



**ТЕХНИЧЕСКИ УНИВЕРСИТЕТ – СОФИЯ**

---

Факултет по телекомуникации

Специалност: Телекомуникации

# Курсова работа по ТКПИК

*Тема:*

Разучаване на работата на Rosen MVPN

**Студент:** инж. Николай Проданов    Фак. №: 111321045    Група: 232

**Преподавател:** доц. д-р инж. Камелия Николова

Дата: .....

Подпис: .....

София, 2022

## Съдържание

Увод .....	3
Теоретична част.....	5
1 MPLS L3VPN .....	5
2 Rosen MVPN.....	8
Използвани източници .....	14

## Увод

В края на 20-ти и началото 21-ви век светът е свързан както никога до сега. Това позволило на бизнеси и компании да се разгърнат отвъд рамките на един град или държава като по този начин могат да намерят по-добри условия. За да може да се осъществи това разгръщане и същевременно да се запази достъпът до бази данни и други ресурси към новите клонове, частната мрежа на компания трябвало да се свърже към някоя публична мрежа като интернет. Това довело до редица рискове понеже давало възможност на външни лица достъп до частната мрежа. За да се реши този проблем се зародила идеята за така наречената виртуална мрежа. Виртуалната мрежа представлява вид абстракция чрез която се създава логическа мрежа върху съществуваща физическа мрежа. Това става прозрачно като логическата мрежа съществува като самостоятелна единица сама по себе си и не знае за физическата мрежа отдолу. Друго предимство на тази абстракция е че върху една физическа мрежа може да се създадат няколко логически мрежи които са непълно независими една от друга. Това прави логическата мрежа една изолирана среда. От тук идва и терминът частна мрежа. С тези цели се развива технологията за виртуална частна мрежа или съкратено VPN (Virtual Private Network).

В днешно време VPN технологиите са залегнали в основата на всички международни компании и необходимостта от тях продължават да расте. Това довежда и до по-голямата необходимост от мултикаст VPN (MVPN). Мултикастът в IP базираните мрежи позволява на един източник да произведе пакет предназначен за повече от един получател или „група“ от получатели. Това се използва за редуциране на големият брой пакети носещи еднаква информация в мрежата. Видео и аудио стрийминг услугите използват тези

функции за да предават кадри от едно и също видео или мелодия към всички слушатели.

Мултикаст VPN-а е технология с която се превъзможват ограниченият на до сегашните VPN технологии които маршрутизират мултикаст пакетите като уникат или поддържат мултикаст но той е много не ефективен.

До скоро начинът за предоставяне на мултикаст през MPLS мрежа беше ISP-то ръчно да изгражда тунели за всяка двойка източник-получател. Това решение изисква голяма административна поддръжка от страна на ISP-то<sup>[1]</sup>.

Росен MVPN е имплементация на мултикаст услуги за предаване на пакети през MPLS\BGP VPN-и.

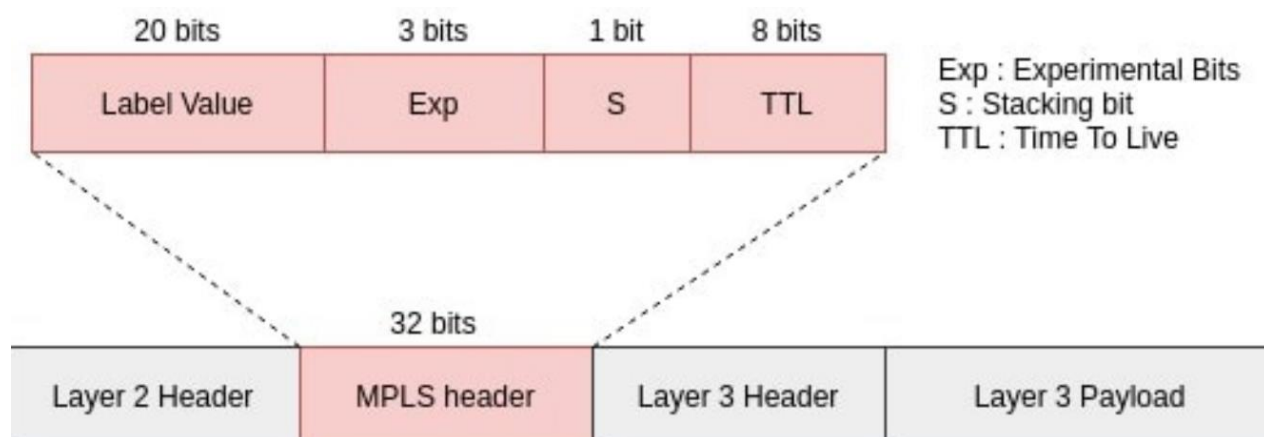
Росен MVPN предава мултикаст пакети и съобщения за сигнализация на PIM инстанции от едната до другата страна на VPN тунела. PIM протоколът във публичната (физическа) мрежа, още наречен R-PIM, не се налага да знае какви съобщения се предават от PIM протокола работещ върху виртуалните мрежи. Това още се нарича C-PIM. Затова при Rosen MVPN C-PIM протокола работещ върху виртуалната мрежа и R-PIM,вървящ върху публичната мрежа са напълно изолирани един от друг и могат да се третираят като самостоятелни логически единици<sup>[2]</sup>.

# Теоретична част

## 1 MPLS L3VPN

MultiPath Label Switching (MPLS) е подход за комутиране на IP дейтаграми използвайки предефинирани етикети, вместо IP адреси. MPLS на теория е независим от протокола чиито пакети пренася, но практически тази технология е най-разпространена в IP базираните мрежи. Това е така защото MPLS предоставя начин за постигане на резервираност и намалява времето за обработка на пакетите в рутера и изборът на път за маршрутизиране.

Когато един пакет постъпи във MPLS мрежа, преди хедъра на IP диаграмата се поставя кратък етикет който съдържа 20 битово число. В всеки от следващите маршрутизатори стойността в този етикет се поглежда в таблица (MPLS маршрутизираща таблица) която диктува от кой изход да се пусне пакета и каква нова стойност на етиката да се постави. Когато пакетът стигне до краен маршрутизатор в мрежата който трябва да го предаде към IP мрежа този етикет се премахва<sup>[3]</sup>.



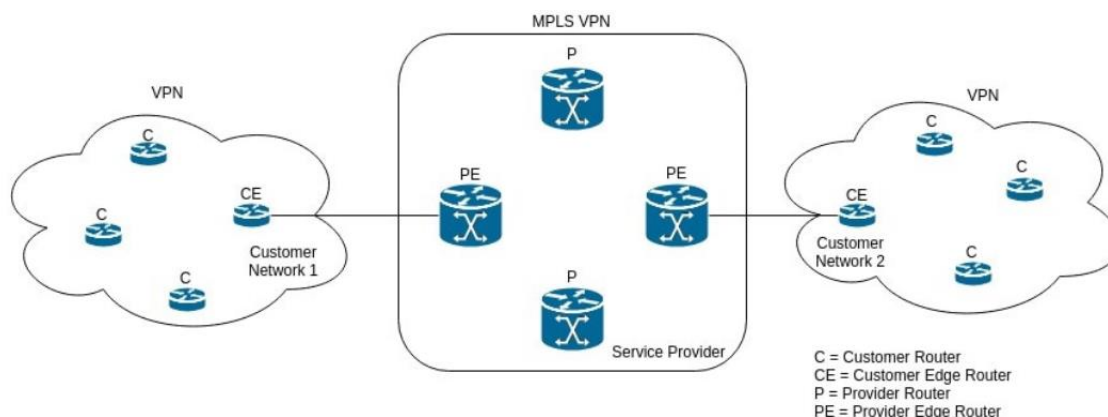
Фиг. 1

В MPLS мрежа маршрутизаторите може да се разграничат на два типа:

- Label Edge Router (LER) – тези маршрутизатори се намират на границата на MPLS/IP мрежите и могат да работят както със MPLS така и с IP пакети. Тези маршрутизатори подготвят пакета когато той влиза във MPLS или IP мрежа. Поради това те поддържат и IP маршрутизираща таблица и могат да изпълняват IP маршрутизиращи протоколи.
- Label Switching Router (LSR) – по дефиниция тези маршрутизатори не разбират от IP протокола, а само от MPLS етикети.

MPLS маршрутизираща таблица се съставя с помощта на протокола Label Distribution Protocol (LDP). В практиката този протокол се използва съвместно с някой Interior Gateway Protocol (IGP). Това е така понеже, повечето производители предлагат MPLS функционалности като софтуерно решение върху стандартните си IP маршрутизатори. Когато избраният IGP протокол постигне сходимост и всички пътища в мрежата са известни, вътрешни процеси в маршрутизатора използват откритите пътища от избрания IGP протокол за да съставят MPLS маршрутизиращи таблици<sup>[4]</sup>.

Реализацията на виртуална частна мрежа (VPN) върху MPLS базирана мрежа е най-разпространеното приложение на MPLS технологията.



Фиг. 2

Конфигурацията показана на Фиг. 2 е стандартна за MPLS VPN имплементациите. Състои се от гранични маршрутизатори на доставчика (Provider Edge routers PEs), маршрутизатори на доставчика (Provider routers Ps), гранични маршрутизатори на клиента (Customer Edge routers CEs) и маршрутизатори на клиента (Customer routers Cs). Като граничните маршрутизатори на доставчика и клиента са свързани на мрежово ниво. Маршрутизаторите в мрежата на доставчика предоставят MPLS VPN като услуга. Те са настроени да предават и приемат и маршрутизират пакети със MPLS етикети.

Когато клиентският граничен маршрутизатор изпрати пакет към входа на мрежата на доставчика, граничен маршрутизатор на доставчика добавя следните етикети:

- VPN етикет – с този етикет граничният рутер на доставчика, който ще има за цел да предаде пакета към мрежата на клиента от другата страна, ще знае този пакет на кой клиент принадлежи [5]
- MPLS етикет – чрез този етикет се осъществява маршрутизацията в MPLS мрежата на доставчика

MPLS етикетът стои преди VPN етикетът.

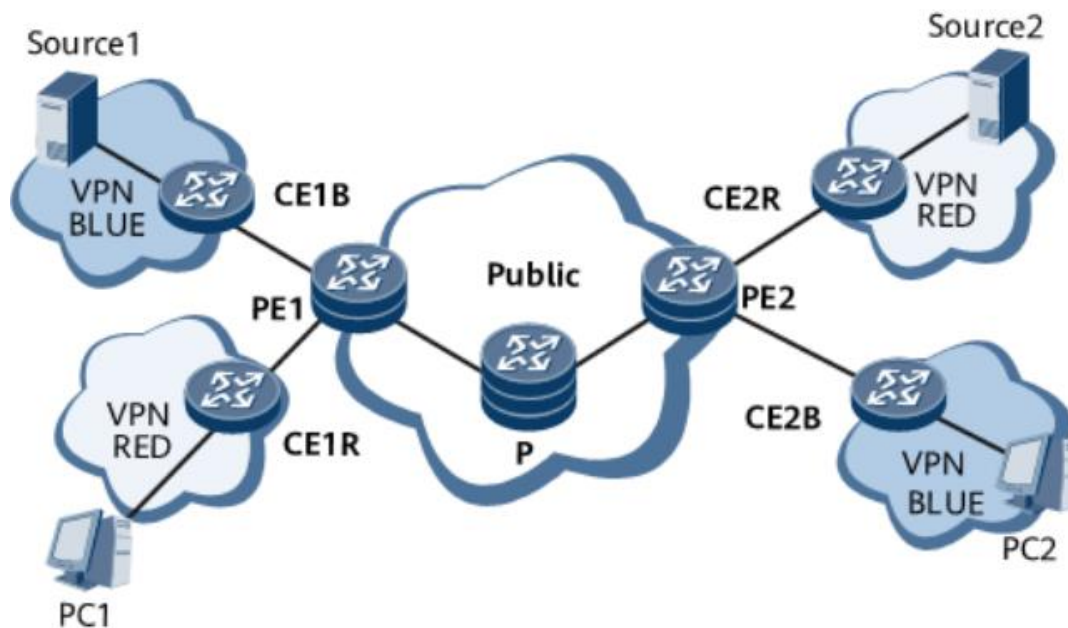
Конфигурацията на MPLS VPN мрежа представена на Фиг. 2, може да се използва за рекламиране на маршрути през 2-те физически мрежи на клиента с помощта на BGP (Border Gateway Protocol). MPLS пренася служебните пакети на BGP и му предоставя възможността да се обменя служебна информация между граничните маршрутизатори на клиента. Това е възможно понеже граничните маршрутизатори на доставчика използват MP-BGP (multi-protocol border gateway protocol) за да предават клиентските маршрути през мрежата на доставчика. Това прави работата на BGP много по ефективна във виртуализираната среда.

## **2 Rosen MVPN**

Основни дефиниции:

- Мултикаст домейн MD (multicast domain) – представлява група от VPN инстанции, изпълняващи се върху PE маршрутизаторите, които могат да предават и получават мултикаст пакети. Една VPN инстанция може да принадлежи само към една група.
- Обща-група – това мултикаст група към която всички VPN инстанции от един мултикаст домейн (MD) се присъединяват.
- Интерфейс на мултикаст тунела MTI (Multicast Tunnel Interface) – представлява входната или изходната точка на мултикаст тунел. Използват се за пренасяне на VPN енкапсулирани пакети през публичната мрежа.





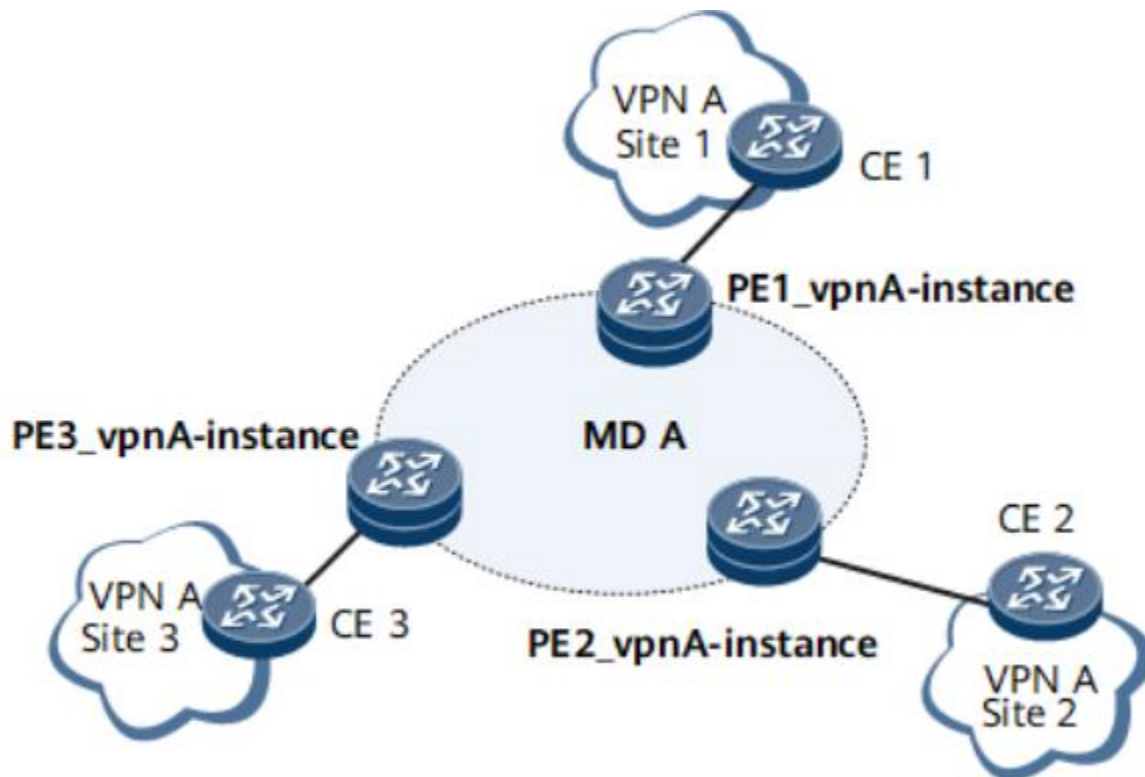
Фиг. 3

Целта на MVPN (multicast VPN) е да предостави възможността да се предават multicast пакети между VPN инстанциите. На Фиг. 3 може да се види конфигурацията на една MVPN услуга. Като всяка клиентска мрежа която физически се свързва със мрежата на доставчика се нарича VPN инстанция. VPN инстанциите представляват виртуализация на граничните маршрутизатори на доставчика, като всяка виртуална инстанция VPN обслужва точно една клиентска мрежа. Когато в мрежата на клиента работи инстанция на протокола PIM който общува с VPN инстанцията във граничния маршрутизатор на доставчика то тази PIM инстанция се нарича C-PIM (Customer PIM). Когато PIM инстанция върви между PE и P маршрутизаторите това се разглежда като PIM инстанция на доставчика или P-PIM (Provider PIM). Между всеки две C-PIM инстанции на даден клиент се изгражда мултикаст тунел или MT (Multicast Tunnel), като всяка C-PIM инстанция използва свой собствен интерфейс за комуникация с тунела или MTI (Multicast Tunnel Interface) с който се свързва с мултикаст тунела. Когато през мултикаст тунела

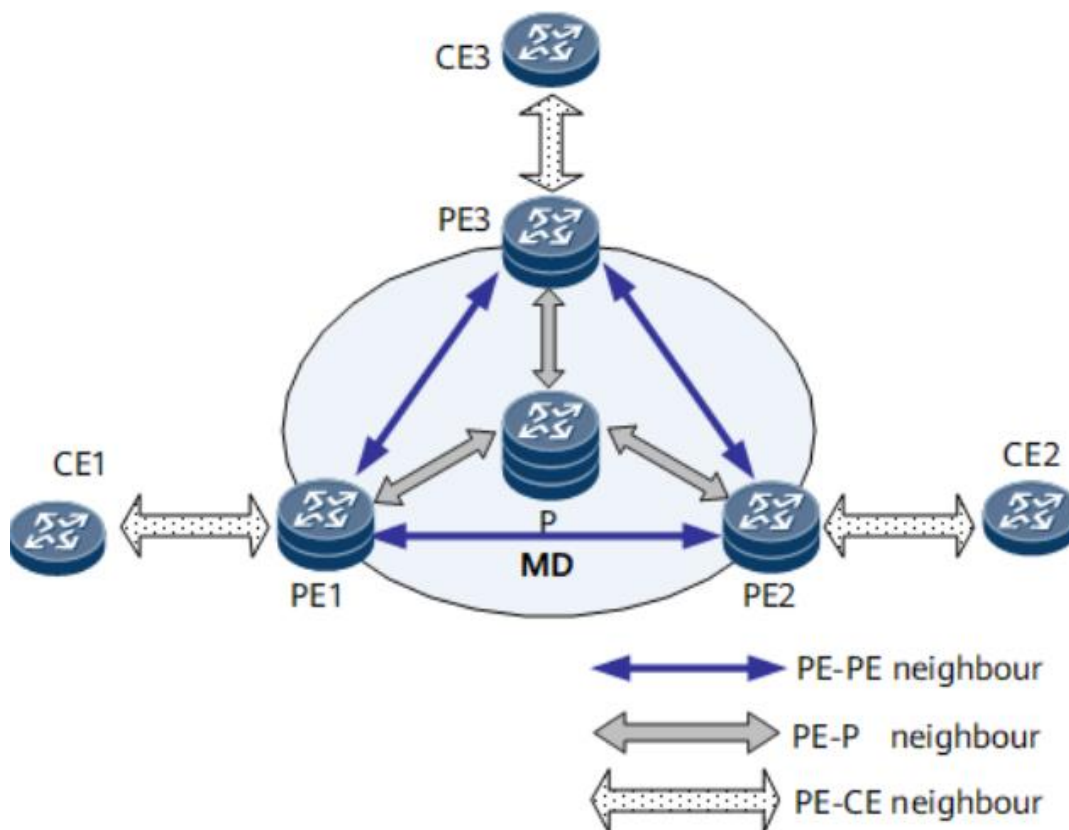
се свържат две C-PIM инстанции те комуникират на канално ниво, което им позволява да провеждат избори, да изпращат Join/Prune съобщения, както и да предават мултикаст пакети [6]

C-PIM инстанциите изпращат контролни или информационни мултикаст пакети към MTP интерфейса където те се енкапсулират и се предават по P-PIM инстанциите на доставчика. По този начин, чрез мултикаст тунелите те реализира MDT (Multicast Distribution Tree) през публичната мрежа на доставчика [6].

PIM съседство се изгражда между две или повече директно свързани мултикаст устройства в общ сегмент от мрежата.



Фиг. 4



Фиг. 5

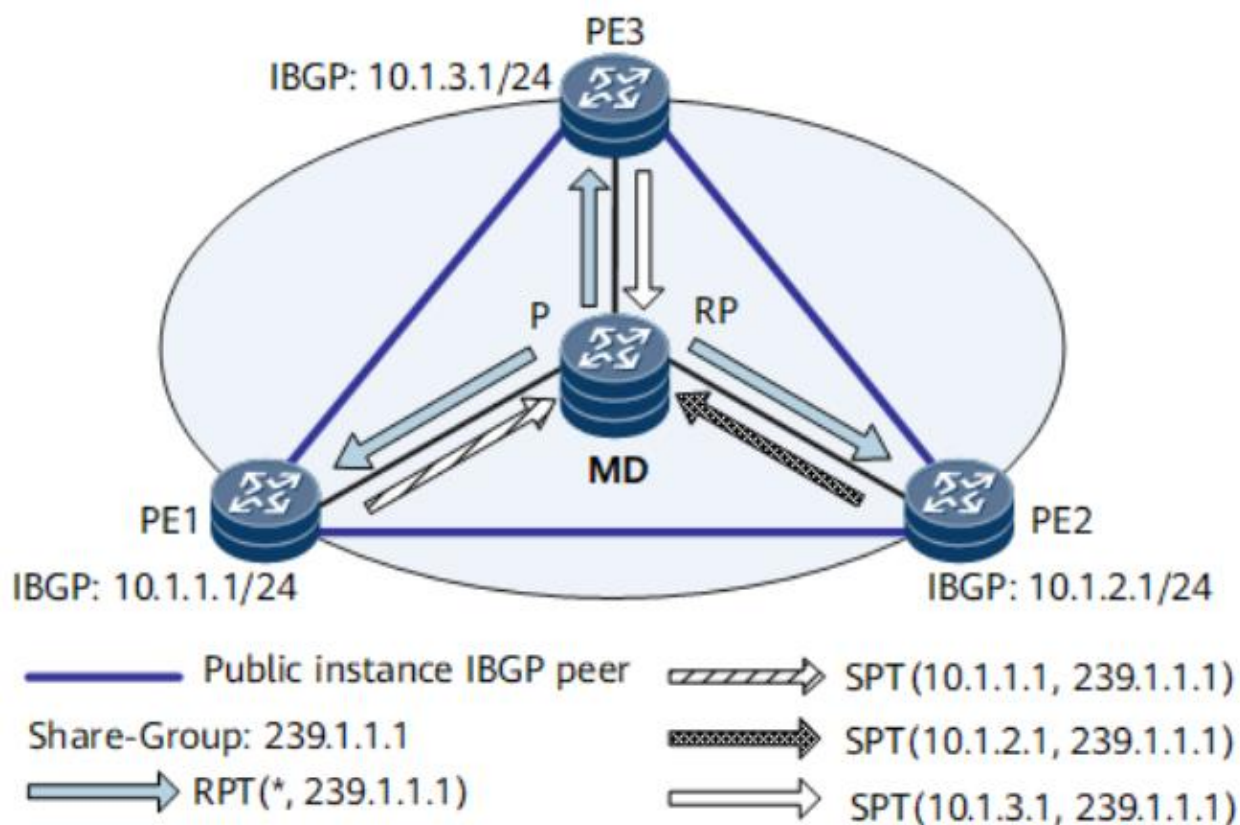
Съседствата между различните маршрутизатори може да се видят на Фиг. 5.

Идеята при Rosen MVPN е да се изгради едно общо мултикаст разпределено дърво share-MDT (shared Multicast Distribution Tree) чрез който да се предават мултикаст пакети и PIM служебни пакети, между всички VPN инстанции за един клиент. За целта на всяко изградено share-MDT дърво се назначава служебен мултикаст адреса общата-група. Тук използваният вариант на PIM протокола е PIM-SM (Sparse Mode PIM).

Изграждането на share-MDT става на два етапа и може да се види на Фиг. 6. При първият етап PE1 изпраща на рандеву точката или RP (Rendezvous Point). Съобщение за присъединяване (Join) към общата група, която в примера използва 239.1.1.1 адрес. Тази операция се повтаря и за PE2 и PE3 понеже и

към тях е свързана мрежа на клиента. Така се изгражда (\*, 239.1.1.1) връзка между RP което е корена и PE1, PE2, PE3 които са листата.

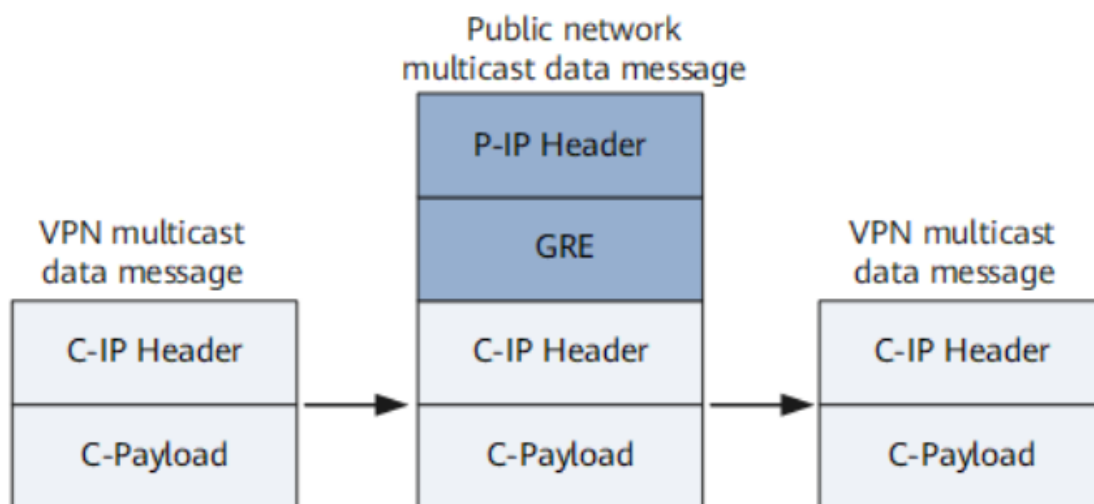
Във вторият етап от изграждането на share-MDT, PE1, PE2, PE3 изпращат Register съобщения които имат адреса на MTI интерфейса за източник и адресът на общата група. RP получава тези съобщения и създава (10.1.1.1, 239.1.1.1), (10.1.2.1, 239.1.1.1), (10.1.3.1, 239.1.1.1) записи.



Фиг. 6

След изграждането на share-MDT, VPN инстанциите могат да обменят мултикаст пакети. Това става по следният начин. VPN инстанцията, излияваща се на някой граничен маршрутизатор на доставчика PE, изпраща мултикаст съобщението към мултикаст тунелиращият интерфейс. Там пакетът се пакетира в мултикаст пакет, този път за P-PIM инстанцията. В резултат на

което IP адресът на източника става IP адресът на тунелиращия интерфейс, а мултикаст IP адресът за дестинацията се сменя със IP адресът на общата-група. Това се прави както за информационните пакети така и за съобщенията за сигнализация. След това пакетът се предава, през публичната мрежа към всички VPN инстанции които са част от общата група. Те от своя страна разпакетират тунелирания пакет и го изпращат към PIM инстанцията на клиента.



Фиг. 7

Форматът на тунелирания и не-тунелирания пакет е показан на Фиг. 7. И се състои от следните етикети:

- C-Payload – това е информацията която носи мултикаст пакета в C-PIM инстанцията. Тук тялото може да носи и служебна PIM информация.
- C-IP header – представлява етикетът на мултикаст пакета и се използва за мултикаст маршрутизиране в клиентската мрежа.
- GRE – GRE етикет за тунелиране.
- P-IP етикет – представлява етикетът на мултикаст пакета и се използва за мултикаст маршрутизиране в мрежата на доставчика. Източникът тук е MTI интерфейса, а получателя, общата група.

## Използвани източници

- [1 Cisco, "Multicast VPN Data Sheet," [Online]. Available:  
] [https://www.cisco.com/en/US/technologies/tk648/tk828/tk363/technologies\\_white\\_paper0900aecd802aea84.html](https://www.cisco.com/en/US/technologies/tk648/tk828/tk363/technologies_white_paper0900aecd802aea84.html).
  
- [2 Huawei, "Overview of Rosen MVPN," [Online]. Available:  
] <https://support.huawei.com/enterprise/en/doc/EDOC1000173015/e0de8568/overview-of-rosen-mvpn>.
  
- [3 S. A. N, "Introduction to MPLS and MPLS VPN technology," [Online]. Available:  
] <https://www.juniper.net/documentation/us/en/software/junos/is-is/topics/concept/ldp-igp-synchronization.html>.
  
- [4 "Understanding LDP-IGP Synchronization," [Online]. Available:  
] <https://www.juniper.net/documentation/us/en/software/junos/is-is/topics/concept/ldp-igp-synchronization.html>.
  
- [5 "BGP/MPLS IP VPN Label Distribution Modes," [Online]. Available:  
] <https://support.huawei.com/enterprise/en/doc/EDOC1100058940/ac98750c/bgp-mpls-ip-vpn-label-distribution-modes>.
  
- [6 Huawei, "Understanding Rosen MVPN," [Online]. Available:  
] [https://support.huawei.com/enterprise/en/doc/EDOC1000173015/cb0fb98c/understanding-rosen-mvpn#EN-US\\_CONCEPT\\_0172354859](https://support.huawei.com/enterprise/en/doc/EDOC1000173015/cb0fb98c/understanding-rosen-mvpn#EN-US_CONCEPT_0172354859).

