

Анализ на проблеми на реализацията на IPv6 в MPLS среда

Венета Алексиева

An analysis of problems in the realization of IPv6 in MPLS network: The paper presents an overview of problems when going on from IPv4 to the IPv6 in MPLS (Multi Protocol Label Switching) networks, because this update of ISP's infrastructure would give more effective ways of supporting of QoS (Quality of Service), functionality and manageability, and offer a perspective on the challenging future of IPv6 evolution.

Key words: IPv6, PE6, MPLS.

ВЪВЕДЕНИЕ

Съвременните телекомуникационни технологии се повлияват от нуждата да се предават различни видове чувствителна на закъснения информация по едни и същи канали за връзка, като им бъде осигурено зададено качество на обслужване (QoS). Днешните изследвания са насочени към изследване на: механизми за сигурност, които да съхраняват правото на лична неприкосновеност на потребителите; поддръжката на QoS и Quality of Experience (QoE); гъвкавост при реализиране на нови дългосрочни и краткосрочни иновации по отношение на мобилността в мрежите.[9]

МИГРАЦИЯ КЪМ IPv6

При създаването на Интернет не е било възможно да се предположи колко устройства ще се включат в мрежата. Към момента те са близо 5 милиарда, а към 2020 година, според прогнозата на IMS Research те ще бъдат близо 22 милиарда. Аналитичите от IDC (International Data Corporation) представят, че за една година общия брой потребители на Интернет са нараснали с 14%. IPv6 е създадена преди 13 години [7], но фактът, че през февруари 2011г. IANA (Internet Assigned Numbers Authority) изчерпа адресното пространство на IPv4, притиска големите доставчици на Интернет да развиват своите мрежи в посока на преминаване към IPv6.

В настоящия момент по данни на Google по-малко от 1% потребители по света получават достъп към Интернет по връзка с IPv6. Arbor Networks представя статистика, че само 0,15% от трафика в Интернет е по IPv6 и само 0,29% от настоящите Web-сайтове поддържат IPv6, както и само 0,5% от заявките към DNS са по IPv6. В същото време доста от ISPs заявяват, че вече използват IPv6 или планират преминаване към нея в най-близко време, като главна причина за преминаването сочат търсене на конкурентни предимства. Например, компанията NTT твърди, че предлага IPv6 на 30% от клиентските си портове, докато Akamai от юни 2011г. предлага достъп към своите ресурси и по двата протокола— IPv4 и IPv6. САЩ имат спусната директива до септември 2012г. публичните сайтове и услуги да осигурят поддръжка на IPv6 [15]. В България най-големият телеком оператор използва IPv6 само за връзки с чуждестранни оператори и все още не предоставя IPv6 на клиентските си портове.

Съвместното използване на IPv6 и IPv4, наложено от изчерпаното адресно пространство на IPv4, предполага поддръжка на преобразуване на адреси с различни способи - Network Address Translation (NAT), CIDR (Classless Inter-Domain Routing) и механизми за съвместна работа между двата протокола като „двоен стек“ IPv6/IPv4 [4,10]. В [5] се прогнозира две възможни посоки за развитие при преминаването от IPv4 към IPv6: IPv6 да се възприеме и приложи изцяло, защото много от съществуващите методи за наблюдение в Интернет са недостатъчно ефективни, или интересът към IPv6 да намалее и механизмите за преминаване към тази версия да не се наложат, защото може производителността на мрежата да не достигне очакванията. Т.к. в повечето страни администраторите на core мрежите

още не са преминали изцяло към тази версия, редица автори изследват възможни решения за преминаване към IPv6 в MPLS мрежи без особени сътресения [14,15,16,17,18]. Производителите на мрежово оборудване, което поддържа MPLS технологии са малко (Cisco, Juniper, Huawei), затова те предлагат свои решения за по-плавен преход от IPv4 към IPv6 върху MPLS [1,19,21]. Juniper Networks се фокусира върху враждане на IPv6 и конфигурации с „двоен стек“- Dual-Stack Lite, но прилага и друг подход — 6PE, предназначен за използване на IPv6 в MPLS мрежи[6]. И Cisco, и Juniper тестват своите рутери за IPv6 съгласно изискванията USGv6 (US Government)[22] и IPv6-Ready[23]. През 2011г. Juniper предлага IPv6 в устройства като MX Series 3D Universal Edge Router и T Series Core Router, които поддържат DS Lite и NAT44/NAT444, а комутаторите им от серии SRX и EX поддържат IPv6. Мрежовото оборудване на Brocade FastIron и серия NetIron за ISPs поддържа високоскоростна доставка по IPv6, различни средства за маршрутизация и безопасност по IPv6, възможности за тунелиране и технологията sFlow за управление и мониторинг на трафика по IPv6. Cisco осигурява поддръжка на USGv6 (особено в областта на IPsec v2) за VPN (Virtual Private Network) с IPv6 на база на Cisco ISR G2(с „двоен стек“). Компанията поддържа транслиране на адреси с NAT64, за да могат сървъри и мрежови устройства, които поддържат само IPv4 да работят без каквито и да е промени [4]. В сериите Cisco ASR 1000 се използва протокола Location/ID Separation Protocol (LISP), който създава тунел „IPv6 върху IPv4“ и услуги за оптимизиране на мрежата и осигуряване на безопасност [6,21].

По отношение на потребителите, ако корпоративната инфраструктура или ISP не поддържат IPv6, може да се започне с използване на IPv6 адреси от работните станции и сървърите, прилагайки „преходни“ протоколи IPv4 – IPv6 (6to4, 6over4, Teredo, ISATAP), предвидени в редица операционни системи. Това решение обаче води до проблеми, свързани с безопасността и нестабилната работа на оборудването. Проучването [20] сочи, че в процеса на миграция възникват опасения по отношение на: информационната безопасност (60%), поддържането на преходни технологии (53%), внедряването (50%), както и липсата на опит при работа с IPv6 (40%).

Използването на IPv6/MPLS може да се разглежда на две нива, притежаващи различни характеристики:

- **Access** - Все още броя на потребителите е твърде малък. Няма директно реализирани IPv6 услуги от ISP или връзките все още не са пригодени за IPv6. Има реализирани IPv4 –IPv6 услуги между агрегирани и крайни потребители.
- **Core** - Реализира се по три начина - чрез частни вериги IPv4 –IPv6; изцяло на IPv6; изцяло на IPv4.

Възможни решения са с изграждане на тунели, Dual Stack и 6PE/6VPE. При core нивото, където повечето мрежи вече са преминали на MPLS, възникват проблеми при съвместното им използване.

MPLS CORE МРЕЖИ

За доставчиците на интернет услуги (ISPs) появата на технологията MPLS, функционираща между втори и трети слой на OSI модела, има редица предимства по отношение на предшестващите я технологии. MPLS теоретически може да работи с кой да е протокол от втори слой, което позволява да се повиши мащабируемостта на тази технология– качество, особено търсено при създаването на гръбначните мрежи (core) при ISPs. Докато при предходните технологии отпадането на една физическа връзка довежда до отпадането на множество виртуални канали, тук проблемът е решен чрез координиране между втори (L2) и трети слой (L3), съвместявайки QoS, управлението на трафика чрез приоритети, гъвкавост и мащабируемост на рутването. Основната идея на MPLS е да се използват къси като дължина етикети, които да се поставят на пакетите при влизане в MPLS

домейна и чрез тях да се реализира рутиране на пакетите, вместо оригиналните им заглавни части (хедъри) [2,13]. Последвалото разработване на GMPLS (Generalized Multi-Protocol Label Switching) разширява възможностите на MPLS и позволява поддръжката както на интерфейси, обработващи пакети (PSC), така и интерфейси от типа Time-Division Multiplex (TDM), Lambda Switch (LSC) и Fiber-Switch (FSC) [3,8,11,12]. По този начин могат да се изграждат йерархични мрежи, при които на по-ниско ниво се прави преадресация на база адресната информация от пакета, а на по-горно – преадресация на база оптично влакно, по което преминават данните.

Към настоящия момент по света съществуват и се експлоатират редица оптични мрежи с различен мащаб. Тъй като в тях доставчиците на услуги ползват вече изградена мрежа (най-често на втори слой е SDH, Frame-Relay, ATM), те преминават от подобни технологии към MPLS решения. Внедряването на MPLS технология върху вече изградена и работеща топология и съвместяването ѝ с IPv6 насочва към търсене на решения на въпроси, свързани с функционалните възможности на съвместната работа на тези протоколи, и ефективността, с която те могат да заменят съществуващия протоколен стек в преносната мрежа.

MPLS с IPv4 предлага гъвкава архитектура, позволяваща унифициране на сценариите за вземане на решение за комутиране на пакета или ползване на информация от оптично ниво, като опростява стека до две нива - IP/MPLS и DWDM. Така изградената IP/GMPLS мрежа предлага универсална транспортна среда, осигуряваща необходимост от надежност и QoS, което се постига с два метода – възстановяване и защита. Възстановяването отнема по-малко мрежови ресурси, отколкото защитата и се използва по-често от ISPs. Решението коя връзка ще бъде алтернативна при отпадане на основна връзка е субективно, не винаги оптимално и в някои случаи след прехвърляне на трафика по резервната връзка се оказва, че тя няма достатъчен капацитет да поеме целия трафик и част от пакетите отпадат и не се доставят. Този проблем няма да бъде преодолян при преминаване към IPv6, т.к. той касае именно механизмите за възстановяване на самата MPLS технология, а не е породен от съвместната ѝ работа с протокола от трети слой на OSI – IP.

Търсените решения трябва обаче да отчитат желанието на ISPs да минимизират цената на вложените средства и количеството заемани ресурси.

ПОЗНАТИ ТЕХНОЛОГИИ ЗА СЪВМЕСТНА РАБОТА НА IPv6 И MPLS

Върху вече изградената и функционираща MPLS core мрежа трябва да се осигури IPv6 достъп до IPv6 услуги, за да се ползват предимствата на MPLS core като скорост, трафик инженеринг, QoS, VPN и гъвкавост. Това поражда и основния проблем – на съществуващия MPLS core има IPv4 услуги, които трябва да съществуват заедно с IPv6 услугите. Досега тук те работят на L2 /L3 ниво с протоколи LDP/RSVP и използват 6PE/6VPE. Новите решения с IPv6/MPLS core трябва да осигуряват смесени услуги IPv4/IPv6 върху IPv4, защото не може да се работи само с IPv6, т.к. още не е създаден LDPv6. Така към момента известните технологии са:

- **IPv6 върху транспортна MPLS среда** – Използва се при ISP с изграден път до оборудването на потребител. На L2 ниво технологията може да бъде Ethernet или ATM. При тази технология основен проблем е разрастването на мрежата, но предимството ѝ е, че ISP не се грижи за поддръжката ѝ.

- **IPv6 тунел върху IPv4/MPLS** - Използва се, за да предложи на ISP услуга върху съществуващите IPv4/MPLS услуги. Ограничено повлиява върху избора на оборудване на ISP, т.к. трябва да се конфигурират тунели, което добавя служебна информация при транспортирането на пакетите. На устройствата на крайните потребители работи Dual Stack IPv4-IPv6, а самия core е реализиран с IPv4.

Към момента това е най-популярното решение за интеграция на услуги. Така само потребителите трябва да имат устройства(CE), на които се конфигурира и работи Dual Stack IPv4-IPv6, което обаче принуждава ISP да реализира напълно свързана топология от CE до CE. Недостатък на това решение също е, че MPLS/VPN се поддържат с IPv4 и IPv6 тунели. ISP не делегира своите IPv6 префикси на CE устройствата.

• **IPv6 MPLS с IPv4 core (6PE/6VPE)** – Използва се от ISP да предлага IPv6 услуги над съществуващите IPv4/MPLS услуги, като ограничено повлиява върху оборудването на ISP. При тази технология проблемите са свързани с откриване и диагностициране на повреди в мрежата и наложените от решението ограничения за прилагане на балансирано натоварване (load-balancing). Може да се реализира по два начина:

– със v4 signaled LSP- когато на CE работи IPv6, а на MPLS core установяването на път(LSP) е с помощта на IGP+LDPv4, докато MP-iBGP peering е постигнат с IPv6/VPNV6;

– със v6 signaled LSP- когато и на CE, и на PE (оборудването на провайдера) работи IPv6, и пътищата се установяват с етикети от LDPv6.

6PE [6] всъщност осигурява транзитен механизъм за предаване, който осигурява уникастен IPv6 достъп по IPv4/MPLS и позволява паралелното съществуване и дистрибутиране на услуги и по IPv4, и по IPv6 на MPLS core, т.е. това отново е тунелна технология, позволяваща връзка peer-to-peer.

Т.к. е дефинирана от Cisco, тя е имплементирана (реализирана) в IOS за Cisco7600 и сериите 10000 и 12000, както и на Catalyst 6500. Това предполага обновяване само на PE устройствата (не и тези на MPLS core), за да поддържат Dual Stack/6PE, а самите пакети се транспортират от 6PE до 6PE вътре в MPLS средата, като достижимостта на CE се осъществява с обмен на информация между 6PE устройствата по iBGP (MP-BGP). Това означава, че LDPv4 дистрибутира етикетите и LSPs се реализират по познатия начин в IPv4/MPLS мрежа, като разликата е, че в етикетния стек обновяванията са с MP-IBGP/IPv6+label update.

• **IPv6 MPLS с IPv6 core** – Използва се от ISP, за да предлага MPLS услуги само в IPv6 контекст. Тази технология предлага най-големи предимства, т.к. MPLS/IPv6 има пълна функционалност. Проблемът тук е, че влиза в конфликт със съществуващата инфраструктура и е сложно да се реализира комуникация с IPv4/MPLS услугите.

ЗАКЛЮЧЕНИЕ

Представени са причините, налагащи преминаване към IPv6 в глобален мащаб. Разгледани са съвременни технологии за преминаване към IPv6 в мрежа, използваща MPLS технология, като са отбелязани проблемите, свързани с тази миграция. Малко са производителите, поддържащи MPLS и тук са отбелязани предлагани от тях решения с минимални инвестиции от страна на ISP.

В редица съществуващи core мрежи, технологията MPLS, притежаваща неоспорими предимства, е внедрена и функционираща, затова миграцията към IPv6 налага да се правят изследвания за интегрирането на IPv6 в тази среда. Телеком операторите в момента са се насочили към решения, които не изискват обновяване на оборудване или преконфигуриране на IPv4/MPLS core, т.к. се стремят към едновременно предлагане на услуги за IPv4, IPv4/VPNs и IPv6 услуги.

Благодарности

Тази разработка е подкрепена финансово от проект: "Подкрепа на творческото развитие на докторанти, постдокторанти и млади учени в областта на компютърните науки", BG 051PO001-3.3.04/13, финансиран от ЕВРОПЕЙСКИ СОЦИАЛЕН ФОНД 2007-2013г., ОПЕРАТИВНА ПРОГРАМА „РАЗВИТИЕ НА ЧОВЕШКИТЕ РЕСУРСИ“

ЛИТЕРАТУРА

- [1] AFNIC's Issue Papers, IPv6, A Passport For The Future Internet, <http://www.cudi.edu.mx/boletin/2011/afnic-issue-paper-ipv6.pdf>
- [2] Andersson L., R. Asati , Multiprotocol Label Switching (MPLS) Label Stack Entry: "EXP" Field Renamed to "Traffic Class" Field, 2009, RFC5462
- [3] Berger L., Generalized Multi-Protocol Label Switching (GMPLS), Signaling Functional Description, 2003, RFC3471
- [4] Bagnulo M., P. Matthews, I. van Beijnum, Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers, RFC6146, April 2011, www.rfc-editor.org/info/rfc6146
- [5] CAIDA, Tracking IPv6 Evolution: Data We Have and Data We Need, ACM SIGCOMM Computer Communication Review, vol.41,№3,July 2011
- [6] Clercq J. De, D. Ooms, S. Prevost, F. Le Faucheur, Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE), RFC4798, February 2007, <http://tools.ietf.org/html/rfc4798>
- [7] Deering S. and R. Hidden. Internet Protocol, Version 6 (IPv6) Specification, 1998, RFC2460, <http://www.ietf.org/rfc/rfc2460.txt>
- [8] Farrel A., A. Ayyangar , Inter-Domain MPLS and GMPLS Traffic Engineering - Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions, 2008, RFC5151
- [9] Hossfeld T., Phuoc Tran-Gia, EuroView 2010: "Vision of Future Generation Networks"-Report of the 10th Wurzburg Workshop on IP: Joint ITG, ITC, Euro-NF Event, ACM SIGCOMM Computer Communication Review, vol.41,№3,July 2011
- [10] Li X., F. Baker, IP/ICMP Translation Algorithm, RFC 6145, April 2011, <http://tools.ietf.org/html/rfc6145>
- [11] Mannie E., Generalized Multi-Protocol Label Switching (GMPLS) Architecture, 2004, RFC3945
- [12] Papadimitriou D., Generalized Multi-Protocol Label Switching (GMPLS), Signaling Extensions for G.709 Optical Transport Networks Control, 2006, RFC4328
- [13] Rosen E., A. Viswanathan , R. Callon, Multiprotocol Label Switching Architecture, 2001, RFC3031
- [14] Орлов С., Диалектика переходного периода , LAN, №08/2005, <http://www.huawei.com/ru/catalog.do?id=1150>
- [15] Орлов С., Один день из жизни IPv6, <http://www.osp.ru/telecom/2011/06/13009351/>
- [16] Wu J., Jessie Hui Wang, Jiahai Yang, CNGI-CERNET2: an IPv6 Deployment in China. ACM SIGCOMM Computer Communication Review, vol.41,№2, April 2011
- [17] <http://www.slideshare.net/CiscoRu/14-40-1450>
- [18] <http://www.npsod.ru/rus2/marketevents/document3436.phtml>
- [19] <http://www.slideshare.net/CiscoRu/cisco-8509433>
- [20] <http://ripe59.ripe.net/presentations/botterman-v6-survey.pdf>
- [21] www.cisco.com/web/solutions/netsys/ipv6
- [22] www-x.antd.nist.gov/usgv6/index.html
- [23] www.ipv6ready.org/

За контакти:

гл.ас.инж. Венета Панайотова Алексиева, Катедра "Компютърни системи и технологии", Технически университет Варна, тел.: 052-383439, e-mail: ven7066@abv.bg

Докладът е рецензиран.



РУСЕНСКИ УНИВЕРСИТЕТ „АНГЕЛ КЪНЧЕВ”
UNIVERSITY OF RUSE „ANGEL KANCHEV“

ДИПЛОМА

Програмният комитет на
Научната конференция РУ&СУ'11
награждава с КРИСТАЛЕН ПРИЗ
“THE BEST PAPER”
гл. ас. инж. ВЕНЕТА АЛЕКСИЕВА
автор на доклада
“Анализ на проблеми на
реализацията на IPv6 в MPLS среда ”

DIPLOMA

The Programme Committee of
the Scientific Conference RU&SU'11
Awards the Crystal Prize
"THE BEST PAPER"
to Assistant Professor VENETA ALEKSIEVA
author of the paper
“An analysis of problems in the
realization of IPv6 in MPLS network ”

РЕКТОР
RECTOR

доц. дтн Христо Белоев
Prof. DSc Hristo Beloev

29.10.2011