

МРЕЖИ С ДЕТЕРМИНИРАНИ ПАРАМЕТРИ С ИЗПОЛЗВАНЕ НА МАРШРУТИЗИРАНЕ НА СЕГМЕНТИ

Цветелина Симеонова

DETERMINISTIC NETWORKS USING SEGMENT ROUTING

Tsvetelina Simeonova

Резюме: Цел на работата е да се направи анализ на новото направление в телекомуникациите - създаване на детерминирани мрежи с използване на технологията маршрутизиране на сегменти в рамките на IPv6. Получените резултати обхващат разглеждането на мрежовите функции при детерминирана IP мрежа (DIP), нейната архитектура и принцип на функциониране. Дадени са различните аспекти на технологията маршрутизиране на сегменти (SR), както и множеството случаи на използване, вкл. инженеринг на трафика, възстановяване на мрежата при повреда, верижно свързване на услуги "без информация за състояние", въвеждане на "срезове" в 5G мрежа, комутация между домейни за свързване на потребители към приложения на сървъри в множество центрове за данни, маршрутизиране на сегменти в SD-WAN. Разгледани са основните технологии на DIP мрежа: оформяне (изглаждане) на трафичния поток, планиране на входа, планиране на интервали за разпределяне на времето.

Приносните моменти са свързани с анализ и изводи за приложимостта, обхвата и развитието на DIP мрежите с използване на технологията маршрутизиране на сегменти в рамките на IPv6.

Ключови думи: детерминирана IP мрежа, маршрутизиране на сегменти, SRv6.

Abstract: The aim of the work is to analyze the new direction in telecommunications - creation of deterministic networks using segment routing technology within IPv6. The results obtained cover the consideration of network functions in a deterministic IP network (DIP), its architecture and principle of operation. The various aspects of segment routing (SR) technology are given, as well as the many use cases, incl. traffic engineering, network failure recovery, stateless chaining of services, introduction of 5G network "slices", cross-domain switching to connect users to applications on servers in multiple data centers, segment routing in SD-WAN. The main technologies of a DIP network are considered: traffic flow shaping (smoothing), input scheduling, time slot scheduling.

The contributions relate to analysis and conclusions on the applicability, scope and development of DIP networks using segment routing technology within IPv6.

Key words: deterministic IP networking, segment routing, SRv6.

1. Необходимост и специфика на мрежовите функции при детерминирана IP мрежа (DIP)

Традиционните IP мрежи предоставят услуги с маршрутизация "най-добър опит" (best-effort). При обслужването се извършва просто статистическо мултиплексиране, което отговаря основно на изискванията за качество на услуги, като видео, сърфиране в мрежата и имейл [1, 2, 3].

Появяващите се нови услуги - като L2VPN, L3VPN, частна наета линия и видеонаблюдение - поставят по-високи изисквания към качеството на мрежовата услуга. Въпреки, че в мрежите могат да се използват технологии като RSVP-TE ((Resource Reservation Protocol-Traffic Engineering)) и DiffServ, за да се осигури приблизителна гаранция за честотна лента, качеството на услугата се влошава значително, когато възникват претоварвания (микросерии, microbursts).

С появата на нови приложения - като индустриален интернет на нещата IoT (Internet of Things), тактилен интернет TI (Tactile Internet), автономно шофиране, интернет на

превозните средства IoV (Internet of Vehicles) и контрол/диагностика в реално време - от мрежите се изисква да предоставят услуги своевременно и по точен начин (детерминирано).

Традиционните IP мрежи не са в състояние да се справят с такива диференцирани и високи изисквания обвързани със споразумения за обслужване SLA. За да се реши този проблем и да се осигури детерминирано забавяне и джитер, се въвеждат мрежи с детерминирани параметри DIP (Deterministic IP networking). Детерминираната IP мрежа осигурява гаранция в IP мрежите да се пренасят услуги с детерминирано забавяне и джитер при пренасочване на пакети "от край до край" (E2E) в IP мрежа, като ефективно отговаря на изискванията за детерминираност при транспорта на новите услуги.

DIP мрежа, базирана на SRv6, използва технологии като: оформяне на трафичния поток в периферията (edge shaping); планиране на вход (gate scheduling); планиране на интервали за разпределяне на времето (interval mapping).

2. Архитектура на DIP мрежа

Архитектурата на DIP мрежата включва:

- оформяне (изглаждане) в периферията (edge shaping),
- планиране на вход (gate scheduling)
- планиране на интервали (разпределяне на времето) (interval mapping).
- транспортна мрежа базирана на SRv6 (SRv6 transport network)

2.1. Режими при предоставяне на услуги в DIP мрежа

Услугите в DIP мрежа могат да се поддържат, например, в следните режими: EVPN VPLS (Ethernet VPN Virtual Private LAN Service) през SRv6 TE Policy; EVPN VPWS (Virtual Private Wire Service) през SRv6 TE Policy. Определени са и механизми за обратна съвместимост на решенията: EVPN (Ethernet VPN) и PBB-EVPN (Ethernet VPN) на Provider Backbone Bridge с VPLS (Virtual Private LAN Service); PBB-VPLS (Provider Backbone Bridge VPLS) [4].

Предоставят се и механизми за интегриране на тези две технологии в една и съща MPLS/IP мрежа на базата на VPN реализация. Това позволява на доставчиците на услуги да въведат EVPN/PBB-EVPN Provider Edges (PE) в своите внедрявания на VPLS/PBB-VPLS мрежи. Необходимо е автоматично откриване на: екземпляр на VPN; едноадресна или многоадресна (мултикаст) операция; операция за мобилност за управление на достъпа до медията (MAC). Това се определя в управляващата равнина. В резултат има интеграция между EVPN и VPLS PE, както и между PBB-VPLS и PBB-EVPN PE.

Технологията "виртуална частна кабелна услуга" EVPN-VPWS [5] е решение базирано на протокол BGP за управляваща равнина за услуги "от точка до точка". Прилага сигнализация и капсулиране за установяване на EVPN екземпляр между двойка PE. Има способността да пренасочва трафик от една мрежа към друга без MAC търсене. Използването на EVPN за VPWS елиминира необходимостта от сигнализация на едносегментни и многосегментни PW (pseudowire) за Ethernet услуги "от точка до точка". Технологията EVPN-VPWS работи върху IP и MPLS ядро; IPcore за поддръжка на BGP и MPLS ядро за прехвърляне на пакети между крайните точки.

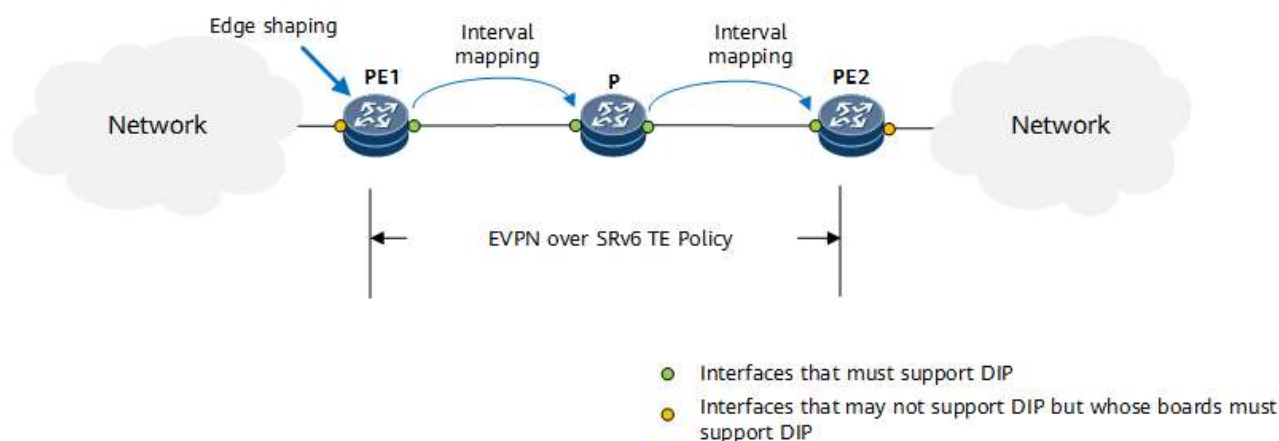
2.2. Принцип на функциониране на DIP мрежа

За да може да се използва EVPN, базирана на SRv6 TE политика, с цел определяне на пътищата за пренасочване на пакети, във всеки възел се внедряват DIP-съвместими платки (boards) и интерфейси. Всеки възел използва периодично запитване за планиране на пренасочването на пакетите с използване на механизъм за планиране на входа (фиг. 1).

Входящото устройство PE1 (в периферията на доставчика, Provider Edges) изпълнява оформяне (изглаждане) на трафика на получените пакети и след това периодично изпраща

изгладения трафичен поток пакети (чрез механизма за планиране на входа) към следващото устройство на доставчика P.

Устройството P изчислява интервала за изпращане на пакети въз основа на правилото за съответствие на интервалите и изпраща пакетите към изходящото устройство PE2 в рамките на планирането на интервалите (interval mapping). След това PE2 препраща пакетите както обикновено. Интерфейсите, които са в рамките на EVPN трябва да поддържат DIP, а "външните" интерфейси може да не поддържат DIP, тъй като внедрените DIP-съвместими платки поддържат DIP.



Фиг. 1. Архитектура на DIP мрежи (източник: [1])

3. Маршрутизиране на сегменти SR (Segment routing)

Технологията "маршрутизиране на сегменти" SR (Segment routing) значително опростява управляващата равнина в IP мрежите. Това е за сметка на преместването на информацията за състоянието от мрежата в заглавието на пакета и осигуряване на транспортна архитектура "от край до край", която обхваща множество мрежови домейни.[6]

„Маршрутизиране на сегменти“ (Segment routing) и „маршрутизиране от източника“ (source routing) са два термина, които описват техника на маршрутизиране, при която маршрутизаторът-източник (или "входящ") определя маршрута, който пакетът ще следва през мрежата, вместо пътят да бъде избран само въз основа на дестинацията на пакета.

Основните цели на разработката на SR са свързани с реализацията и простотата на работа при инженеринг на трафика, като основно разграничение от наследените протоколи за инженеринг на трафика (RSVP-TE¹, LDP² и MPLS-TP³).

Например, при RSVP-TE се изисква рутерите в мрежата да съхраняват информация за състоянието на всеки път (per-path state information), а SR изисква състояние само в изходния (source (ingress)) рутер. Премахването на изискването за поддържане на състояние в цялата мрежа води до възможността за увеличена мащабируемост на мрежата и гъвкавост на услугите. Свързването на SR с централизирано софтуерно дефинирано управление на мрежата SDN (Software-Defined Networking) допълнително опростява някои приложения на SR.

Технологията SR е предназначена да работи с всички равнини за IP пренасочване (all IP forwarding planes), като независимо от равнината на пренасочване наборът от функции на

¹ RSVP-TE: Resource Reservation Protocol - Traffic Engineering

² LDP: Label Distribution Protocol

³ MPLS-TP: Multiprotocol Label Switching - Transport Profile

SR е същият при различните SR стандарти. Стандартите за маршрутизиране на сегменти, поддържащи различните IP равнини на пренасочване, са както следва: SR-MPLS (IPv4, MPLS, IPv6 (SRv6)), SRv6 (IPv6), SRm6 (IPv6).

3.1. Функциониране на маршрутизирането на сегменти

Когато пакет пристигне във входен възел поддържащ SR, той се обработва в съответствие с определена политика. Ако пакетът отговаря на условията за съвпадение за път, базиран на SR, входният възел на SR капсулира пакета в SR тунел, който преминава през SR пътя, сегмент по сегмент [7].

Всеки сегмент в път на SR завършва във възел на крайна точка на сегмент. Когато пакет пристигне в крайна точка на сегмент, крайната точка проверява най-външния етикет, след това го изтрива и препраща пакета към следващата крайна точка. Този процес продължава, докато пакетът пристигне в крайна точка, която може да бъде изходен възел на SR. Когато пакет пристигне в изходен възел на SR, този възел определя дали пакетът е в края на своя път. Ако е така, възелът премахва информацията за заглавие на SR и препраща пакета въз основа на IP адреса на местоназначението.

Тъй като транзитните маршрутизатори просто препращат пакетите въз основа на идентификатора на сегмента SR, SID (Segment Identifier), SR може да се използва и за съответно пренасочване на пакети, свързани с краен потребител или приложение, към специфични мрежови функционални услуги.

Това се прави, като се определя път до точката, където услугата ще бъде приложена, и се предоставят инструкции за услугата, както и допълнителна информация за пътя на услугата от входния до изходния рутер (шлюз) на SR домейна (SR domain egress router).

3.2. Предимства при използване на маршрутизирането на сегменти в IP мрежа

- Основно предимство при използване на SR е възможността да се опрости мрежата и да се намали използването на ресурси, което улеснява управлението и мениджмънта на мрежата.

- Използването на инженеринг на трафика при SR осигурява QoS на приложенията, както и съответствието на мрежовите услуги към крайните потребители и приложения.

- SR осигурява устойчивост в мрежата относно надеждността (безотказността) на пътя в случай на прекъсване на мрежата чрез възстановяване на "главния край" (headend), с помощта на алгоритъм "алтернативен път без цикли независимо от топологията" TI-LFA (Topology-Independent Loop-Free Alternate) и механизъм за бързо пренасочване FRR (Fast Re-routing)

- Когато се използва с WAN PCE⁴ контролер, SR предлага допълнителни предимства. При SR се осигурява резервиране на честотна лента с опростен инженеринг на трафика, тъй като контролерът има способността да присвоява атрибути на връзката и ограничения на пътя и да извършва изчисления на пътя въз основа на ограничения протокол "първо най-краткия път" CSPF (Constrained Shortest Path First).

- При SR се подобрява качеството на изживяване на крайния потребител, като се дефинират специфични мрежови пътища според определени изисквания (това се използва и за създаване на мрежови "срезове" (network slicing)). "Срез" (slice) се нарича специфичната конкретна логическа топология и свързаните с нея ресурси, отнесени към определен конкретен сценарий на дадено приложение.

- При SR се улеснява автоматизацията на обслужването на мрежата чрез непрекъснато оценяване на мрежовите условия в реално време.

⁴ PCE (Path Computation Element) - елемент за изчисляване на пътя.

3.3. Инженеринг на трафика с контролери за маршрутизиране на сегменти

- SR контролерът е тип SDN контролер, който осигурява централизирано изчисляване на пътя, инженеринг на трафика и детайлна видимост и контрол на потока на трафика за равнини за пренасочване на SR в мрежи на доставчик на услуги и предприятия.
- Контролерът SR позволява на мрежовите оператори да оптимизират своята мрежова инфраструктура чрез проактивен мониторинг и планиране и чрез динамично маршрутизиране на големи трафични натоварвания въз основа на определени ограничения.
- Чрез преместване на информацията за състоянието на пътя, от транзитни рутери в пакета, маршрутизирането на сегменти елиминира необходимостта от протоколи като LDP (Label Distribution Protocol) и RSVP-TE, които разпределят информация за пътя в мрежата. SR контролерите решават този проблем, защото могат да наблюдават цялата топология на мрежата и предаваните трафични потоци в реално време.
- Контролерът SR изпълнява три основни операции: анализиране, оптимизиране, автоматизиране.

3.4. Настоящи и перспективни направления за случаи на употреба на SR

3.4.1. Трафик Инженеринг/Насочване на трафика (Traffic Engineering/Traffic Steering)

Доставчиците на услуги традиционно са използвали RSVP-TE за инженеринг на трафика, но RSVP-TE може да бъде тромав и сложен за изпълнение. Също така, докато някои оператори са внедрили широко RSVP-TE в своите мрежи, други не са го направили. SR предлага алтернатива на RSVP-TE при инженеринг на трафика, както и при насочване на трафика. Например, доставчиците на услуги внедряват SR за приложения, при които RSVP-TE се оказва твърде сложен. Важно за доставчици на услуги, които имат RSVP-TE мрежи, е използването на централизиран контролер, което позволява съвместното съществуване на RSVP-TE и SR, и плавна еволюция от RSVP-TE към SR.

3.4.2. Възстановяване на мрежата при повреда (възстановяване на "главния край" и използване на алгоритъм TI-LFA)

Възстановяването на "главния край" (Headend) осигурява възстановяване "от край до край" при повреда в даден път, който пренася трафика на TE тунела. Това възстановяване се постига чрез конфигуриране в "главния край" на два пътя за свързване от входен към изходен възли на SR. Единият път осигурява основна, а другият резервна свързаност. Когато входният възел на SR открие повреда на основния път, той изпраща трафика към резервния път.

За да се осигури мрежово покритие за 100% от сценариите при повреда на връзка (link) или възел, при SR се използва алгоритъм за дефиниране на "алтернативен път без цикли независимо от топологията" TI-LFA (Topology Independent – Loop-Free Alternates). TI-LFA използва механизъм за бързо пренасочване FRR (fast-reroute).

3.4.3. Верижно свързване на услуги "без състояние на мрежата" (Stateless Service Function Chaining)

Верижното свързване на услуги (Service chaining) описва свързването на множество виртуални мрежови функции при предоставяне на конкретна услуга на краен клиент. Например, даден оператор може да достави услуга, включваща верига от балансатор на натоварването (load balancer), защитна стена (firewall) и прокси (proxy). Това е важна

концепция при виртуализацията на мрежовите функции NFV (Network Functions Virtualization).

Перспективни случаи на употреба. Тъй като SR придобива все по-голямо разпространение в рамките на доставчиците на услуги и тъй като съществуващите предизвикателства намаляват, има нови случаи на употреба.

3.4.4. Въвеждане на "срезове" в 5G мрежа (5G Network Slicing)

Въвеждането на "срезове" в мрежата "от край до край" ще бъде от решаващо значение за операторите при предлагането на пълния спектър от случаи на използване на 5G, включително комбинация от заложените в 5G мрежови услуги [8, 9]:

- ултранадеждни комуникации с ниска латентност URLLC (Ultra-Reliable Low Latency Communications);
- масови комуникации машинен тип mMTC (Massive Machine-Type Communications);
- подобрена мобилна широколентова връзка eMBB (Enhanced Mobile Broadband).

Със спецификациите за производителност, радикално различни в целия спектър от потенциални случаи на използване на 5G, една мрежа не може да се справи с всички. В същото време обаче поддържането на напълно отделни мрежи за различни случаи на употреба няма как да бъде рентабилно.

Въвеждането на срезове в мрежата позволява на операторите да разделят услугите така, че споразуменията SLA и основните ключови показатели за ефективност KPIs (Key Performance Indicators) – като латентност, пропускателна способност и надеждност – да могат да бъдат осигурени в рамките на различни „срезове“ (slices), работещи в рамките на обща мрежова инфраструктура [10].

Изследванията от литературата [6] показват, че първоначалните внедрявания на 5G са фокусирани основно върху услуги за по-високите широколентови скорости (като eMBB), за които се очаква, че няма да изискват множество мрежови сегменти.

Когато случаите на използване на услуги, базирани на URLLC и mMTC, се увеличат, със сигурност ще бъде необходима поддръжката за въвеждане на "срезове" "от край до край", за което ще е необходима стандартизирана координация между транспортната мрежа и мрежата за радио достъп RAN (Radio Access Network).

3.4.5. Комутация между домейни за свързване на потребители към приложения на сървъри в множество центрове за данни

Първоначалното използване на SR е вътрешнодомейново, като SR насочва трафика през определен брой рутери, всички в рамките на един и същ домейн. Ако доставчикът на услуги използва централизиран контролер, този контролер действа само на рутерите, които се намират в рамките на домейна. Така мрежите с маршрутизиране на сегменти съществуват като отделни острови между доставчиците на услуги или дори в рамките на техните мрежи (в случаите, когато има множество домейни).

Реален пример е свързаността на центъра за данни. За да насочват трафика в своите центрове за данни, доставчиците на услуги използват SR-MPLS. Транспортът на трафика от даден център за данни до целевия център за данни обикновено се извършва през основната мрежа (гръбнака) на MPLS. Целевият център за данни може да използва SR в рамките на собствения си домейн.

В тази връзка, SR предоставя предимства за управление на трафика в центъра за данни или в рамките на домейн, но е необходим някакъв вид кръстосано свързване на домейни, за да се насочва трафикът "от край до край" от един домейн към друг, каквато универсална технология понастоящем не съществува.

3.4.6. Маршрутизиране на сегменти в SD-WAN

Софтуерно дефинираната широкообхватна мрежа SD-WAN (Software-Defined Wide-Area Network) се очертава като перспективна опция за свързване за корпоративни облачни приложения с бъдещо силно развитие. Въпреки че някои компании позиционират SR и SD-WAN като конкурентни технологии, в литературата те се разглеждат като допълващи се иновации [6]. Когато се комбинират, тези технологии могат да осигурят значителна диференциация за операторските SD-WAN услуги.

Възможността за задаване на политики за всеки трафичен поток е един от най-важните аспекти на SR за случаи на използване в SD-WAN, като предоставя на доставчиците на услуги (и техните корпоративни клиенти) способността да координират между наслагването (SD-WAN) и основната мрежа (IP транспорт) по начин, който не е бил възможен.

Взаимодействието между SD-WAN и SR обикновено изисква контролер за SD-WAN, както и контролер за SR. Контролерът за SR може да се основава на:

- Протокол за изчисление на пътя PCEP (Path Computation Element Protocol). PCE (Path Computation Element) е устройство, което изчислява пътища за възлите в мрежата.
- Протокол за мрежова конфигурация NETCONF (Network Configuration Protocol) [11]. NETCONF е протокол за мениджмънт на мрежата, разработен и стандартизиран от IETF. NETCONF предоставя механизми за инсталиране, манипулиране и изтриване на конфигурацията на мрежови устройства. Неговите операции се реализират върху прост слой за извикване на отдалечена процедура RPC (Remote Procedure Call). Протоколът NETCONF използва базирано на XML (Extensible Markup Language) кодиране на данните за конфигурационните данни, както и за съобщенията на протокола. Съобщенията на протокола се обменят върху защитен транспортен протокол.

3.5. Предизвикателства при приемането на SR

Въпреки съществуващата приложимост, остават предизвикателства пред по-голямото приемане на SR. В литературата [6] се описват три класа предизвикателства, относно:

- миграция към SDN управление (Migration to SDN Control);
- поддръжка на IPv6 (IPv6 support);
- съвместимост (Compatibility with Installed Base).

3.6. Перспективи на маршрутизирането на сегменти

Технологията SR може значително да опрости мениджмънта на IP мрежите.

- Търсенето на доставчици на услуги за SR е силно и първоначалните внедрявания са фокусирани върху възможностите за възстановяване на мрежата независимо от топологията, насочване на трафика, инженеринг на трафика и др. В тази връзка има множество нововъзникващи възможности за използване, включително сложни приложения за инженеринг на трафика, SR за създаване на "срезове" в 5G мрежа, свързване между домейни, SR основна мрежа (SR underlay) в SD-WAN и др.

- От друга страна: някои приложения са ефективни в мрежи без контролер (като насочване на трафика (traffic steering)), много се възползват от централизирано управление, а някои изискват абсолютно централизиран мрежов изглед.

- При внедряването на IPv6 има два IETF стандарта (SRv6 и SRm6), като функциите са еднакви, независимо от използваната равнина на данни.

- SR-MPLS може да се справи с повечето настоящи и бъдещи случаи на употреба, стига мрежовото оборудване да поддържа MPLS.

3.7. Развитие на SR към SRv6

Интерес представлява използването на SR с IPv6 като равнина за транспорт/данни. SRv6 споделя много от същите характеристики, предимства и цели приложения на SR, разгърнати в MPLS равнина на данни (т.е. SR-MPLS), но добавя някои нови функции:

- **Повишена достъпност:** 128-битовото адресно пространство, поддържано от IPv6, осигурява достатъчно адреси за огромния растеж на устройствата, свързани в мрежата, очакван с нарастващото приемане на IoT приложения.
- **Опростена работа в мрежа:** При SRv6 се използват разширения на заглавието на IPv6 (IPv6 extension headers), като в IPv6 пакета директно се включват базирани на IPv6 идентификатори на сегменти SID (segment IDs).

Това означава, че отделни протоколи за тунелиране като L2TP, GRE (Generic Routing Encapsulation) и дори MPLS могат да бъдат елиминирани от мрежата, опростявайки цялостното мрежово функциониране и поддръжка.

SRv6 може да се използва като **единен обединяващ протокол** за предаване на пакети от дадено устройство до местоназначението, било то друго устройство или приложение в облака (с подходящия капацитет, латентност и надеждност).

- **Мрежова програмируемост:** При SRv6 може да се активира нова гама от мрежови приложения чрез концепция „мрежово програмиране“. Могат да бъдат създадени и използвани специални идентификатори на сегменти SID (segment IDs) за включване на информация за местоположение, за идентификатор на функция и за състояние.

След това SRv6 пакетът може да бъде пренасочен към мрежова функция, намираща се в конкретна VM или контейнер в център за данни, и да премине към данни специфични за това приложение (информация за състоянието), за да изпълни тази функция.

Това е много подобно на начина, по който променливите се предават на подпрограми в компютърното програмиране. При използване на този принцип мрежата всъщност се превръща в компютър. Мрежовото програмиране може да осигури елегантно решение на предизвикателството за осигуряване на свързаност към виртуализирани функции, намиращи се в центрове за данни по прост, мащабируем и сигурен начин.

4. Основни технологии на DIP мрежа

DIP мрежата се реализира на базата на синхронизация на генераторите (clock synchronization) между устройствата в мрежата. Рутерите поддържат синхронизация на генераторите с помощта на протокол PTP (Precision Time Protocol, timing-over-packet protocol) [12] и синхронни Ethernet технологии.

Основни технологии на DIP мрежите:

- оформяне (изглаждане) на трафичния поток в периферията (edge shaping),
- планиране на входа (gate scheduling),
- планиране на интервали за разпределяне на времето (interval mapping).

4.1. Оформяне (изглаждане) на трафичния поток в периферията (edge shaping)

Процесът на оформяне (изглаждане) на трафичния поток пакети в периферията оформя множеството пакети с неравномерни времена на пристигане, в поток от услуги във всеки период на планиране (scheduling period), определен във времева последователност на крайното периферно устройство, където трафикът на услугата влиза в мрежата. Това гарантира, че пакетите ще бъдат изпратени последователно въз основа на периода на планиране. Изглаждането на трафичния поток пакети се извършва само веднъж на входното устройство, а транзитните устройства не вземат участие в процеса.

За да се извърши изглаждане на трафичния поток пакети, рутерът използва метод "кофа за оформяне" (shaping bucket). Размерът на кофата може да бъде гъвкаво променян въз основа на действителния обем на трафика на услугата и хардуерните възможности.

Оформянето (изглаждането) на трафика в периферията елиминира зависимостта от стриктното време за постъпването на пакети.

4.2. Планиране на входа (gate scheduling)

При DDP, пакетните опашки могат да бъдат класифицирани като:

- **Опашка за управление на входа (Gate control queue):** Планирането на опашката се извършва на базата на фиксиран период и пакетите в опашката не се приоритизират.
- **Обща опашка (Common queue):** Не се извършва периодично планиране. Общата опашка винаги е активирана и планирането на QoS за пакети в опашката се извършва въз основа на приоритети.

Планирането на входа (Gate scheduling) е механизъм за планиране на списък (график), който управлява активирането и деактивирането на опашките за управление на входа (gate control queues) на базата на фиксиран интервал.

4.3. Планиране на интервали за разпределяне на времето

Планирането на интервали (Interval mapping) е на базата на фиксиран алгоритъм и се отнася за планирането на интервалите през които устройствата изпращат по веригата едни и същи пакети (upstream and downstream).

Преди пакетът да влезе в опашката за управление на входа (gate control queue), рутерът капсулира информацията за DDP заглавието в пакета. В равнината на пренасочване може да се въведе нов опционален IPv6 хедър НВН (Hop-by-Hop), който носи информацията на DDP заглавието. Фиг. 2 показва формата на заглавието на НВН опциите.

| Next Header | Hdr Ext Len | Option Type | Option Length |
|-------------|-------------|-------------|---------------|
| Flags | DipLabel | | |

Фиг. 2. Формат на опциите на заглавието при предаване "НВН", капсулираща информацията в заглавието при DDP (източник [1]). DipLabel показва интервала за изпращане на пакети на устройството.

5. Области и развитие на DDP мрежите

Работната група за детерминирани мрежи (DetNet [13]) се фокусира върху детерминирани пътища за данни, които работят върху сегменти, с мостово свързване на слой 2 и маршрутизирани на слой 3, при което такива пътища могат да осигурят граници на латентността, загубите и джитера (вариацията на закъснението) на пакетите, както и висока надеждност. Работната група се занимава с аспектите на ниво 3 за поддържане на приложения, изискващи детерминирана мрежа. Работната група си сътрудничи с IEEE802.1 TSN (Time-Sensitive Networking), който отговаря за операциите на слой 2, за да дефинира обща архитектура, както за слой 2, така и за слой 3.

Примерни приложения за детерминирани мрежи включват професионални и домашни аудио/видео, мултимедия в транспорта, системи за управление на двигатели и други общи промишлени и автомобилни приложения, които се разглеждат от работната група IEEE 802.1 TSN. Работната група се фокусира върху решения за мрежи, които са под единен административен контрол или в рамките на затворена група с общ административен контрол; те включват не само мрежи в целия кампус, но могат да включват и частни WAN. Работната група DetNet няма да разглежда решения за големи групи домейни като Интернет.

МРЕЖИ С ДЕТЕРМИНИРАНИ ПАРАМЕТРИ С ИЗПОЛЗВАНЕ НА МАРШРУТИЗИРАНЕ НА СЕГМЕНТИ
ЦВЕТЕЛИНА СИМЕОНОВА

Работната група е отговорна за цялостната архитектура на DetNet и специфичните за DetNet спецификации, които обхващат равнината на данни, Операции, администриране и поддръжка ОАМ (Operations, Administration, and Maintenance), синхронизация на времето, мениджмънт, управление и аспекти на сигурността, които са необходими за активиране на мулти-хоп път и препращане по пътя, с детерминирани свойства на контролирана латентност, ниска загуба на пакети, нисък джитер и висока надеждност.

Работата се прилага за потоци "от точка до точка" (unicast) и "от точка до много точки" (multicast), които могат да бъдат характеризирани по начин, който позволява на мрежата да резервира подходящите ресурси за потоците предварително и да освободи тези ресурси, когато вече не са необходими. Работата обхваща характеризирането на потоците, капсулирането на рамки, изискваното поведение при пренасочване, както и състоянието, което може да се наложи да се установи в междинните възли. Технологиите за равнина на данни от слой 3, които могат да се използват, включват: IP и MPLS и капсулации от слой 2, които работят през IP и/или MPLS, като псевдопроводници (pseudowires) и GRE.

Работната група документира кои среди за внедряване и видове топологии са в (или извън) обхвата на архитектурата DetNet. Работата се фокусира върху аспектите на равнината на данни и е независима от всеки протокол или механизъм за определяне на път. Документират се и подходите относно равнината на контролера (DetNet Controller Plane), които използват съществуващи IETF решения, като PCE (Path Computation Element). При това ще се определя работната група, отговорна за разширенията, необходими за поддръжка на DetNet.

Документите на работната група са съвместими с работата, извършена в IEEE802.1 TSN и други работни групи на IETF. Обхватът на работната група изключва модификации на транспортни протоколи, ОАМ, пренасочване на ниво 3 и капсулации, но може да включва изисквания за такива модификации, координирано със съответната работна група.

Дейностите по DIP (DetNet) включват следните области:

Обща архитектура: Общата архитектура обхваща равнината на данните, ОАМ, синхронизацията на времето, мениджмънта, управлението и аспектите на сигурността.

Равнина на данни: Документира се как да се използва IP и/или MPLS и свързаната ОАМ, за да се поддържа метод на равнина на данни за идентификация на потока и обработка на пакети през слой 3. Могат да се използват и други технологии за равнина на данни, дефинирани от IETF.

Равнина на контролера: Равнината на контролера (Controller Plane) е дефинирана в RFC 8655 като „обединяване на равнините за мениджмънт и управление“. Документира се как да се използват решения за управляваща равнина на IETF за поддръжка на DetNet, включително идентифициране на всякакви пропуски в съществуващите решения.

Модел на информация за потока от данни: Тази работа ще идентифицира информацията, необходима за установяване и управление на потока (flow establishment and control) и ще бъде използвана от протоколи за резервиране и от модели на данни YANG.

YANG модели: Представят се възможностите на устройството, връзката (поддръжка на функции) и ресурсите (напр. буфери, честотна лента) - за използване в конфигурацията на това устройство и отчитането на състоянието. Такава информация може също да се използва, когато се рекламират (обявяват) детерминирани мрежови елементи към управляващата равнина. Информацията, свързана с управляващата равнина, ще бъде независима от протокола/ите, който може да се използва за рекламиране на тази информация (напр. IS-IS или GMPLS разширения).

Вертикални изисквания (при необходимост): Уточняват се изискванията за детерминирани мрежи в различни индустрии, които преди това не са били документирани и не могат да бъдат поддръжани с помощта на дефинирани решения DetNet. Изследва се

дали съществуващите механизми за криптиране в равнината на данни могат да бъдат приложени за подобряване на сигурността и поверителността.

Работната група поддържа връзка с подходящи групи в IEEE и други организации за разработване на стандарти SDO (Standard Development Organisations).

6. Заключение

Има различни фактори, които определят развитието на технологичната концепция DIP мрежи. На база на разгледаните специфични особености при функционирането и изискванията за предоставяне на услуги на DIP мрежите, в съчетание с иновативната технология SR (SRv6), може да се приеме, независимо от съществуващите все още предизвикателства, че това развитие в голяма степен е на завършващ етап.

В тази връзка е необходимо приемането на национални политики, разработването на индустриални стандарти, както и ключови технологични пробиви. Съществено е, че трябва да има консенсус около цялостната концепция.

- **Национални политики.** Понастоящем има публикувани документи за ускоряване на цифровата индустриализация и насърчаване на икономическата и социална цифрова трансформация. Наличието на политики насърчава промишлените предприятия да изследват нови технологии, като синергията на облак-мрежа, детерминирани мрежи и SRv6, с цел реконструкция на вътрешните мрежи на предприятията и насърчаване на конвергенцията на IT и OT (Over the Top) мрежи. Индустриалната цифровизация и IT-OT конвергенцията на индустриалния интернет генерират много нови изисквания към мрежите. Проучването на нови DIP технологии е ново направление, предпочитано в националните политики.

- **Индустриални стандарти.** Понастоящем има одобрение за разработка на DIP мрежови стандарти, свързани с цялостната архитектура, както и на технически изисквания за DIP мрежи и за мрежови устройства за DIP.

- **Пробив в ключовите технологии.** В технологията на DIP мрежите има значително развитие в цялостната архитектура и техническо изпълнение. Тестове в някои отрасли са потвърдили, че технологиите могат да отговорят на изискванията на новите услуги. Следваща стъпка за DIP мрежите е комерсиалното внедряване на нови услуги, както и постепенно разширяване на приложението към мрежите на различни индустрии и клиенти.

В резюме, развитието на DIP мрежите се подкрепя от национални политики, формулират се свързани индустриални стандарти и се развиват ключови технологии. На база на разпространението на свързани технически познания ще бъде постигнат консенсус относно DIP мрежите между всички заинтересовани страни в индустрията, за да се насърчи тяхното цялостно внедряване и приложение.

ИЗПОЛЗВАНИ ИЗТОЧНИЦИ (REFERENCES)

[1] NetEngine 8000 M14K, M14, M8K, M8, M4, 8000E M14 M8, 8100 M14 M8 V800R022C00SPC600 Configuration Guide. Deterministic IP Networking. *Huawei* [online]. [viewed 10.05.2024]. Available from: https://support.huawei.com/enterprise/en/doc/EDOC1100279274/f27e93a1/deterministic-ip-networking#EN-US_TOPIC_0000001242269745

[2] ПЕТРОВ, Георги. *Развитие на Интернет и отворените системи*. Част 1. София: Авангард Прима, 2017. ISBN 978-619-160-834-8. [PETROV, Georgi. *Razvitie na Internet i otvorenite sistemi*. Chast 1. Sofia: Avangard Prima, 2017. ISBN 978-619-160-834-8]

МРЕЖИ С ДЕТЕРМИНИРАНИ ПАРАМЕТРИ С ИЗПОЛЗВАНЕ НА МАРШРУТИЗИРАНЕ НА СЕГМЕНТИ
ЦВЕТЕЛИНА СИМЕОНОВА

- [3] ИВАНОВА, Йоана. Моделиране на корпоративна глобална IP мрежа с мултимедийни услуги. *Годишник Телекомуникации* [онлайн]. 2019, Т.6, с. 45-53 [прегледан 10.05.2024]. eISSN 2534-854X. Достъпен на: <https://doi.org/10.33919/YTelecomm.19.6.5> [IVANOVA, Yoana. Modelirane na korporativna globalna IP mreza s multimedijni uslugi. *Godishnik Telekomunikatsii* [onlayn]. 2019, T.6, s. 45-53 [pregledan 10.05.2024]. eISSN 2534-854X. Dostapen na: <https://doi.org/10.33919/YTelecomm.19.6.5>]
- [4] Seamless Integration of Ethernet VPN (EVPN) with Virtual Private LAN Service (VPLS) and Their Provider Backbone Bridge (PBB) Equivalents. RFC 8560. *Datatracker* [online]. [viewed 10.05.2024]. Available from: <https://datatracker.ietf.org/doc/rfc8560/>
- [5] *EVPN Virtual Private Wire Service (VPWS)* [online]. [viewed 10.05.2024]. Available from: https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/vpn/63x/b-l2vpn-cg-ncs5500-63x_chapter_01001.pdf
- [6] Will Segment Routing Deliver on Its Promise? *Juniper Networks* [online]. January 2020 [viewed 10.05.2024]. Available from: <https://www.juniper.net/content/dam/www/assets/validation-reports/us/en/2020/will-segment-routing-deliver-on-its-promise.pdf>
- [7] What is segment routing. *Juniper Networks* [online]. [viewed 10.05.2024]. Available from: <https://www.juniper.net/us/en/research-topics/what-is-segment-routing.html>
- [8] ПАСАРЕЛСКИ, Росен и Теодора ПАСАРЕЛСКА. Виртуализация и сигурност в петото поколение 5G мобилни клетъчни мрежи. *Научна конференция „Знание, наука, технологии, иновации“* [компактдиск]. 2023. ISSN 2815-3480. [PASARELSKI, Rosen i Teodora PASARELSKA. Virtualizatsia i sigurnost v petoto pokolenie 5G mobilni kletachni mrezi. *Nauchna konferentsia „Znanie, nauka, tehnologii, inovatsii“* [kompaktdisk]. 2023. ISSN 2815-3480.]
- [9] ПАСАРЕЛСКИ, Росен и Теодора ПАСАРЕЛСКА. Изследване на мрежовите функции и референтната архитектура на 5G мобилни системи. *Сборник доклади от Научна конференция „Знание, наука, иновации, технологии“* [компактдиск]. 2023. ISSN 2815-3480. [PASARELSKI, Rosen i Teodora PASARELSKA. Izsledvane na mrezhovite funktzii i referentnata arhitektura na 5G mobilni sistemi. *Sbornik dokladi ot Nauchna konferentsia „Znanie, nauka, tehnologii, inovatsii“* [kompaktdisk]. 2023. ISSN 2815-3480.]
- [10] АЛЕКСАНДРОВ, Ангел и Тереза СТЕФАНОВА. *Излъчване и разпространение на електромагнитните вълни*. София: Аскони-Издат, 2014. ISBN 954-071-736-1. [ALEKSANDROV, Angel i Tereza STEFANOVA. *Izlachvane i razprostranenie na elektromagnitnite valni*. Sofia: Askoni-Izdat, 2014. ISBN 954-071-736-1.]
- [11] The Network Configuration Protocol (NETCONF). *Wikipedia: The free encyclopedia* [online]. [viewed 10.05.2024]. Available from: <https://en.wikipedia.org/wiki/NETCONF>
- [12] IEEE 1588-2008. *IEEE.org* [online]. [viewed 10.05.2024]. Available from: <https://standards.ieee.org/ieee/1588/4355/>
- [13] Deterministic Networking (detnet). *Datatracker* [online]. [viewed 10.05.2024]. Available from: <https://datatracker.ietf.org/group/detnet/about/>

Информация за автора:

ас. д-р инж. Цветелина Симеонова, Нов български университет, ул. Монтевидео № 21, департамент „Телекомуникации“, Тел. 02 8110609, tsvsimeonova@nbu.bg

Contacts:

Chief Assistant Prof. Tsvetelina Simeonova, PhD, New Bulgarian University, 21 Montevideo St., Sofia, Department Telecommunications, Tel.: 02 8110609, e-mail: tsvsimeonova@nbu.bg

Дата на постъпване на ръкописа (Date of receipt of the manuscript): 27.04.2023

Дата на приемане за публикуване (Date of adoption for publication): 30.09.2023