркиран. За целта се създава политика за обработка на трафика. Обработката се състои в маркирането му със съответната кодова точка (DSCP). Кодовите точки afXX (XX - пореден номер) и кодова точка ef са приети за еталонни. Използването на еталонните кодови точки не е задължително и може да се използват действителните стойности, но те не дават гаранция за еднакво третиране на трафика в различните мрежи.

За прихващането на трафика може да се използват различни критерии (IP адрес, номер на порт, използван протокол и др.).

3. Прилагане на политиката:

След като се класифицира трафика и се създаде политика, тя трябва да бъде приложена на интерфейс във входяща или изходяща за мрежовото устройство посока:

```
interface fa 0/1
 service-policy output WEB
```

Опитни резултати

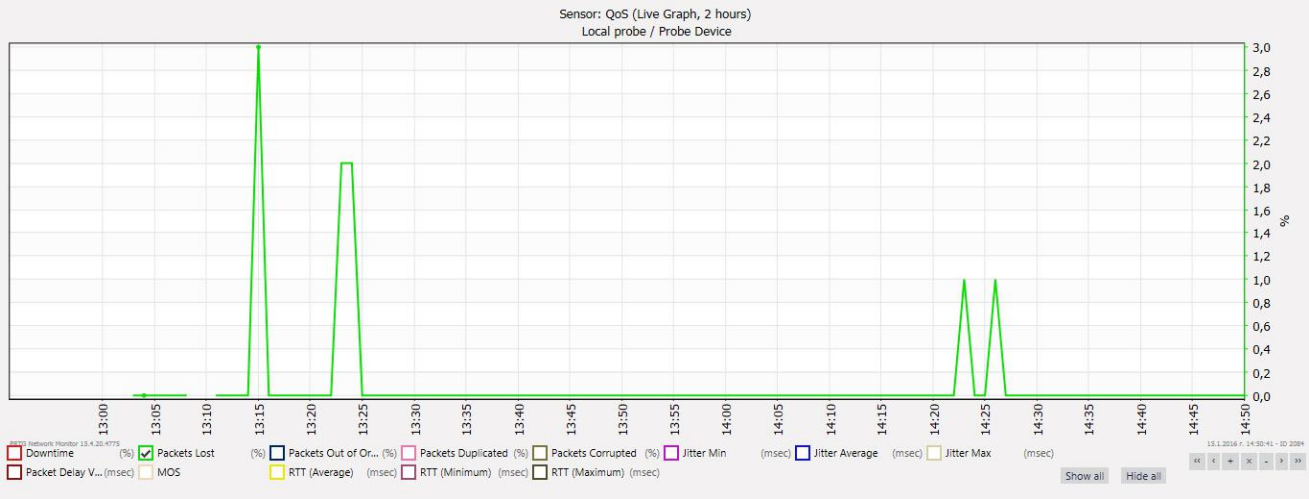
За изследване състоянието на мрежата и поведението на устройствата спрямо трафика, се използва програмата Paessler. Програмата използва един сървър, който изпраща определен брой пакети, с определен размер, използвайки UDP протокол, до една или няколко отдалечение сонди. За целта в сървъра се добавят сензори, които изпращат, получават и обработват информацията. За нуждите на изследването се използва сензор, който следи параметрите на качеството на обслужване. Тъй като отдалечените сонди се инсталират на машини с точно определен, известен адрес и използват определен номер на порт (50000 по подразбиране, но може да се променя за отделните сонди), трафика изпращан до тях и от тях може да бъде разпознат и да бъде прихванат в мрежата. Тази възможност се използва, за да се конфигурират устройствата в мрежата, да маркират този трафик с определени dscp стойности и по този начин да се изследва поведението на мрежата и устройствата по отношение на маркирания трафик. За настоящите изследвания се използват две отдалечени сонди, инсталирани на различни компютри, като трафика от програмата се маркира с dscp стойност *ef* (идентично маркиране с гласовия трафик) към едната отдалечена сонда, и с dscp стойност *af22* (идентично с FTP трафик). Освен тези два типа трафик, в мрежата преминава още няколко трафика, който се маркират и това са HTTP трафик, SIP трафик и трафика от маршрутизиращия протокол, който е необходим, за да функционира мрежата. За да може да се натовари мрежата и да се изследва поведението на политиките за качество на обслужване се използва допълнителен софтуер, който генерира трафик и предизвиква задръстване в мрежата. Пакетите от тази програма не се маркират и преминават без предимство през мрежата.

Информацията за маркирания трафик и начина на обработка от маршрутизаторите е следната:

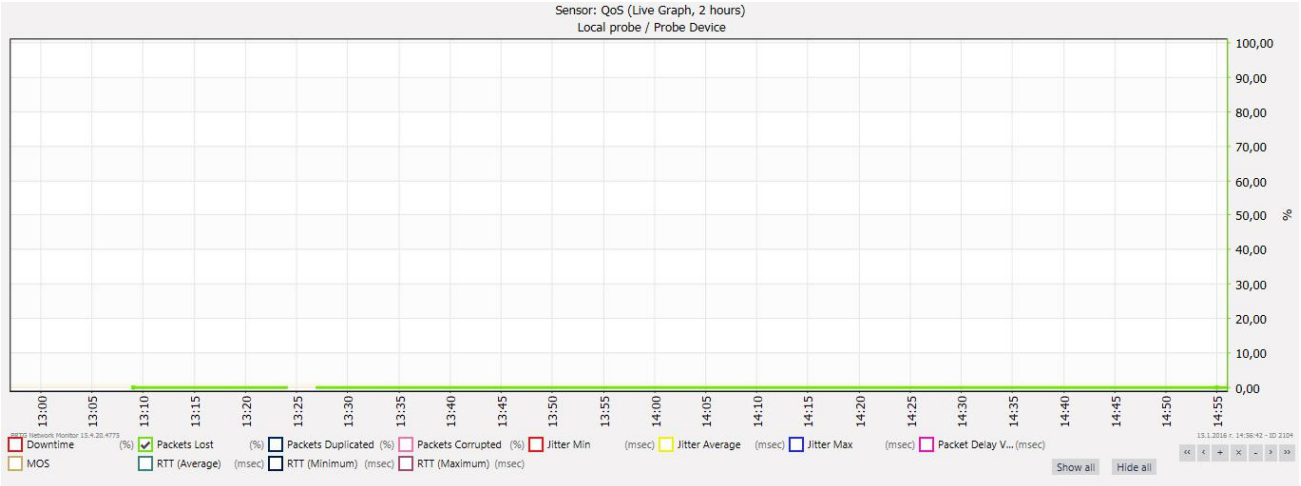
```
Service-policy output: WEB_VOICE
  queue stats for all priority classes:
    queue limit 64 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 24661/4924686
  Class-map: HTTP (match-all)
    43152 packets, 64749534 bytes
    30 second offered rate 0 bps, drop rate 0 bps
    Match:  dscp af21 (18)
    Queueing
    queue limit 64 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 43152/64749534
    bandwidth 30% (150 kbps)
  Class-map: FTP (match-all)
    55500 packets, 11766000 bytes
```

30 second offered rate 11000 bps, drop rate 0 bps
Match: dscp af22 (20)
Queueing
queue limit 64 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 55500/11766000
bandwidth 30% (150 kbps)
Class-map: VOICE (match-any)
23202 packets, 4833382 bytes
30 second offered rate 2000 bps, drop rate 0 bps
Match: dscp ef (46)
23119 packets, 4804163 bytes
30 second rate 2000 bps
Match: dscp af41 (34)
83 packets, 29219 bytes
30 second rate 0 bps
Priority: 20% (100 kbps), burst bytes 2500, b/w exceed drops: 14
Class-map: EIGRP (match-all)
1473 packets, 90612 bytes
30 second offered rate 0 bps, drop rate 0 bps
Match: protocol eigrp
QoS Set
precedence 6
Packets marked 1473
Priority: 8 kbps, burst bytes 1500, b/w exceed drops: 0
Class-map: class-default (match-any)
93686 packets, 135515294 bytes
30 second offered rate 0 bps, drop rate 0 bps
Match: any
Queueing
queue limit 64 packets
(queue depth/total drops/no-buffer drops/flowdrops) 0/2319/0/2319
(pkts output/bytes output) 91367/132059984
Fair-queue: per-flow queue limit 16

От изведената информация може да се види колко пакети са преминали през устройствата и каква част от общата пропускателна способност са резервирани за съответния трафик. Всяко устройство разполага с една приоритетна опашка, която се обработва с предимство преди всички останали. В този случа тя е предназначена за гласовия трафик (VOICE) и трафика на маршрутизиращия протокол (EIGRP). Но приоритетната опашка е ограничена (policed), т.е. пакетите в нея могат да превишават зададения размер (burst), но губят приоритета си и се третират като немаркирани пакети. Поради тази причина има и няколко изхвърлени пакета, маркирани с dscp стойност *ef (exceed drops)*. На фигура 2 и 3 са показани графики на загубите на пакети при маркиране на трафика с dscp стойност ef (фиг. 2) и стойност af22 (фиг. 3).

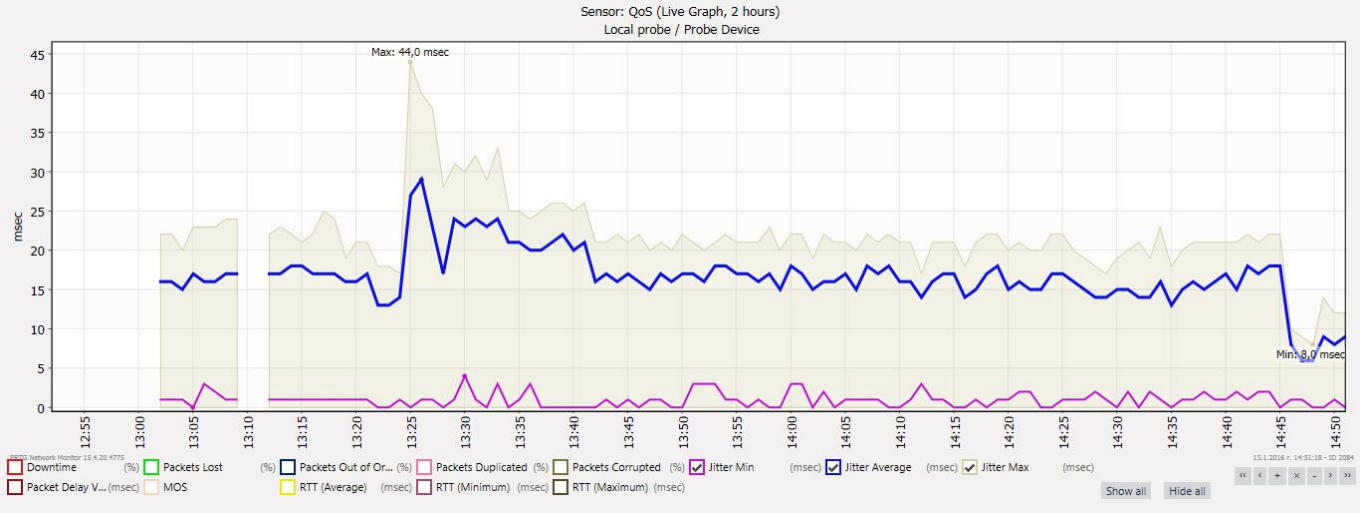


Фиг. 2. Графики на измерените загуби на пакетите, когато през мрежата преминава HTTP, FTP и гласов трафик, като пакетите от тестващата програма се маркират като гласов трафик.

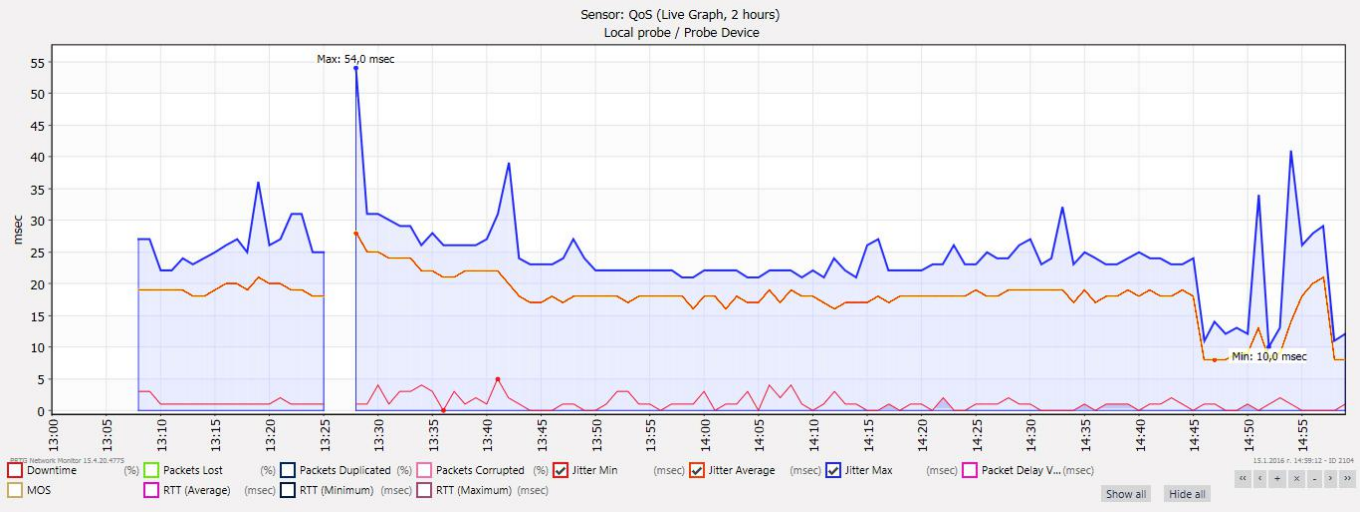


Фиг. 3. Графики на измерените загуби на пакетите, когато през мрежата преминава HTTP, FTP и гласов трафик, като пакетите от тестващата програма се маркират като FTP трафик.

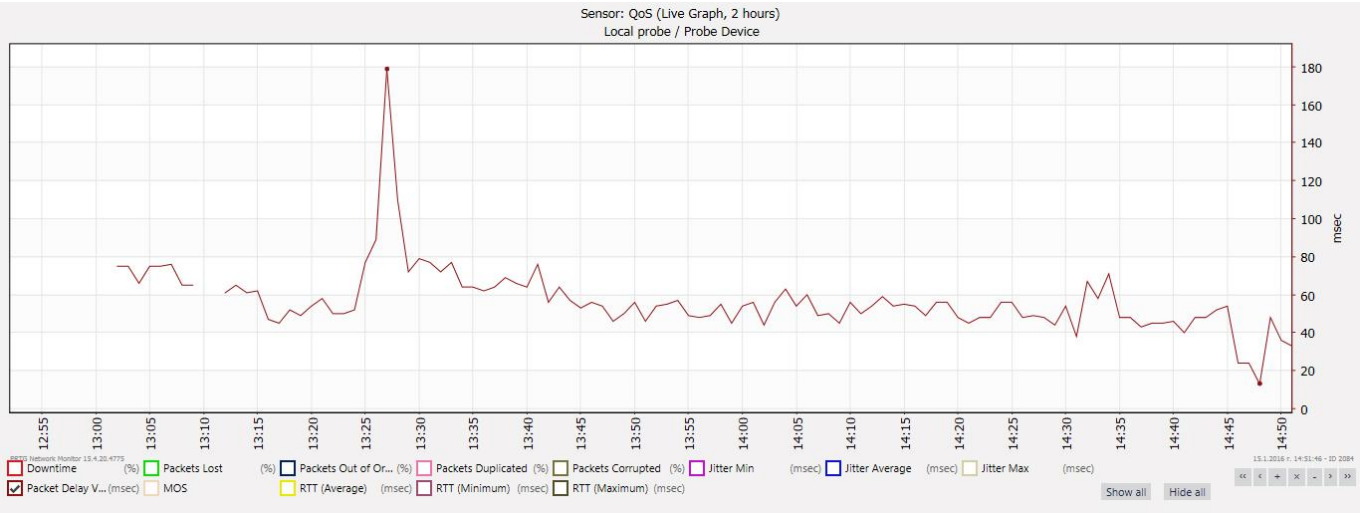
Причината за наличието на загуби при предаване на трафик, маркиран със стойност ef е тази, че той използва приоритетната опашка и се изхвърлят пакетите, използващи превишаването на размера burst traffic). На следващите фигури са показани графики на останалите параметри, влияещи върху качеството на обслужване - закъснение на пакетите, вариации на закъснението (jitter) и време за двупосочно преминаване (round trip time - RTT).



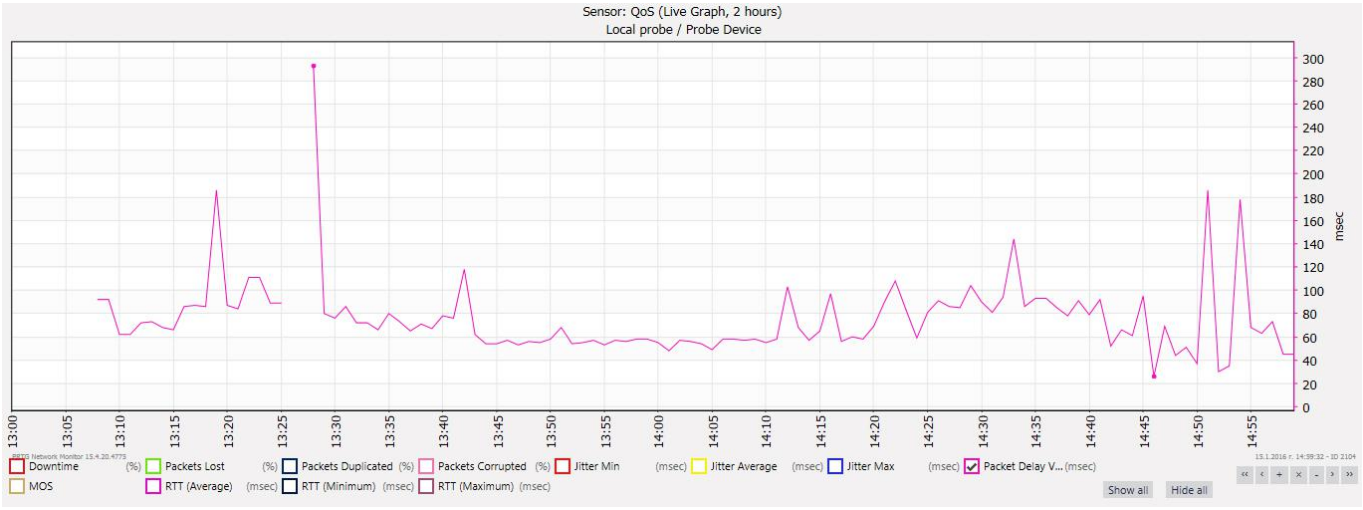
Фиг. 4. Графики на измерения джитер, когато през мрежата преминава HTTP, FTP и гласов трафик, като пакетите от тестващата програма се маркират като гласов трафик - минимален, следен и максимален..



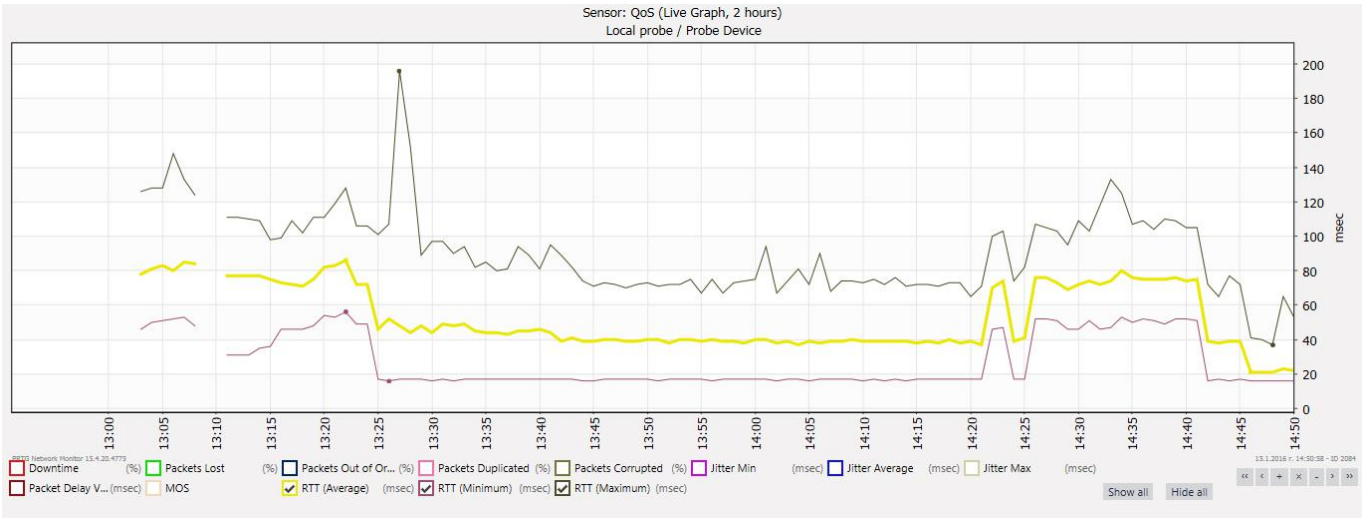
Фиг. 5. Графики на измерения джитер, когато през мрежата преминава HTTP, FTP и гласов трафик, като пакетите от тестващата програма се маркират като FTP трафик - минимален, среден и максимален..



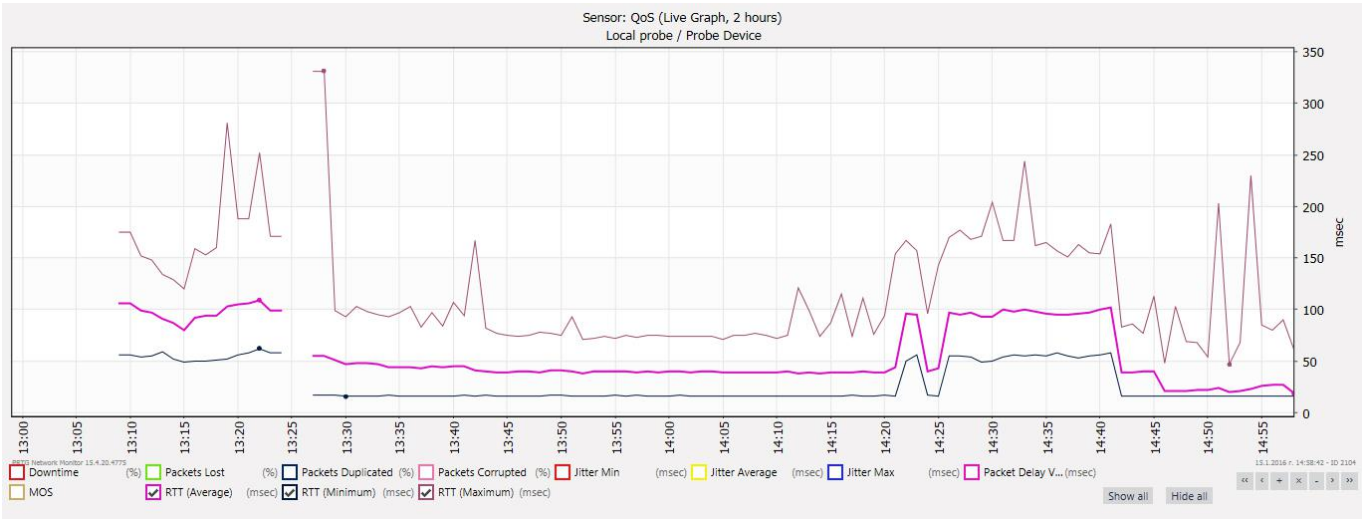
Фиг. 6. Графики на измереното закъснение на пакетите, когато през мрежата преминава HTTP, FTP и гласов трафик, като пакетите от тестващата програма се маркират като гласов трафик.



Фиг. 7. Графики на измереното закъснение на пакетите, когато през мрежата преминава HTTP, FTP и гласов трафик, като пакетите от тестващата програма се маркират като FTP трафик.



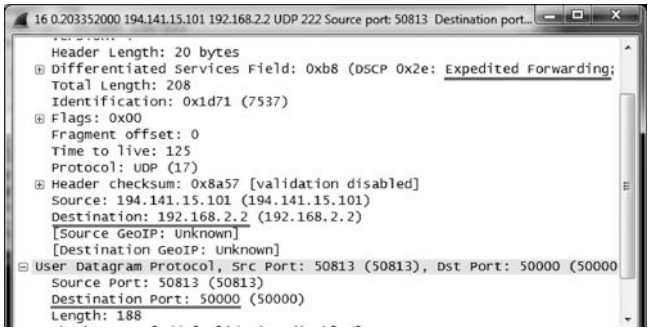
Фиг. 8. Графики на измереното време за двупосочно преминаване на пакетите, когато през мрежата преминава HTTP, FTP и гласов трафик, като пакетите от тестващата програма се маркират като гласов трафик - минимално, средно и максимално.



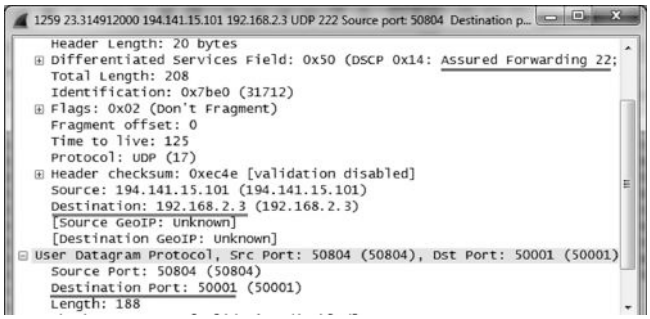
Фиг. 9. Графики на измереното време за двупосочно преминаване на пакетите, когато през мрежата преминава HTTP, FTP и гласов трафик, като пакетите от тестващата програма се маркират като FTP трафик - минимално, средно и максимално.

От представените графики се вижда, че параметрите на трафика, когато той се маркира със стойност ef са по-добри в сравнение с тези, когато той се маркира с af22. Това означава, че този трафик получава приоритет спрямо маркирания с af22. Това показва, че трафика използващ приоритетната опашка преминава по-бързо и с по-добри параметри през мрежата, затова този трафик се използва от услугите в реално време - глас и телевизия по IP. От представената по-рано статистика за преминалия през маршрутизаторите трафик се вижда, че единствения трафик, който се изхвърля и страда от задръстванията в мрежата е този, който не се маркира и към който не се прилагат никакви политики за качество на обслужването. На фигура 10 и 11 са показани заглав-

ните части на пакети, преминали през устройствата. Тези пакети са прихванати с програмата Wireshark и показват какво се е случило с пакетите, преминали през мрежата.



Фиг. 10. Заглавна част на тестов пакет, маркиран като гласов трафик



Фиг. 11. Заглавна част на тестов пакет, маркиран като FTP трафик

Вижда се заглавната част на два пакета, изпратени от тестовата програма Paessler. Единия пакет се маркира като гласов трафик, което е от dscp стойността - Expedited Forwarding (EF), а другия като FTP трафик със стойност Assured Forwarding 22 (AF22). Освен това на фигурите са показани адресите на получателя, както и порта, който се използва от отдалечената сонда. Тъй като те са различни се използват като признаци за разпознаване и маркиране на трафика.

ЗАКЛЮЧЕНИЕ

Предложената схема е приложима и предоставя възможност да се изследват различни сценарии за осигуряване на качество на обслужването. Тя позволява да се покажат, как работят едновременно и си взаимодействат няколко услуги в една насложена мрежа при различни условия. Това позволява някой от услугите, за които са от критично значение параметрите на мрежата, да бъдат приоритизирани пред останалите и да преминат през нея по начин, който да позволи висока скорост и качество на данните.

ЛИТЕРАТУРА

[1] Славов М., Проектиране на опитна постановка за изследване на типични сценарии за качество на обслужването, Международна научна конференция UNITECH 2015, Габрово 2015.

[2] https://en.wikipedia.org/wiki/Quality_of_service.