

Проектиране, изграждане и експериментална оценка на телекомуникационна мрежа с поддръжка на мобилност посредством IPv4

Дияна Кючукова, Георги Христов

Design, deployment and evaluation of IPv4 network with mobility support: Due to the increasing of mobile nodes, there has been an increasing demand for Mobile Internet access. However, some problems need to be solved before mobile access to the Internet can become widespread. A first problem is caused by the way the Internet Protocol (IP) routes packets to their destination according to IP addresses. These addresses are associated with a fixed network location and would not work in a mobile environment since when the mobile node moves, it will eventually reach a new network, with a new network number and a new IP address.

Key words: Mobile Internet Protocol, Mobile IPv4, Home Agent, Foreign Agent, Mobile Node, Correspondent Node, Care-of-Address, Roaming, TCP, UDP, ICMP.

ВЪВЕДЕНИЕ

Едно от най-значимите постижения в сферата на комуникациите – Интернет, доведе до обрат в начина, по който хората общуват и правят бизнес. През последните години значително се увеличили броя на мобилните устройства, което предполага нарастване на търсенето на мобилен Интернет достъп. Мобилността е силно желана и важна характеристика за компании, организации и служители, които непрекъснато изискват достъп до различни web услуги, електронни пощи, електронно банкиране и др. Ето защо тя е задължителна функция на IP протокола. Преди мобилният интернет достъп да стане широко разпространен, обаче трябва да се решат няколко проблема. Първият проблем е причинен от начина, по-който Интернет протокола маршрутизира пакети според техните IP адреси. Тези адреси принадлежат на стационарни мрежи и заради това те не могат да функционират в мобилна среда. Когато потребителите са в движение, те рано или късно напускат своята локална мрежа и достигат до друга такава, която използва друго адресно пространство. За да могат устройствата да запазят достъпа си до Интернет, дори когато се движат и сменят точката си за достъп се налага използването на Мобилният Интернет протокол (Mobile IP). Той дава възможност мобилните устройства да комуникират, запазвайки IP адресите си дори при смяна на точката си за достъп.

ПРЕГЛЕД НА MOBILE IP ПРОТОКОЛА

Мобилният IP познат още като IP mobility, е стандартен интернет протокол разработен и дефиниран от IETF (*Internet Engineering Task Force*). Основната му функция е да поддържа IP комуникация между мобилни устройства, докато преминават от една мрежа в друга, без да променят IP адресите си. Той реализира комуникация, независеща от местоположението на устройствата.

Предаването на дейтаграми от едно устройство към друго се извършва от маршрутизаторите. Това са устройства, които съдържат информация за мрежите и тяхното местоположение. Те използват мрежовата част на IP адреса за да преценят къде да изпратят съответните IP пакети. Последният маршрутизатор – този който е директно свързан към мрежата на получателя, използва потребителската част на IP адреса за да достави IP пакетите. Процесът по доставянето на пакети се усложнява, когато получателят на тези IP пакети е мобилен, тоест в момента на доставянето на пакети, той може да „отсъства“ от локалната мрежа, към която принадлежи. За да успее да получи предназначените за него дейтаграми, дори когато е извън своята мрежа, се намесва мобилният IP протокол.

За да се разбере как работи мобилността, е важно да се знаят елементите на

мобилният интернет протокол. В една мобилна мрежа има три вида устройства: локален маршрутизатор (*Home-Agent*), отдалечен маршрутизатор (*Foreign-Agent*) и мобилно устройство (*Mobile Node*) - фиг.1.



Фиг. 1 - Елементи на мобилна комуникационна IP мрежа [1]

Мобилно устройство (*Mobile Node*) – известно още като роуминг устройство. Мобилното устройство може да бъде маршрутизатор или крайно потребителско устройство, които използват мобилния IP протоколен стек. То може да променя точката си за достъп, като едновременно с това поддържа връзка с локалната си мрежа. [1]

Локален маршрутизатор (*Home Agent*) – шлюз по подразбиране на локалната мрежа. Този маршрутизатор отговаря за доставката на дейтаграми към мобилното устройство. В случаите, когато мобилното устройство е извън своята мрежа, локалния маршрутизатор (*HA*) тунелира дейтаграмите към отдалечения маршрутизатор (*FA*). [1]

Отдалечен маршрутизатор (*Foreign Agent*) – шлюз по подразбиране на посетената от мобилното устройство мрежа. Той детунелира дейтаграмите, получени от локалния маршрутизатор и ги предава към мобилното устройство. [1]

Освен трите термина относящи се до типовете устройства в мобилна мрежа, ще бъдат изяснени и някои понятия, касаещи принципа на действие на мобилността.

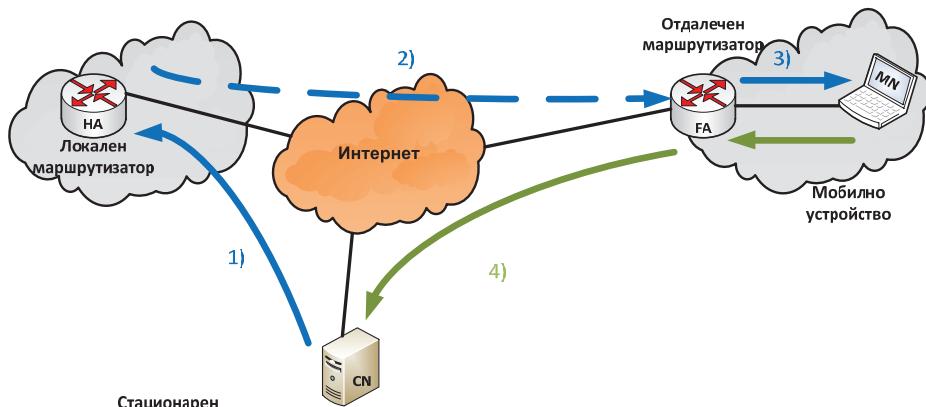
Носещ адрес (*Care-of-Address*) – крайната точка на тунела, която доставя дейтаграмите до мобилното устройство. Мобилното устройство може да има няколко носещи адреси, но този който е съгласуван с локалния маршрутизатор се счита за основен носещ адрес. [2]

Откриване на маршрутизатор (*Agent Discovery*) – Всички мобилни маршрутизатори (*Home-Agent*, *Foreign-Agents*) обявяват своята наличност в мрежата, като изпращат периодични съобщения, чрез които предлагат своите услуги. Когато даден нов клиент се присъедини към мобилна мрежа, той изпраща съобщение, под формата на запитване (*solicitation message*) за да открие дали има налични мобилни маршрутизатори. [3]

Вписване (*Registration*) – вписването е процес, при който Мобилното устройство, намиращо се в отдалечена мобилна мрежа (*Foreign Network*), съгласува своя носещ адрес с локалния маршрутизатор.

Тунелиране (*Tunneling*) – след процеса на регистрация (вписване) локалния маршрутизатори (*HA*) и отдалечения такъв (*FA*) изграждат помежду си тунел. През този тунел се предават дейтаграмите към мобилното устройство, когато то се намира извън своята локална мрежа. [4]

На фиг. 2 е представен схематично принципа на действие на мобилния интернет протокол (Mobile IPv4). [3]



Фиг. 2 - Принцип на действие на мобилния IPv4 протокол [1]

Мобилността в IPv4 протокола се управлява от три компонента – локален маршрутизатор, отдалечен маршрутизатор и мобилно устройство. Всяко мобилно устройство притежава два IP адреса – първия е статичен адрес, който е част от локалната мрежа на мобилното устройство, а вторият е носещ адрес, който се променя всеки път, когато мобилното устройство сменя точката си за достъп. Когато мобилното устройство се намира в локалната си мрежа, доставянето на пакети до него се реализира на база на стандартно маршрутизиране.

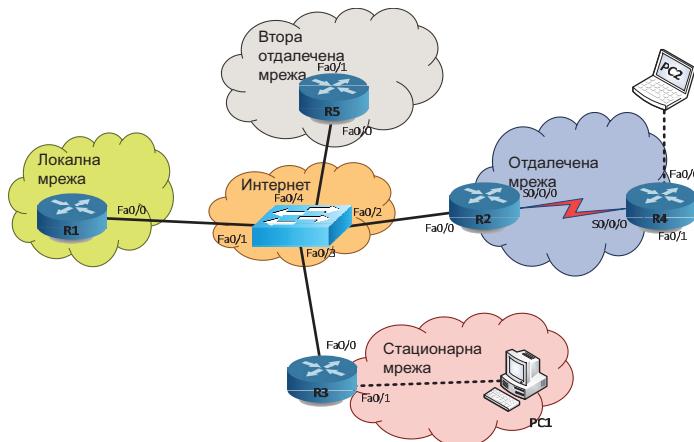
В една мобилна мрежа могат да се забележат два типа маршрутизиране на данните – индиректно и директно предаване. Когато даден стационарен клиент изпраща данни до мобилното устройство, в заглавната част на мрежовия протокол се добавя информация за адреса на получателя. Този адрес в случая е постоянния адрес на мобилното устройство. Постоянният адрес е част от адресното пространство на локалната мрежа, затова тези данни, които стационарния потребител изпраща се получават в локалния маршрутизатор. Характерно за мобилността е, че локалния маршрутизатор синхронизира информация с отдалечения маршрутизатор. Благодарение на това синхронизиране, локалния маршрутизатор „знае“ в коя мрежа се намира мобилното устройство. Между двата маршрутизатора се изгражда тунел, по който се предават данните от локалния маршрутизатор до мобилното устройство. Този тип предаване се нарича индиректно. Директно предаване е това, при което мобилното устройство генерира данни до стационарен клиент. Когато се капсулират тези данни, в заглавието на IP пакета се добавя адреса на стационарен клиент. Отдалечения маршрутизатор използва стандартно маршрутизиране на данните от мобилното устройство до стационарен клиент. Цялостната комуникация между мобилното устройство и стационарен клиент преминава през така нареченото триъгълно маршрутизиране. Информация за триъгълното маршрутизиране може да се намери в литературни източници [1], [2], [3], [4], [5] и [6].

СХЕМА НА ОПТИЧНАТА ПОСТАНОВКА

За проектирането и изграждането на телекомуникационна мрежа с поддръжка на мобилност е използван софтуерен продукт GNS (*Graphical Network Simulator*). Този продукт се използва за симулирането на сложни мрежи. Работи съвместно с няколко емулятора, благодарение на които не се налага използването на специализиран мрежови хардуер (комутатори, маршрутизатори и други), необходим за реализирането и експерименталната оценка на телекомуникационна мрежа

поддържаща мобилност. В настоящата разработка е използван софтуерен емулятор *Dynamips*, който емулира CISCO IOS операционна система върху компютърна машина. С други думи този продукт използва ресурсите на компютър за да го накара да работи като мрежови хардуер.

На фиг. 3 е илюстрирана телекомуникационна мрежа поддържаща мобилност посредством IPv4 протокола, която е проектирана с цел експериментална оценка на мобилността.



Фиг. 3 - Дизайн на телекомуникационна мрежа поддържаща мобилност посредством IPv4 протокола

Емулирани са CISCO маршрутизатори, чиято платформа е c3700. Петте маршрутизатора работят с една и съща операционна система – c3725-adviservicesk9-M. Както се вижда от фигурата по-горе, R1 е локалния маршрутизатор, R2 и R5 – отдалечени маршрутизатори, R3 – шлюз по подразбиране за стационарен клиент, а R4 играе роля мобилно устройство.

Най-лесният начин да се провери дали проектираната мрежа е изградена и конфигурирана правилно, е да се изпратят ICMP заявки от мобилното устройство до стационарното и обратно. За да се проверят и преходите, през които преминават данните е най-удобният използването на *tracert* команда в командния прозорец на съответното устройство. Изходните данни са показани в таблиците по долу.

Табл. 1 - ICMP заявка от стационарния до мобилния клиент

```
C:\Users\Miro>tracert 93.15.20.20
```

```
Tracing route to DIYANA-PC [93.15.20.20]
over a maximum of 30 hops:
```

1	13 ms	9 ms	7 ms	192.168.30.1	!!! Fa0/1 - R3 !!!
2	32 ms	33 ms	23 ms	192.168.10.1	!!! Fa0/0 - R1 !!!
3	53 ms	50 ms	46 ms	172.16.10.1	!!! Loopback int - R4 !!!
4	54 ms	49 ms	46 ms	DIYANA-PC [93.15.20.20]	

```
Trace complete.
```

```
C:\Users\Miro>
```

Табл. 2 - ICMP заявка от мобилния до стационарния клиент

C:\Users\DIYANA>tracert 192.168.30.10

```
Tracing route to MIRO-PC [192.168.30.10]
over a maximum of 30 hops:
```

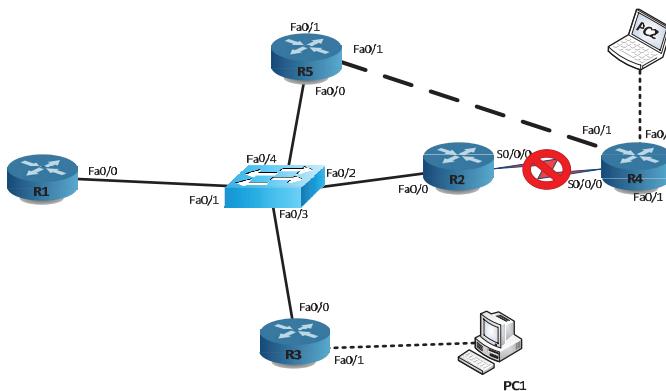
1	24 ms	9 ms	9 ms	93.15.20.0	!!! Fa0/0 - R4 !!!
2	32 ms	28 ms	29 ms	192.168.20.1	!!! S0/0/0 - R2 !!!
3	47 ms	39 ms	40 ms	192.168.10.3	!!! Fa0/0 - R3 !!!
4	42 ms	42 ms	55 ms	MIRO-PC [192.168.30.10]	

Trace complete.

C:\Users\DIYANA>

ЕКСПЕРИМЕНТАЛНА ОЦЕНКА НА ПРОЕКТИРАНАТА МРЕЖА

След като мрежата е вече изградена следва експериментална оценка. Направени са няколко теста, който имат за цел да проследят мрежовото закъснение, загубата на пакети по време на роуминг и честотната лента. Роуминг се нарича прехода от една отдалечена мрежа към друга по време на комуникация. Той е реализиран чрез изграждане на *Ethernet* връзка между R4 (мобилния маршрутизатор) и R5 (вторият отдалечен маршрутизатор) и премахване на серийната връзка между R4 и R2 (първият отдалечен маршрутизатор). Това е показано на фиг.4.



Фиг. 4 - Преход от една отдалечена мрежа към друга по време на комуникация - роуминг

Мрежовото закъснение е времето от предаването на рамка до нейното получаване. Източниците на мрежово закъснение са 3 – мрежови карти, преносна среда, мрежови устройства. Мрежовите карти добавят мрежово закъснение изразено във времето необходимо за конвертиране на битовете информация в сигнални импулси – електрически, светлинни или радио. Преносната среда също добавя мрежово закъснение, което е вследствие на разпространението на сигналните импулси по кабели/ефир. Третият източник на мрежово закъснение са мрежовите устройства. Те добавят закъснение, като е вследствие на процесите по обработване на получената информация – декапсулиране и повторно капсулиране на кадрите/пакетите.

За измерване на мрежовото закъснение и загубата на пакети отново се използва ICMP заявки. Изходните данни от командата ping показват отчетеното

мрежово закъснение. Първият тест е направен, чрез изпращане на стандартни ICMP пакети, чиято големина е 32 байта.

```
C:\Users\Miro>ping -t 93.15.20.20
Pinging 93.15.20.20 with 32 bytes of data:
Reply from 93.15.20.20: bytes=32 time=56ms TTL=125
Reply from 93.15.20.20: bytes=32 time=54ms TTL=125
Reply from 93.15.20.20: bytes=32 time=47ms TTL=125
Reply from 192.168.10.4: Destination host unreachable.
Reply from 93.15.20.20: bytes=32 time=75ms TTL=125
Reply from 93.15.20.20: bytes=32 time=51ms TTL=125
Reply from 93.15.20.20: bytes=32 time=52ms TTL=125
Ping statistics for 93.15.20.20:
    Packets: Sent = 7, Received = 7, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 47ms, Maximum = 75ms, Average = 55ms
Control-C
^C
C:\Users\Miro>
```

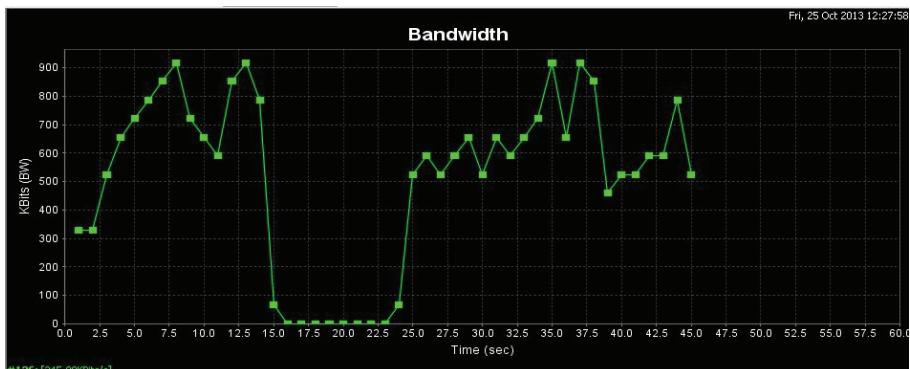
От изходните данни се вижда времето от предаването на кадър, до получаване на потвърждение за неговото получаване. Това време е вследствие на мрежовото закъснение. Забелязва се също и един пакет, който не успял да достигне до крайната цел. Причината за това е роуминга – прехода от една мрежа в друга и времето необходимо на маршрутизиращите протоколи да конвергират мрежата.

Вторият тест е направен с използване отново на ICMP заявки, но този път големината на пакетите е 1024 байта.

```
Pinging 93.15.20.20 with 1024 bytes of data:
Reply from 93.15.20.20: bytes=1024 time=57ms TTL=125
Reply from 93.15.20.20: bytes=1024 time=63ms TTL=125
Reply from 93.15.20.20: bytes=1024 time=54ms TTL=125
Reply from 93.15.20.20: bytes=1024 time=51ms TTL=125
Reply from 93.15.20.20: bytes=1024 time=45ms TTL=125
Reply from 93.15.20.20: bytes=1024 time=69ms TTL=125
Reply from 93.15.20.20: bytes=1024 time=56ms TTL=125
Reply from 93.15.20.20: bytes=1024 time=51ms TTL=125
Reply from 93.15.20.20: bytes=1024 time=164ms TTL=125
Reply from 93.15.20.20: bytes=1024 time=82ms TTL=125
Reply from 93.15.20.20: bytes=1024 time=44ms TTL=125
Request timed out.
Request timed out.
Reply from 93.15.20.20: bytes=1024 time=44ms TTL=125
Reply from 93.15.20.20: bytes=1024 time=47ms TTL=125
Reply from 93.15.20.20: bytes=1024 time=49ms TTL=125
Reply from 93.15.20.20: bytes=1024 time=61ms TTL=125
Reply from 93.15.20.20: bytes=1024 time=68ms TTL=125
Reply from 93.15.20.20: bytes=1024 time=50ms TTL=125
Reply from 93.15.20.20: bytes=1024 time=50ms TTL=125
Reply from 93.15.20.20: bytes=1024 time=47ms TTL=125
Reply from 93.15.20.20: bytes=1024 time=47ms TTL=125
Ping statistics for 93.15.20.20:
    Packets: Sent = 22, Received = 20, Lost = 2 (9% loss),
Approximate round trip times in milli-seconds:
    Minimum = 44ms, Maximum = 164ms, Average = 59ms
Control-C
C:\Users\toni>C:\Users\toni>ping -t 93.15.20.20
```

Вторият тест показва две загуби. Може да се направи извода, че при по-големи пакети загубите са по-големи. Отново тези загубени ICMP пакети са вследствие на прехода от една мрежа за достъп към друга. От изходните данни може да се види също, че мрежовото закъснение е по-голямо, но това е нормално, тъй като и големината на пакетите е по-голяма.

Последният тест измерва честотната лента. За него е използван софтуерен продукт jperf. Той представлява графичен анализатор, който генерира определен вид трафик, като изчертава графика на характера на трафика. Изходните данни от последния тест са показани на фиг. 5.



Фиг. 5 - Честотна лента (Bandwidth)

От фиг.5 може да се направи извода, че от 15 до 25 сек няма предаване на информация. Този период от време, в който честотната лента е „празна“ е вследствие отново на роуминга.

ЗАКЛЮЧЕНИЕ

Триъгълното маршрутизиране има няколко основни недостатъка. Един от тях е, че маршрутизирането е изключително неефективно, ако мобилният клиент и стационарният потребител се намират в една мрежа, тъй като те не могат да си комуникират директно на локално ниво. Вторият недостатък се поражда от факта, че заявките от стационарния клиент към мобилния се изпращат до един адрес, а отговорите се получават от друг. В този случай комуникацията може да бъде блокирана от политики за сигурност, инсталирани на стационарния клиент. При новото поколение интернет протокол – IPv6, триъгълното маршрутизиране е избегнато и при него липсват тези недостатъци.

ЛИТЕРАТУРА

- [1] Raab, Stefan, Chandra, Madhavi W., Leung, Kent & Baker, Fred. Mobile IP Technology and Applications. Publisher: Cisco Press, 2005
- [2] Hagen, Silvia. IPv6 Essentials, Second edition, O'Reilly, 2006
- [3] Dooley, Kevin & Brown, Ian. Cisco IOS Cookbook, 2nd Edition Publisher: O'Reilly, 2006
- [4] Perkins, C. (ed.). IP Mobility Support <http://www.ietf.org/rfc/rfc2002.txt>, 2011
- [5] Janevski, Toni. Traffic Analysis and Design of Wireless IP Networks. Norwood: Artech House, Incorporated, 2003
- [6] Chang, Sujeong, Park, Jaehyung, Won, Yonggwan, Yang, Mijeong, and Chung, Min Young, (2005). Performance Comparison of TCP Traffic over Mobile IPv4 and IPv6

Networks and a Mobile Network Deployment Approach, the 2005 The Fifth International Conference on Computer and Information Technology (CIT'05).

БЛАГОДАРНОСТИ

Публикуваните резултати са получени при работа по проект BG051PO001-3.3.06-0008 „Подпомагане израстването на научните кадри в инженерните науки и информационните технологии“ с подкрепата на Европейския социален фонд и Министерството на образованието и науката на Република България и по проект 2013-ФЕЕА-02 на Русенски Университет „Ангел Кънчев“.

За контакти:

Дияна Кючукова, Катедра “Компютърни системи и технологии”, Русенски университет “Ангел Кънчев”, тел.: 0889-643-456, e-mail: diyana.kyuchukova@abv.bg

доц. Георги Христов, Катедра “Компютърни системи и технологии”, Русенски университет “Ангел Кънчев”, тел.: 082-888-663, e-mail: gchristov@uni-ruse.bg

Докладът е рецензиран.