Нов български университет

Проектиране на корпоративни мрежи

Част V

IP адресни схеми

Доц. Д-р Емил Стоилов

Департамент по Информатика на НБУ

София, май 2016

Съдържание

В този доклад са разгледани различни схеми на IP адресиране позволяващи обобщаване на маршрути. Особеностите на използваните в слой 3 на корпоративните мрежи маршрутизиращи протоколи като Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF) и Border Gateway Protocol (BGP), както и препоръките за тяхното конфигуриране ще бъдат поместени в отделен доклад.

1. Избор на подходящи схеми за IP адресиране

Проектирането на IP адресната схема на професионално ниво изисква съобразяването с няколко фактора. В този раздел ще разгледаме значението на правилния избор и планиране на IP адресите, като и важността на тяхното обобщаване (summarization).

1.1 Планиране на IP адресите като основен елемент при проектирането

Структурираното и модулно окабеляване на мрежовата инфраструктура води до един добър дизайн с ниски разходи за поддръжка и надграждане. По подобен начин добре планираната IP адресна схема лежи в основата за по-голяма ефективност в работата и поддръжката на мрежата. Без правилното предварително планиране мрежите не са в състояние да се възползват от предимствата на обобщените маршрути присъщи на много протоколи за маршрутизация.

Обобщаването на маршрутите е изключително важно за мащабираемостта на всеки маршрутизиращ протокол. Някои съществуващи схеми за IP адресиране обаче може да не позволяват такова обобщаване. Много време и усилия трябва да отделим за да организираме правилно IP подмрежите в блокове така, че да улесним обобщаването. Ползата от използването на обобщени адреси се изразява в това, че се намалява маршрутизирания трафик и натоварването на самия маршрутизатор, както и че получаваме по-бърза сходимост на протоколите. Въпреки, че при съвременните маршрутизатори процесорите лесно могат да се справят със значително увеличения обем работа в сравнение с по-старите маршрутизатори, то намаляването на натоварването смекчава въздействието на периодите на интензивна мрежова нестабилност. Най-общо, обобщените маршрути забавят или намаляват объркването в маршрутизацията и по този начин правят мрежата по-стабилна. В допълнение обобщените маршрути водят до по-бърза сходимост. Откриването и отстраняването на повреди в мрежите използващи обобщени маршрути е по-лесно, тъй като в маршрутната таблица има само няколко пътя които се обявяват.

Точно както определянето на подходящите блокове от адреси води до по-ефективна маршрутизация, така и внимателното определяне на задачите на отделните подмрежи може да подпомогне техните функции в структурата на адресната схема. Това от своя страна дава възможност за ефективни и лесно управлявани списъци за контрол на достъпа (Access Control Lists – ACL), за качеството на услугите (Quality of Service – QoS) и за целите на сигурността.

В допълнение към разпределянето на подмрежите в обобщени блокове, препоръчително е и да се изберат и блокове от адреси в рамките на тези подмрежи, които лесно да могат да бъдат обобщавани или описвани, като се използва заместващо маскиране (wildcard masking) в списъците за контрол на достъпа (ACL). С една добре подбрана схема за адресиране в корпоративната мрежа списците за достъп ACL стават лесни за поддръжка.

1.2 Обобщени адресни блокове

Обобщените адресни блокове са от ключово значение за създаването и използването на обобщени маршрути. Как да разпознаем блоковете от адреси, които могат да бъдат обобщени? Един блок от IP адреси може да се обобщи ако адресите са с последователни номера в един от октетите. Тази последователност от номера трябва да отговаря на

определен образец от битове подходящ за обобщаване. Този образец трябва да може да бъде описан без използването на двоична аритметика.

За да могат адресите с последователните номера да бъдат обобщени, блокът трябва да съдържа n адреси, където n е степен на 2. В допълнение първият номер в последователността трябва да е кратен на n. Последователността винаги трябва да свършва преди следващото кратно на n.

Например всеки блок от адреси, кото отговаря на следните условия може да се обобщи:

- 128 последователни номера, като се започне с кратно на 128 (0 или 128)
- 64 последователни номера, като се започне с кратно на 64 (0, 64, 128 или 192)
- 32 последователни номера, като се започне с кратно на 32
- 16 последователни номера, като се започне с кратно на 16

Да разгледаме последователните адреси от 172.20.160.0 до 172.20.191.0. В този блок от адреси имаме 191 – 160 + 1 = 32 адреса с последователни номера в третия октет. Да отбележим, че 32 е равно на 2 на 5-та степен. Освен това 160 е кратно на 32 (5 x 32 = 160). Тъй като този обхват от адреси отговаря на условията, то последователността от адреси от 172.20.160.0 до 172.20.191.0 може да бъде обобщена.

Намирането на правилната маска става изключително лесно при обобщените адресни блокове. Формулата е да извадим n от 256. Например за блок от 32 адреса имаме 256 – 32 = 224. Понеже блокът е в третия октет, 224 се поставя в този октет и маската придобива вида 2255.255.224.0.

Обобщеният маршрут изразен като 172.20.160.0, 255.255.224.0 или като 172.20.160.0/19 описва как да се достигнат подмрежите с адреси от 172.20.160.0 до 172.20.191.0.

1.3 Обобщаване на адресите при IPv6

Въпреки че форматът на адреса при IPv6 е различен от формата при IPv4, принципът е един и същ. Блоковете от последователни IPv6 /64 подмрежи могат да бъдат обобщени в по-големи блокове с цел да се намали размера на маршрутната таблица и да се увеличи нейната стабилност. В известна степен обобщаването на маршрутите при IPv6 е по-просто отколкото при IPv4, защото не е необходимо да се разглеждат маски с променлива дължина (Variable Length Subnet Mask –VLSM). Повечето IPv6 подмрежи имат дължина на префикса 64 бита, така че се търсят непрекъснати блокове от /64 подмрежи. Броят на подмрежите в такъв блок трябва да бъде степен на 2, началният адрес трябва да е кратен на същата степен на 2 и тогава блокът може да бъде обобщен.

Например да разгледаме блок от 2001:0DB8:0:A480::/64 до 2001:0DB8:0:A4BF::/64. Един бърз анализ на този адресен блок показва, че различията са в последните два шестнадесетични знака, които са 0x80 за първата подмрежа и 0xBF за последната подмрежа в диапазона. Преобразуването на тези числа в десетичен формат дава 0x80 = 128 и 0xBF = 191. Това е блок от 191 − 128 + 1 = 64 подмрежи. След проверката, че 128 е кратно на 64 можем да заключим, че този блок от подмрежи може да бъде обобщен.

За да изчислим дължината на префикса, трябва да намерим броя на битовете представляващи блока от 64 адреса. 6 бита трябва да се извадят от дължината на оригиналния префикс /64 за да получим дължината на префикса на обобщението, която е /58.

Следователно можем да използваме обобщения маршрут 2001:0DB8:0:A480::/58 за да достигнем до подмрежите от 2001:0DB8:0:A480::/64 до 2001:0DB8:0:A4BF::/64.

1.4 Технологии изискващи промени в схемите за IP адресиране

Понякога се налага препроектиране на схемата за адресиране. Някои по-нови технологии изискват допълнителни подмрежи, например:

- **IP телефония**: За да се поддържат гласовите услуги са необходими допълнителни подмрежи или адресни диапазони. В някои случаи при внедряване на IP телефония броят на подмрежите се удвоява.

- **Видеоконферентна връзка**: Всеобхватните приложения TelePresence използват голяма честотна лента и са чувствителни към пропадания и забавяния. Добрата практика е тези устройства да бъдат отделени, което създава необходимостта от повече подмрежи.

- **Комутиране в слой 3 на границата на мрежата**: Използването на комутиране в слой 3 на границата на корпоративната мрежа е друга тенденция налагаща необходимостта от повече подмрежи. При тази технология обикновенно се появяват много на брой, но малки подмрежи. В този случай адресното пространство бързо се изчерпва и се налага препроектиране на адресната схема.

- **Контрол на достъпа до мрежата (Network Admission Control - NAC)**: NAC също се използва в много организации. При някои Cisco 802.1X и NAC внедрявания динамично се присвояват виртуални локални мрежи (VLAN) въз основа на входните данни на поребителя или на неговата роля. В такива случаи ACL контролира връзката към сървърите и мрежовите ресурси въз основа на подмрежата-източник, която пък е базирана на ролята на потребителя.

- **Корпоративни изисквания**: Корпоративните инициативи за повишаване на сигурността често водят до отделяне и изолиране на групи от сървъри при което се извършва допълнителна сегментация на мрежата. Изграждането на нови подмрежи може да направи управлението на мрежата по-сложно. В този случай е желателно описанието на позволения трафик в ACL да бъде само с няколко реда. Затова се стремим да използваме обобщаващо адресиране, което да подпомогне администраторите ефективно да управляват техните мрежи.

1.5 Планиране на адресите

Първата стъпка в прилагането на подходящо за ACL адресиране е да се определи необходимостта. В среда с подмрежи за IP телефони и NAC, подмрежите трябва да бъдат включени в ACL. При IP телефоните ACL вероятно ще се използва както за нуждите на QoS, така и за правилата за сигурностт при гласовата комуникация. При подмрежите изпълняващи ролята на NAC, ACL най-вероятно ще се използва за целите на сигурността.

Сървърите в средните и големи изчислителни центрове трябва най-малкото да бъдат групирани така, че сървърите с различни функции или нива на критичност да се намират в отделни подмрежи. С това се избягва изписването на индивидуални IP адреси в дългите ACL. Ако сървърите са в подмрежи свързани към различни комутатори за достъп, може да бъде полезно използването на модел със заместващо маскиране (wildcard) в ACL.

Ако адресната схема позволява да бъдат написани прости правила със заместващо маскиране, то тези прости ACL правила могат да се използват навсякъде. Така се избягва използване на ACL свързани с местоположението в които са дефинирани адресите на източника или местоназначението на локалните подмрежи. Подходящото за ACL

адресиране поддържа една или няколко глобални ACL, които се прилагат по идентичен начин в различните точки на мрежата. Това обикновено се постига с инструмент като Cisco Security Manager.

В списъците за достъп на IPv6 заместващо маскиране обикновено не се използва. Всички адреси на източника и местоназначението се отбелязват с използването на префикси. Поради това е важно подмрежите, които ще бъдат групирани в списъците за достъп да попадат в обобщен адресен диапазон.

2. Приложения на обобщените адресни блокове

Обобщените адресни блокове могат да бъдат използвани в различни мрежови приложения, например:

- Разделяне в отделни VLAN на гласовите комуникации и данните. Използване на адресиране в зависимост от ролята на подмрежата.
- Разделяне на битовете при обобщаване на маршрути
- Адресиране на клиентите на виртуална частна мрежа (VPN)
- Преобразуване на мрежовите адреси (Network Address Translation - NAT)

Тези приложения ще бъдат разгледани по-подробно в следващите раздели.

2.1 Прилагане на адресиране зависимо от ролята на подмрежите

Прилагането на адресиране зависимо от ролята на подмрежата (role-based addressing) най-лесно се обяснява, ако използваме мрежа 10. По-долу е представена една проста схема, която може да се използва при шкафовете с L3 устройства, а именно да определим адресите по следния начин

10.number_for_closet.VLAN.x /24

като избегнем двоичната аритметика. При този подход вторият октет се използва за номериране на шкафовете или L3 комутаторите (number_for_closet), третият октет се използва за номериране на виртуалните локални мрежи (VLAN), а четвъртият октет – за хостовете.

Ако имате повече от 256 шкафа или L3 комутатори и вторият октет не ви е достатъчен, то можете да заемете за вашата цел битове от началото на третия октет, понеже едва ли ще имате нужда от 256 VLAN в комутатор или шкаф.

Друг подход е да се използват някои или всички частни адресни блокове от клас B на мрежите. При този подход обикновено се налага използването на двоична аритметика. Най-лесният начин е да се определят битове като се използва тяхното разделяне. Да вземем например мрежата 172.0001 xxxx.xxxx xxxx.xxhh hhhh. В този случай 6 бита в четвъртия октет са резервирани за хостовете, или 62 хоста за подмрежа (VLAN). Битовете x се разделят допълнително.

При този формат използваме десетичен запис за първия октет и двоичен запис за втория, третия и четвъртия октет с цел да сведем до минимум преобразуването в двете посоки.

Ако е необходимо да използвате битове от втория октет за идентифициране на допълнителни шкафове можете да използвате нещо като 172.16.cccc cccr.rrhh hhhh, където:

- Седемте бита означени с буквата с позволяват използването на до 128 шкафа или L3 комутатори.

- Трите бита означени с буквата r са отделени за подмрежи изпълняващи определена роля (например 8 NAC, блок от шкафове или някаква друга роля) за комутатор.

- С буквите h са означени шестте бита заделени за хостове в подмрежите. Следователно при това разпределение имаме до 62 хоста във всяка подмрежа.

Този адресен план е достатъчен за да покрие изискванията за една голяма корпоративна мрежа. Във втория октет имаме на разположение още 4 бита, които можем да използваме при нужда.

Използвайки такива схеми на адресиране ние можем да напишем малък брой глобални изявления (statements) за разрешение или отказ на всяка роля. Това значително опростява поддръжката на ACL в граничните маршрутизатори. Значително по-лесно е да се поддържа един ACL за всички VLAN или интерфейси на ръба на мрежата, отколкото различни ACL за всеки L3 комутатор в слоя за достъп или в разпределителния слой.

2.2 Разделяне на битовете при обобщаване на маршрути

Токущо описаният метод може да се използва и когато искаме обобщен адресен блок за нуждите на маршрутизиращите протоколи, но не можем да ползваме разделение на границата на октетите. Главната идея тук е да започнем с мрежовата част на адреса (network prefix), а именно от 10.0.0.0 за мрежите от клас A, за мрежа в диапазона от 172.16.0.0 до 172.31.0.0 за клас B, от 192.168.n.0 за клас C. Останалите битове можем да възприемем като достъпни за адресиране на област, подмрежа или хостове. Полезно е да означим тези битове с x, след което да ги заместим с a, s или h в зависимост от това за какво те отговарят. Означението n в адреса показва частта от адреса, която не подлежи на промяна или преотстъпване.

Обикновено имаме информация за големината на подмрежите. Например можем да заменим шест x бита с h с което ограничавате броя на хостовете в дадената подмрежа до 62.

След това можем да определим броя на необходимите WAN връзки и броят на областите, които е необходима да се покрият, т.е. да определим броя на битовете x които ще бъдат заменени с a. Останалите битове ще бъдат от вида s. Ако не използвате всичките подмрежи, то имате определен адресен запас за бъдещо развитие.

Например да приемем че използваме мрежа 172.16.0.0, с подмрежи във всяка от които имаме по 62 хоста. Това определя последните 6 бита в четвъртия октет за адрес на хостове. Ако имаме нужда от 16 или по-малко области, можем да заделим 4 бита за номер на област. Останалите 6 бита са от типа s и са заделени за номериране на подмрежите. Следователно във всяка област можем да имаме по 62 подмрежи, което е достатъчно много.

2.3 Пример: Разделяне на битовете за OSPF област 1

Този пример илюстрира подхода за разделяне на битовете при определяне на адресите за област 1 (Area 1) на протокола OSPF. Първите четири x бита в адреса заменяме с номера на областта, т.е. с 0001. Това са битове от типа a. Следователно адресите в област 1 са от вида 172.16.0001 ssss.sshh hhhh. Това означава, че стойността на третия октет в десетичен вид е между 16 и 31. Адресите в диапазона от 172.16.16.0 до 172.16.31.255 са определени за област 1. Ако повторим тази логика, лесно е да се убедим, че адресите за област 0 са от 172.16.0.0 до 172.16.15.255, а област 2 ще има адреси от 172.16.32.0 до 172.16.47.255.

Лесно се вижда, че например първите 5 подмрежи в оласт 1 ще бъдат с адреси съответно 172.16.16.0/26, 172.16.16.64/26, 172.16.16.128/26, 172.16.16.192/26 и 172.16.17.0/26.

Една препоръка в съответствие с добрите практики в обобщаването на адресите е последната подмрежа във всяка област да се раздели допълнително на подмрежи /30 или /31, чиито адреси да се използват за WAN връзките.

2.4 Адресни схеми за VPN клиенти

Определени ползи можем да получим и ако насочим вниманието си към IP адресирането на VPN клиентите. Ако за основа на сигурността приемем класификация по отделните роли които се изпълняват, то трябва да групираме VPN клиентите въз основа на тези роли, а именно като администратори, служители, различни групи от изпълнители или консултанти, външни организации, гости и т.н. Може да се използват различни VPN групи за различни VPN клиенти. Достъпът до мрежата в зависимост от ролята може да бъде контролиран посредством механизъма за групова парола. За всяка група ще бъде определена VPN крайна точка или с други думи краен адрес (endpoint address). Адресът на източника на трафика генериран от потребителския компютър (source address) ще бъде именно този VPN краен адрес. Тогава различните подмрежи или блокове от крайни VPN адреси могат да бъдат използвани в списъците за достъп ACL за контрол до мрежовите ресурси. Ако се използват обобщени адресни блокове, то маршрутизирането на обратния трафик до клиентите става значително по-лесно.

2.5 Използване на NAT

Системата за преобразуване на адреси NAT (Network Address Translation) е мощен инструмент за работа с IP адреси. Тя е много полезна в предприятието, защото позволява преобразуването на частните вътрешни адреси в публични адреси в точката за връзка към Интернет. Въпреки това ако тя се използва прекомерно, може да се окаже и вредна.

NAT, както и PAT (Port Address Translation) са често срещани инструменти в защитните стени. Те се прилагат и в устройствата за балансиране на натоварването в зависимостост от съдържанието. Когато NAT е изградена по контролируем и дисциплиниран начин, тя може да бъде много полезна.

Избягвайте използването на NAT или PAT за преобразуване на вътрешни адреси във вътрешни адреси. Използването на NAT в тази роля значително затруднява и обърква процеса на откриване на неизправности в мрежата и тяхното отстраняване. Например може да бъде трудно да установите към коя от мрежите с номер 10 в организацията потребителят е свързан в момента.

Понякога се налага използването на вътрешни NAT или PAT при свързване на мрежи след корпоративно сливане или придобиване. Много организации използват като вътрешна мрежа 10.0.0.0, в резултат на което при сливането се появяват „две вътрешни мрежи 10.0.0.0“. Тази ситуация не е добра дори и само защото откриването и отстраняването на неизправности в мрежата, както и поддържането на нейната документация е много трудно. Трябва да се предвиди преадресиране колкото е възможно по-скоро. Препоръчителната практика тук е да се изолират всички сървъри, достъпът до които е през устройства следящи съдържанието (content devices) използващи NAT. Тези сървъри обикновено са изолирани, тъй като пакетите с NAT адреси не са използваеми никъде другаде в мрежата. NAT също може да бъде използвана в изчислителния център за изграждане на система от малки управляващи VLAN.

NAT се оказва полезна и в случая, когато една организация има повече от няколко външни бизнес партньори. Някои компании обменят динамична маршрутизираща информация с

външни бизнес партньори. Обменът изисква доверие. Недостатък на този подход е, че статичен маршрут от вашата мрежа към партньора може по някакъв начин да се рекламира обратно към вас. Такова рекламиране, ако се възприеме, може да доведе до това, че част от вашата мрежа ще стане недостъпна. Един от начините да се справим с такава ситуация е да приложим двупосочно филтриране на маршрутите към партньорите: Да се рекламират само подмрежи до които партньорът да има достъп и да се одобряват само маршрути към подмрежи на партньора, до които вашия персонал или сървъри трябва да имат достъп.

Някои организации предпочитат да използват статично маршрутизиране за достигане до пратньорите, което да бъде контролирано плътно. Следващият скок понякога е към виртуален адрес на двойката маршрутизатори контролирани от партньора, като се използват протоколите Hot Standby Router Protocol (HSRP) или Gateway Load Balancing Protocol (GLBP).

Когато партньорът е огромен, например голяма банка, статичното маршрутизиране е твърде трудоемко. Импортирането на хиляди външни маршрути във вътрешния маршрутизиращ протокол за всеки от няколкото големи партньори води до раздуването на маршрутната таблица.

Другият подход е маршрутизирането от партньора да завършва в граничния маршрутизатор (edge router), като при това се използват обобщени маршрути. След това можем да използваме NAT за да преобразуваме всички адреси на партньора в набор от локално присвоени адреси. Различни адресни блокове на NAT се използват за различните партньори. Този подход превръща широк кръг от партньорски адреси в строго контролиран набор от адреси и опростява откривнето и отстраняването на неизправности. При него също се избягват потенциални проблеми когато много организации използват мрежа 10.0.0.0/8.

Ако блоковете от адреси в NAT са избрани от по-голям блок, който може да бъде обобщен, то преразпределеният (redistributed) статичен маршрут на този по-голям блок дава възможност всички партньори да бъдат достъпни. Вътрешната маршрутизация тогава има само един маршрут и той е „път към мрежите на всички партньори“. При този подход имаме по-бърза сходимост при вътрешната маршрутизация, като подмрежите на пратньорите не са в маршрутните таблици на предприятието. Недостатък на този подход е по-трудното проследяване на източниците на IP пакетите. Ако все пак това е необходимо, то можете да получите тази информаци от таблицата на NAT.

3. Адресни схеми за IPv6

Понеже адредното пространство на IPv6 е много по-голямо от адресното пространство на IPv4, то изграждането на подходящи адресните схеми за IPv6 е в много отношения по-просто. Разделянето на адресното пространство на IPv4 винаги представлява акт на балансиране между желанието да получим определен брой подмрежи, определен брой хостове във всяка подмрежа, групирането на подмрежите по начин позволяващ тяхното обобщаване, като в същото време осигурим възможност за бъдещо разрастване. При IPv6 създаването на адресната схема е много по-просто.

Препоръчително е всички IPv6 подмрежи да имат префикс /64, т.е. за номер на мрежата да бъдат заделени 64 бита. Това ни позволява във всяка една подмрежа да имаме повече хостове, отколкото един бродкаст домейн физически може да поддържа. Съществуват известни опасения, че при такъв вид адресиране, при всяка връзка, например от точка до точка (point-to-point), ненужно ще се пропилява адресно пространство. Ето защо някои организации използват също и префикси /126.

Използването на префикс /64 за всяка подмрежа, която съдържа крайни хостове, премахва всякакви съображенията за броя на хостовете в подмрежата при изграждането на

адресната схема. Второто съображение при IPv4 адресните схеми е да се определи точния брой на подмрежите във всеки обект. Местните Интернет регистри често определят префикс /48 за техните адресни блокове отнасящи се за всеки потребителски обект. Следователно ни остават 16 бита за номериране на подмрежите в обекта, т.е. можем да имаме до 65,536 подмрежи, което е напълно достатъчно дори и за прекалено големи обекти.

Тези 16 бита, които са достъпни за номерирането на подмрежите могат свободно да се използват за прилагане на обобщени адресни схеми или за адресиране съгласно ролята която изпълняват подмрежите.

3.1 Разделяне на битовете при IPv6

Битовете, определени за адресиране на подмрежи, могат да бъдат разделени по много различни начини. Също както при IPv4, при IPv6 адресната схема е неразделна част от цялостния дизайн на мрежата и трябва да бъде синхронизирана с други проектантски решения. В една съществуваща мрежа трябва да се помисли за еднозначното съответствие между IPv6 адресната схема и някои известни вече параметри, като например броя VLAN и IPv4 адресите. Това съответствие облекчава управлението на мрежата и задачата за отстраняване на възникнали неизправности, понеже мрежовите оператори могат да свързват структурата на IPv6 адресите със съществуващата адресна структура.

Следват примери на IPv6 адресни схеми, при които 16-те бита за подмрежи са разделени по различен начин с цел задоволяване на различни проектантски изисквания:

- **Разделяне по област**: Ако обектът е разделен на области, например като OSPF области, това трябва да се отрази в адресната структура за да може да се извърши обобщаване на адресите. Например първите 4 бита могат да представят дадена област, докато останалите 12 бита са заделени за кодиране на VLAN. По този начин имаме 16 области с 4096 подмрежи във всяка от тях. Един малък диапазон от VLAN номера следва да бъдат заделени за връзки от точка до точка в рамките на областта.

- **Съответствие с IPv4 адресна схема**: Ако съществуващата IPv4 адресна структура се основава на мрежа 10.0.0.0/8 и всички подмрежи са с /24 или по-къс префикс, средните 16 бита в IPv4 адреса могат да бъдат нанесени директно в IPv6 адреса. Например, ако подмрежата има IPv4 префикс10.123.10.0/24, средните два октета 123.10 магат да бъдат преобразувани в шестнадесетична форма: 123 = 0x7B и 10 = 0x0A. Ако полученият от регистъра на Интернет префикс е 2001:0DB8:1234::/48, добавянето към него на 16 бита извлечени от IPv4 адреса води до 2001:0DB8:1234:7B0A::/64 като префикс на IPv6 подмрежа. Този метод е много удобен, понеже то установява еднозначно съответствие между добре известните IPv4 адреси и новите IPv6 адреси. Все пак, за да се използва този метод, IPv4 адресната схема трябва да изпълнява определени условия, като да не се използват повече от 16 бита за подмрежи.

- **Адресиране базирано на роли**: За по-лесното създаване на списъците за достъп ACL и определянето на правилата на защитните стени, може да бъде полезно да се кодират отделни роли (например гласова комуникация, корпоративни данни, гост-потребители) в адресната схема. Например първите 4 бита маже да се използват за представяне на ролята, следващите 4 бита – за областта, а последните 8 бита – за VLAN. Тогава ще имаме 16 различни роли, 16 области и 256 VLAN за всяка област за всяка роля. С използването на 4 последователни бита за област става изключително лесно да се конфигурират списъците за достъп и правилата на защитните стени, понеже всички подмрежи за специфична роля попадат в един /52 адресен блок. Обобщаването е по-малко ефективно отколкото при схема, която е чисто базирана на

области. Вместо един обобщен адресен блок за област, тук ще имаме обобщен блок за роля.

Методите, които са показани тук, са само примерни. Когато създаваме адресната схема като част от проекта на мрежата, внимателно трябва да се обмислят и други параметри и мрежови елементи, така че изготвената адресна схема да взема под внимание и тях.

4. Дизайн на IPv6 корпоративните мрежи

Три основни модела за внедряване могат да бъдат използвани при реализацията на IPv6 в комплекса от фирмени сгради (кампуса) на корпорацията [1]: модел с двоен стек (dual-stack model), смесен модел (hybrid model) и модел с обслужващ блок (service block model) [2]. Изборът на определен модел силно зависи от това дали в различните области на мрежата се използва IPv6 хардуерно комутиране.

Използването на модела с двоен стек води до най-голяма гъвкавост и работоспособност при внедряването на IPv6 в съществуващите IPv4 среди. IPv6 може да се активира там, където IPv4 е реализирана заедно със свързаните функции необходими да направят IPv6 маршрутизируема, високо достъпна и сигурна. В някои случаи IPv6 не може да бъде активирана в конкретен интерфейс или устройство поради наличието на наследени приложения или хостове, в които не се поддържа IPv6. И обратното, IPv6 може да бъде активирана в интерфейси и устройства, в които поддръжката на IPv4 не е вече необходима.

Едно от основните изисквания за внедряване на модела с двоен стек е комутирането на IPv6 пакетите да се извършва хардуерно във всички комутатори на кампуса. Ако някои области на мрежата на кампуса не поддържат IPv6 хардуерно комутиране, то трябва да се използват тунелни механизми за да се интегрират тези области в IPv6 мрежата. Смесеният модел обединява подхода с двоен стек в областите работещи под IPv6 с тунелните механизми, като например Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) [3] и ръчно конфигурираните IPv6 тунели, където е необходимо.

Смесеният модел адаптира колкото е възможно повече характеристики на съществуващата мрежова инфраструктура. При него са избрани прехвърлящи механизми на базата на множество критерии, като IPv6 хардуерните възможности на елементите на мрежата, броя хостове, видовете приложения, местата, където са разположени IPv6 услугите, както и поддръжката от мрежовата инфраструктура на тези различни преходни механизми.

Моделът с обслужващ блок използва различен подход към въвеждането на IPv6. Той разглежда IPv6 като услуга, подобно на предоставянето на други услуги, като например гласова комуникация или достъп на гости в мрежата. Този тип услуги се поставят в едно централно място. Моделът с обслужващ блок е уникален с това, че може да се изгради като надстройка на съществуващата IPv4 мрежа и е напълно централизиран. Изграждането на такава надстройка може да стане много бързо, като в същото време позволява висока наличност на IPv6 услугите, възможности за QoS и ограничаване на достъпа до IPv6 ресурсите. Всичко това става с много малко или никакви промени в съществуващата IPv4 мрежа. След като съществуващата мрежа на кампуса започне да функционира с IPv6, моделът с обслужващ блок може да бъде децентрализиран. Връзките към обслужващия блок се заменят с тунели (конфигурирани ръчно или с ISATAP) и се преобразуват във връзки на модела с двоен стек. Когато всички слоеве на мрежата на кампуса започнат да работят по модела с двоен стек, обслужващият блок може да бъде демонтиран или да се използва за други цели.

Тези три модела не са нещо изключително и завършено само по себе си. Елементи взети от различните модели могат да бъдат комбинирани за да се изпълнят някои специфични мрежови изисквания.

В крайна сметка моделът с двоен стек е за предпочитане. Останалите два модела могат да се разглеждат като преходни решения. От тях може да се премине към модела с двоен стек по елегантен начин, без да са необходими принудителни хардуерни обновявания в целия кампус. От гледна точка на планирането на адресите това означава, че изграждането на адресната схема трябва да предвиди използването на пълен модел с двоен стек в бъдеще.

4.1 Модел с двоен стек

Моделът с двоен стек използва IPv4 и IPv6 паралелно, без никакви тунели или преобразувания между тези два протокола. IPV6 е активиран в слоя за достъп, в разпределителния слой и в ядрото на мрежата на кампуса. Този модел прави IPv6 прост за внедряване и е много мащабируем. Не съществуват зависимости между дизайните на IPv4 и IPv6, което води до по-лесно внедряване и отстраняване на възникналите проблеми.

Използването на модела с двоен стек предлага няколко предимства пред останалите модели. Основното предимство на модела е, че той не изисква изграждането на тунели вътре в мрежата на кампуса. Двата протокола IPv4 и IPv6 функционират успоредно и независимо един от друг. Единственото общо нещо са мрежовите ресурси, които те споделят. При тях имаме независима маршрутизация, висока достъпност, QoS, сигурност и политики за групово предаване (multicast policies). Моделът с двоен стек предлага също и някои експлоатационни предимства, например пакетите се комутират директно, без да е необходимо тяхното капсулиране и претърсване.

Тези предимства правят модела с двоен стек предпочитан модел. Той обаче изисква всички комутатори в кампуса да работят с IPv6.

4.2 Смесен модел

Стратегията на смесения модел е да се използват два или повече прехвърлящи механизми с една и съща цел на внедряване. Гъвкавостта е ключов аспект на смесения подход. Всяка комбинация от прехврлящи механизми трябва най-добре да отговаря на мрежовата среда. Смесеният модел използва модела с двоен стек във всички области на мрежата, където оборудването поддържа IPv6. Тунелни механизми се прилагат в областите, които в момента не поддържат хардуерно IPv6. Тези области могат по-късно, когато се обнови хардуера, да бъдат прехвърлени към модела с двоен стек.

Различни тунелни механизми и сценарии за внедряване могат да бъдат част от смесения модел. В този раздел са откроени два общи сценария.

Първият сценарий, който може да изисква използването на смесен модел, е когато в ядрото на мрежата на кампуса не е активиран IPv6. Това се случва често когато в ядрото нямаме хардуерна поддръжка на IPv6 изобщо, или пък имаме някакво ограничена поддръжка, но с много ниска производителност. При този сценарий ръчно конфигурираните тунели се използват от разпределителния или агрегиращ слой. Два тунела от всеки комутатор се използват за резервиране и балансиране на натоварването. От гледна точка на IPv6 тунелите се разглеждат като виртуални връзки между комутаторите на разпределителния или агрегиращия слой. В тунелите маршрутизирането и груповото предаване за IPv6 се конфигурира по същия начин, както при конфигурирането по метода с двоен стек. Скалируемостта на този метод е ограничена, но все пак това е добър модел когато ядрото на мрежата на кампуса се ремонтира или когато има планове да бъде модернизирано, но в същото време имаме и изисквания за достъп до IPv6 услуги преди тази модернизация да се извърши.

Вторият сценарий се фокусира върху ситуацията, когато хостовете разположени в слоя за достъп трябва да използват IPv6 услуги, но в разпределителния слой не е активиран IPv6. Комутаторът от разпределителния слой обикновено е първият шлюз от слой 3 за

устройствата от слоя за достъп. Ако нямаме налични IPv6 възможности в съществуващите комутатори от разпределителния слой, то хостовете няма да получат достъп до необходимата маршрутизираща информация, например до DHCP за IPv6, и следователно няма да имат достъп до останалата част от IPv6 мрежата. При този сценарий тунелите могат да се използват от работещите с IPv6 хостове за достигане до IPv6 услуги, намиращи се над разпределителния слой. Например трябва да се разреши IPv6 на работещите под Windows хостове и да се изгради статичен ISATAP тунел. Използвайки ISATAP IPv4 адрес, хостовете изграждат тунел до IPv6 маршрутизаторите в ядрото и получават IPv6 адреси за достъп до останалата част от мрежата.

Завършването на ISATAP тунелите в ядрото прави този слой да изглежда като слой за достъп за IPv6 трафика, което може да бъде нежелателно от гледна точка проектирането на горните нива. За да се избегне смесването на функциите на ядрото и на слоя за достъп, ISATAP тунелите трябва да се терминират в друга група комутатори, например в комутаторите в агрегиращия слой на изчислителния център.

Основната причина да се избере смесен модел е внедряването на IPv6 без да преминаваме през незабавна смяна на хардуера в части от мрежата. Това позволява комутаторите, които не са достигнали края на жизнения си цикъл да останат на разположение като се избягнат допълнителните разходи свързани с обновяването на оборудването.

Този модел има и някои недостатци. Използването на ISATAP тунели не е съвместимо с IPv6 груповото предаване. Затова всички устроства в слоя за достъп или в разпределителния слой, които изискват използването на IPv6 приложения за групово предаване трябва да използват модела с двоен стек. Ръчно изградените тунели поддържат IPv6 груповото предаване и по тях може да преминава IPv6 трафик през IPv4 ядро. Друг недостатък на смесения модел са добавените усложнения сврзани с тунелите. Трябва да бъдат отчитани много и различни съображения свързани с производителността, управлението, сигурността, скалируемостта и наличността.

4.3 Модел с обслужващ блок

Моделът с обслужващ блок има няколко прилики със смесения модел. IPv4 мрежата се използва за като основа при внедряването на IPv6. Връзката на хостовете в слоя за достъп се осигурява от ISATAP. За достъп до приложенията и услугите намиращи се в агрегиращия слой на изчислителния център се използват ръчно конфигуриране тунели. Конфигурирана е IPv4 маршрутизация между ядрото и комутаторите на обслужващия блок.

Това което най-много го различава от смесения модел е, че при модела с обслужващ блок свързването с IPv6 става централизирано, като се използва двойка отделни допълнителни, редундантни комутатори. При конкретното решение използваме наприме два комутатора от серията Cisco Catalyst 6500 в които са вградени Cisco Supervisor Engine 32 или Supervisor 720 модули. Ключът към поддържането на високо мащабируема и редундантна конфигурация е използването на високопроизводителни комутатори със супервайзорни модули, които да управляват трафика от ISATAP, ръчно конфигурираните тунели в връзките на модела с двоен стек за цялата мрежа на кампуса.

Най-голямото предимство на този модел в сравнение със смесения модел е, че централизираният подход ви позволява да разгърнете IPv6 по контролиран начин. По същество, моделът с обслужващ блок осигурява контрол върху темповете на въвеждането на IPv6 услугите, като се възползва от следното:

- За всеки потребител или VLAN може да конфигурираме чрез ISATAP следене на връзките и измерване на IPv6 трафика.

- Достъпът до определен сървър или приложение може да се контролира със списъци за достъп или с прилагане на определена маршрутизираща политика в комутаторите на обслужващия блок. Такова ниво на контрол позволява достъпа до една или повече IPv6 услуги, като в същото време останалите услуги остават IPv4 до момента на тяхната модернизация или подменяне. Това дава възможност за въвеждане на IPv6 последователно, услуга след услуга.

- Използването на отделна двойка редундантни комутатори в обслужващия блок позволява висока надеждност на ISATAP и ръчно конфигурираните тунели, както и на всички връзки работещи по модела с двоен стек.

- Разполагаме с гъвкави възможности за достъп на хостовете по IPv6 до доставчиците на Интернет услуги (Internet Service Providers – ISP). Първата възможност е да се използват отделни връзки само за Интернет IPv6 трафик. Можем също така да осигурим връзки до комутаторите на ръба на мрежата, след което да използваме съществуващите от там IPv4 и IPv6 канали към Интернет.

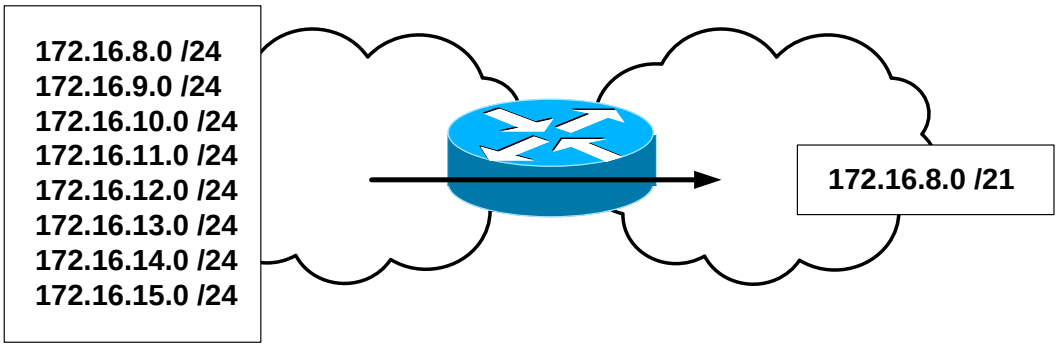
- Използването на модела с обслужващ блок не нарушава съществуващите мрежова инфраструктура и услуги. Поради сходството си със смесения модел, този метод обаче страда от същите недостатъци свързани с използването на тунели. Допълнително тук трябва да добавим и цената на редундантните комутатори в обслужващия блок.

5. Проектиране с модерни методи на маршрутизиране

В този раздел ще разгледаме някои особености на модерните методи на маршрутизиране използващи обобщени маршрути и маршрути по подразбиране, филтриране и преразпределение (redistribution).

5.1 Обобщени и подразбиращи се маршрути

Процедурите за обобщаване на маршрути кондензират информацията за маршрутите. Без обобщаване, всеки маршрутизатор в мрежата трябва да съхранява маршрут до всяка подмрежа. Когато се използва обобщаване, маршрутизаторите могат да сведат някои групи от маршрути до единично рекламиране, като по този начин намаляват както натоварването на маршрутизатора, така и възприемането на сложността на цялата мрежа. Важността на обобщаването на маршрутите се увеличава с нарастването на размера на мрежата, както е показано на Фиг. 1.



Фиг.1 Обобщаване на маршрути

Обикновено към маршрутизиращите протоколи в големите и средни мрежи предявяваме по-големи изисквания отколкото в малките мрежи. Колкото мрежата е по-голяма, толкова по-голямо внимание трябва да отделим на правилното мащабиране на маршрутизиращия протокол. Стабилността, предвидимостта, управлението и сигурността на

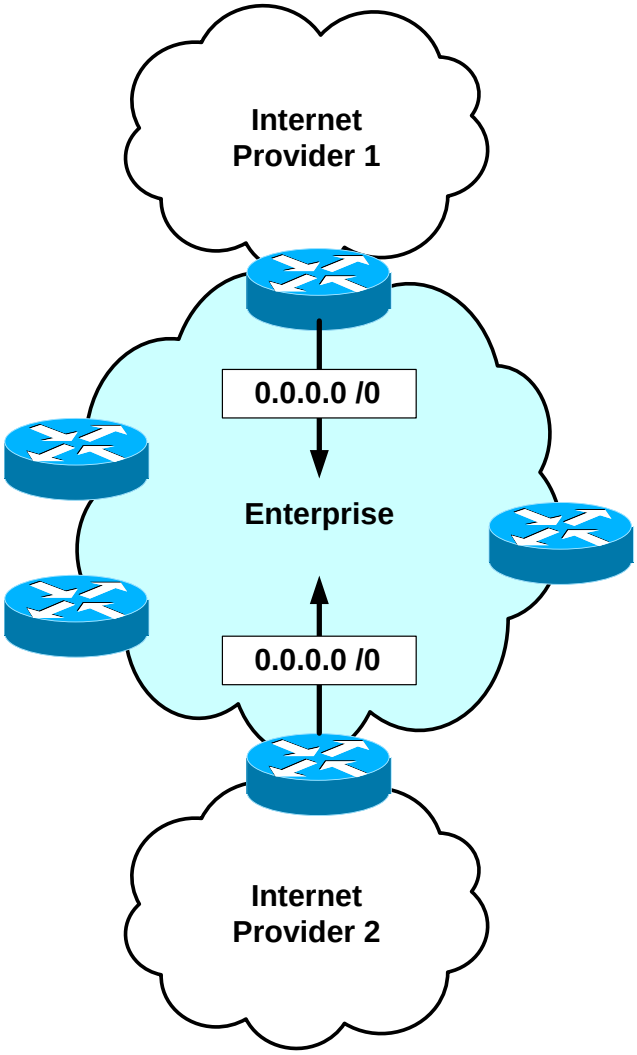
маршрутизирането също са важни. Интегрираните мрежи все повече се използват за IP телефония, съхраняване на данни и друг подобен трафик, чувствителен на пропадане и забавяне. Следователно мрежите трябва да бъдат проектирани така, че възстановяването на маршрутите да става колкото е възможно по-бързо.

Обобщаването на маршрутите е ключов елемент в проектирането на мрежата за получаване на управляемо и бързо сходимо маршрутизиране. Препоръките за използване на такова обобщаване са ясни и включват:

- Използване на обощени маршрути за добро мащабиране на проектите
- Използване на адресни блокове, които магат да бъдат обобщени
- Използване на маршрути по подразбиране където е възможно.

5.1.1 Източник на маршрутите по подразбиране

Понятието за източник на маршрутите по подразбиране е полезно за процеса на обобщаване на маршрутите. Повечето мрежи използват някаква форма на маршрути по подразбиране. Едно интелигентно решение е маршрутът по подразбиране да е (0.0.0.0 /0), който динамично да бъде рекламиран в останалата част от мрежата от маршрутизатор или маршрутизатори които са свързани директно към доставчика на Интернет услуги (ISP). Този маршрут рекламира пътя към всяко местоназначение, което не е намерено в маршрутната таблица, както е показано на Фиг.2.



Фиг.2 Източници на маршрути по подразбиране

Изобщо не е добра идеята да се конфигурират статични маршрути по подразбиране във всеки маршрутизатор, дори когато се използва рекурсивно маршрутизиране. При рекурсивното маршрутизиране, за всеки маршрут в маршрутната таблица, чийто IP адрес на следващия скок не се намира в директно свързан интерфейс на маршрутизатора, маршрутизиращият алгоритъм претърсва рекурсиво маршрутизиращата таблица докато намери директно свързан интерфейс по който да препрати пакетите. Ако конфигурирате статичен маршрут по подразбиране във всеки маршрутизатор към маршрутизатор на ISP, то следващия скок по-скоро е към някой имащ път към ISP маршрутизатор, отколкото към директно свързания граничен маршрутизатор. Този подход може да доведе до появата на черни дупки в мрежата, ако изходната точка се промени или се добави втора връзка към ISP.

Ако използваме ръчно конфигуриране за следващите скокове, то ще трябва да напишем повече конфигурационни команди. Този подход също води до появата на затворени маршрути и при него трудно се правят промени. Ако имаме алтернативни пътища, този статичен подход не позволява да се възползваме от тях.

Препоръчителната алтернатива е да конфигурирате всеки свързан с ISP маршрутизатор със статичен маршрут по подразбиране, и този маршрут да се преразпредели (redistribute) в динамичния маршрутизиращ протокол. Конфигурирането на статичния маршрут по подразбиране се извършва само в мрежовите устройства на ръба на мрежата, т.е. в граничните маршрутизатори. Всички останали маршрутизатори научават за маршрута динамично и изходящият трафик от корпоративната мрежа използва най-близкия изход. Ако свързаният с ISP маршрутизатор изгуби връзката или се повреди, то маршрутът по подразбиране не се рекламира повече в мрежата на организацията.

Може да е необходимо да използвате командата *default-information originate* с множество опции, за да преразпределите маршрутът по подразбиране в динамичния маршрутизиращ протокол. Да отбележим, че точният синтаксис на командата за инжектиране на маршрут по подразбиране във вътрешен маршрутизиращ протокол (Interior Gateway Protocol – IGP) зависи от използвания IGP. Горната команда се използва в RIP, OSPF, IS-IS и BGP. За EIGRP трябва да използваме командата *ip defaultnetwork*.

5.1.2 Междинни райони и маршрути по подразбиране

Изричното формулиране на обобщените маршрути не е единствения начин за постигане на предимствата, които ни дава обобщаването. Различните видове OSPF междинни райони могат да се разглеждат като по-опростена форма на обобщаване. Смисълът на използване на OSPF междинни райони, или както още ги наричат остатъчни области, като stub areas, totally stubby areas, и not-so-stubby areas (NSSA) [4] е да се намали количеството маршрутизираща информация, която се рекламира. Информацията, която се подтиска, се заменя с маршрут по подразбиране 0.0.0.0/0 (IPv4) или ::/0 (IPv6).

OSPF не може да филтрира префиксите в дадена област. Филтрирани са само маршрутите между граничните маршрутизатори Area Border Router (ABR).

Използването на OSPF междинни райони не е приложимо при изграждането на VPN с IPSec и GRE капсулиране в тунелите. В този случай маршрутът по подразбиране 0/0 трябва да бъде насочен към ISP. Една алтернатива на маршрута по подразбиране е да се рекламира обобщен маршрут към организацията като „корпоративен маршрут по подразбиране“ и да се филтрират префиксите в ABR. Понеже OSPF не филтрира маршрутите вътре в областта, то тя ще продължи да бъде наводнявана с рекламирания.

Този подход може да се използва и при EIGRP. За конфигуриране на маршрут по подразбиране използваме командата *ip default-network network-number*. Маршрутизаторът

конфигуриран с тази команда разглежда мрежата записана в нея като кандидат-маршрут при изчисленията на шлюза по подразбиране. Тази мрежа трябва да присъства в маршрутната таблица или като статичен маршрут или като IGP маршрут преди маршрутизаторът да я обяви за кандидат за маршрут по подразбиране на другите EIGRP маршрутизатори. Тя трябва да бъде означена в маршрутната таблица като произлязла от EIGRP мрежа, или да бъде генерирана от статичен маршрут, който е преразпределен в EIGRP.

При EIGRP маршрутът по подразбиране обикновено се конфигурира в ISP точките на свързване. Използват се филтри, така че към отдалечените обекти се изпраща само маршрута по подразбиране и някои други критични префикси. В много WAN дизайни с централизиран достъп до Интернет, главната квартира на корпорацията просто трябва да се рекламира по подразбиране за филиалите като „към останалата част на мрежата или към Интернет“. Ако филиалите имат директен достъп към Интернет, корпоративното обобщаване се свежда до „към останалат част от фирмата“.

При IPSec VPN мрежа свързваща два обекта може да бъде полезно рекламирането на корпоративен обобщен маршрут или маршрут по подразбиране (например 10.0.0.0 /8) към отдалечените офиси. Предимството на това е, че не е необходимо всички останали корпоративни префикси да бъдат рекламирани.

Филтрирането на ненужните навън маршрути спестява честотна лента и процесорно време, които се изразходват за предоставяне на маршрутизираща информация към отдалечените офиси. Това увеличава стабилността и ефективността на мрежата. Отстраняването на бъркотията от маршрутните таблици прави откриването на неизправности по-лесно и ускорява сходимостта.

5.2 Филтриране на маршрути

Филтрирането на маршрутите може да се използва за управление на транспортните потоци в мрежата, като се избегне неподходящия транзитен трафик между отдалечените възли и се осигури защита срещу неточни или неподходящи маршрутни актуализации. В различните протоколи обикновено се използват различни техники на филтриране.

5.2.1 Неподходящ транзитен трафик

Транзитен е външният трафик преминаващ през дадена мрежа или възел. При лошо изградена топология, лошо конфигурирано филтриране и неправилно обобщаване, част от мрежата може да се използва неоптимално, като през нея преминава неподходящ транзитен трафик.

Връзките към отдалечените обекти обикновено са с по-ниска скорост, отколкото скоростта в ядрото на мрежата. Отдалечените обекти рядко са желани като транзитни мрежи за преминаване на трафика от едно място на друго. Те обикновено не могат да обработват такъв обем трафик, какъвто е присъщ на ядрото на мрежата. По принцип, когато свързаността в ядрото е нарушена, трафикът не може да бъде отклонен през отдалечен обект.

При OSPF почти не можем да котролираме вътрешнообластия трафик. Рекламираният LSA не могат да бъдат филтрирани вътре в дадена област. OSPF не позволява трафикът произволно да влиза и след това да излиза от областта. Единственото изключение е област 0, която се използва като транзитна.

При EIGRP може да е желателно да се конфигурират междинни (stub) мрежи. Това информира централните маршрутизатори, че те не могат да използват отдалечените обекти като транзитни мрежи. В допълнение, използването на такива междинни мрежи намалява

ненужните EIGRP заявки като ускорява сходимостта. Филтрирането помага при дефинирането кои части от мрежата са достъпни за транзитен трафик в една EIGRP мрежа и кои не.

При BGP най-често срещаме проблеми с транзитния трафик когато обектът има две връзки към Интернет. Ако няма филтриране, връзките рекламират маршрути. Това рекламиране създава риск за обекта да стане транзитен. Няма проблем, ако двете връзки са към един и същи ISP, поради наличието на номера на автономната система в атрибутите на пътя. Маршрутизаторт на ISP игнорира всички пътища рекламирани от ISP към обекта и след това обратно от него към ISP.

Когато сме свързани към два различни ISP, обектът по невнимание може да се превърне в транзитен обект. Най-добрият подход в този случай, е да се филтрират изходящите маршрутни рекламирания към ISP, като по този начин се гарантира, че се рекламират само маршрути към подмрежите на фирмата. Маркирането на маршрутите като принадлежащи на определена BGP общност е най-лесния начин това да се направи. Всички входящи маршрути получени от ISP трябва също да бъдат филтрирани, така че да одобрявате само маршрутите, които ви изпраща ISP.

5.2.2 Защитно филтриране

Филтрирането на маршрути може да се използва и като защита срещу неправилно или неподходящо маршрутизиран трафик. Един често срещан проблем, с кото някои организации се сблъскват, е че те получават в наследство неподходящ маршрут от друга организация, като например от бизнес партньор. Вашият бизнес партньор не трябва да рекламира вашите мрежи обратно към вас. До тези дестинации не трябва да се достига през партньора. Маршрутът по подразбиране не трябва да стига до партньора, освен ако то не ви осигурява Интернет свързаност.

Неподходящите партньорски рекламирания могат да нарушат маршрутизацията ако не използваме филтриране. Например партньорът може да дефинира статичен маршрут към вашия изчислителен център. Ако такъв маршрут се появи в процеса на вашето маршрутизиране, то част от вашата мрежа може да помисли, че изчислителния център е изнесен в място намиращо се зад маршрутизатора на партньора.

Защитното филтриране предпазва мрежата от некоректни рекламирания от страна на другите. Можете да конфигурирате кои промени на маршрути от страна на партньора трябва да бъдат одобрявани и кои промени трябва да бъдат игнорирани. Например не трябва да се одобряват маршрутни промени сврзани с това как да достигате до собствените си подмрежи или засягащи маршрутизирането по подразбиране.

От съображения за сигурност, към партньора трябва да се рекламират само подмрежите, до които искате той да има достъп. Това захранва партньора с минималната необходима информация за вашата мрежа и е част от т.н. слоест подход за сигурност. То също гарантира, че ако има случайно изтичане на статични или други маршрути на партньора към вашия процес на динамично маршрутизиране, неподходящата информация няма да прехвърли и към другите ви партньори.

Подходът на блокиране на маршрутни рекламирания се нарича маршрутно укриване (route hiding). Трафикът от партньора не може да стигне до укритите мрежи, освен ако имаме в наличност и обощен маршрут. За подобряване на сигурността допълнително трябва да се използват ACL с филтриране на пакетите.

5.3 Проектиране на преразпределението

Преразпределението (redistribution) е мощен инструмент за манипулиране и управление на маршрутните актуализации, особено когато два маршрутизиращи протокола присъстват в мрежата.

В някои случаи маршрутното преразпределение е полезно и дори необходимо. Те включват преминаването от един маршрутизиращ протокол към друг, корпоративните сливания, реорганизациите и поддръжката на устройства, които работят само с RIP или OSPF. Впреки това, преразпределението трябва да се използва с планиране и с известна степен на внимание. При преразпределението лесно могат да бъдат създадени затворени маршрути (rooting loops). Това е особено вярно, когато имаме няколко точки на преразпределение съчетано с използването на статични маршрути, с непоследователни маршрутни обобщения, както и с използването на филтри.

Опитът ни учи, че е много по-добре да имаме различни области от маршрутизиращи протоколи и преразпределение между тях, отколкото да имаме случайна смесица от маршрутизатори и протоколи с някакво специално (ad hoc) преразпределение. Ето защо една корпоративна мрежа, в която се използва EIGRP с преразпределение към RIP и OSPF за областите, в които се използват маршрутизатори на други производители, е напълно работоспособна, стига да и отделим необходимото внимание. От друга страна, произволното смесване на OSPF и EIGRP маршрутизатори и разчитането на някакво специално преразпределение е просто покана за сериозни проблеми.

Когато съществува повече от една точка на свързване между две области, в които се използват различни маршрутизиращи протоколи, обикновено прилагаме двупосочно преразпределение. Когато в двете области имаме съответно OSPF и EIGRP, то препоръчително е да направим преразпределение на OSPF в EIGRP, както и на EIGRP в OSPF.

5.3.1 Филтрирано преразределение

Когато използваме двупосочно преразпределение, трябва да предотвратим обратното рекламиране на информацията в областта или автономната система, от която тя първоначално идва.

Например трябва да използваме филтрите така, че информацията от OSPF, която е преразпределена в EIGRP, да не бъде обратно рекламирана в OSPF. Същото важи и в обратната посока. Това понякога се нарича ръчно разделен хоризонт (manual split horizon). Разделянето на хоризонта е функция на маршрутизиращия протокол. Основната идея тук е, че е контрапродуктивно да рекламирате информация обратно към източника на тази информация, понеже информацията може да бъде остаряла или неточна, и поонеже предполагаме, че източникът на информацията е по-добре информиран.

Ако не направите такова филтриране, или не използвате ръчно разделен хоризонт, то по всяка вероятност след временно прекъсване на работата на мрежата, вие ще установите странна сходимост, зациклени маршрути и най-общо ще изпитате проблеми свързани с нестабилност в маршрутизирането.

И двата протокола, EIGRP и OSPF, поддържат маркиране на маршрутите. Можем да използваме маршрутна карта за да добавим цифров маркер към специфични префикси. След това маркерната информация се предава заедно с маршрутните актуализации. Другият маршрутизатор може да филтрира маршрутите които съответстват или несъответстват на маркера. Това се извършва като се използва *route-map* в списъка за преразпределение [5]. Смисълът е да получим информацията директно, а не по странични пътища, където тя може вече да е остаряла.

6. Мигриране между маршрутизиращи протоколи

Съществуват два общи подхода за мигриране между маршрутизиращи протоколи. Единият подход е да се използва административното разстояние (administrative distance - AD). Другит подход е да се използва преразпределение и подвижни граници (moving boundary).

Мигрирането чрез AD не използва преразпределение. Вместо това два маршрутизиращи протокола се изпълняват едновременно с едни и същи маршрути. Това предполага да имаме достатъчно памет, процесорно време и честотна лента.

Първата стъпка при миграцията от един протокол към друг чрез използване на AD е да включим новия протокол, но трябва преди това да се уверим, че той има по-висок AD отколкото работещият протокол, т.е. той няма да е предпочетен. При тази стъпка протоколът се стартира, установяват се съседствата, проверяват се базите данни, но в действителност не се разчита на новия маршрутизиращ ротокол да взима решения за маршрутизиране.

Когато новият протокол е напълно разгърнат, тогава могат да се направят различни проверки използвайки командите *show* с цел да се потвърди правилното внедряване. След това новият протокол трябва да стане с по-нисък AD. Процесът се нарича cutover, и се състои в превключване на протоколите.

Последните стъпки включват следното:

- Проверка на всички префикси научени само от стария протокол
- Проверка за някакви странни следващи скокове. Обикновено тук се използва някаква програма за автоматично сравняване.

При мигрирането чрез преразпределение, процесът е разделен на поредица от малки стъпки. Във всяка стъпка част от мрежата преминава от стария към новия протокол. За да се осигури пълна свързаност в процеса на мигриране чрез преразпределение, граничните маршрутизатори между две части на мрежата трябва двупосочно да преразпределят между протоколите. Филтрирането с маркери може да бъде един прост начин да се направи това. Граничните маршрутизатори се преместват след като част от областта е мигрирала.

7. Литература

[1] Стоилов Емил, Проектиране на корпоративни мрежи. Част I Архитектура, Technical Report, Научен електронен архив на НБУ, 2014, http://eprints.nbu.bg/2219/

[2] Cisco Systems, Inc. Deploying IPv6 in Campus Networks at www.cisco.com/en/US/docs/solutions/Enterprise/Campus/CampIPv6.html

[3] Cisco Systems, Inc. ISATAP Tunnel Support for IPv6 at http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/configuration/xe-3s/ir-xe-3s-book/ip6-isatap-xe.html

[4] Cisco System, Inc. What Are OSPF Areas and Virtual Links at http://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13703-8.html

[5] Cisco Systems, In. Route-Map for IP Routing Protocol Redistribution Configuration at http://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/49111-route-map-bestp.html