



ПРИЛОЖЕНИЕ F

Попълнени таблици за упражняване на планирането

Глава 1

Таблица 1.3 Преглед на конструкцията

Цел на дизайна	Възможни избори за реализация, разглеждани в тази глава
Конструкцията изисква броя на елементите в таблицата на маршрутите на един маршрутизатор да бъде намален.	Обобщаване
Конструкцията изисква използването на протокол за маршрутизация с вектор за разстояние. Идентифицирайте двата подхода, които може да се използват от протокол за маршрутизация с вектор за разстояние за предотвратяване на примките (2).	Split Horizon Poison Reverse
Конструкцията изисква използването на протокол за маршрутизация връзка-състояние (2).	Използване на OSPF. Използване на IS-IS
Конструкцията изисква трафикът IPv6 да преминава от IPv6 адрес източник към най-близкото устройство или няколко устройства, на които е присвоен един и същи IPv6 адрес на получателя.	Използване на предаване до всеки.
Конструкцията изисква използването на NBMA мрежа. Идентифицирайте проблемите в конструкцията, които може да бъдат срещнати при използването на EIGRP или OSPF (2).	Проблем с EIGRP: Split Horizon. проблем с OSPF: Заделян маршрутизатор.
Конструкцията изисква използването на Hot Standby Router Protocol (HSRP). Идентифицирайте условието, което може да бъде създадено, когато връщащият се трафик преминава през маршрутизатор HSRP в покой.	Асиметрично маршрутизиране (или изливане с единично предаване).
Конструкцията трябва да смекчи глобално условие за синхронизация (при което всички TCP потоци едновременно навлизат в бавен старт на TCP).	Използване на WRED.

4 CCNP Routing and Switching ROUTE 300-101 Официално ръководство за...

Цел на дизайна	Възможни избори за реализация, разглеждани в тази глава
Конструкцията изисква една мрежа да бъде преместена към друг протокол за маршрутизация (2).	Конфигуриране на двата протокола за маршрутизиране и използване на Administrative Distance (AD) за контрол на използвания протокол за маршрутизиране. Използване на преразпределение на маршрути, докато преминават през отделните части от мрежата.
Конструкцията изисква вие да виртуализирате няколко маршрутизатора вътре във физически маршрутизатори и да пренасяте трафика за виртуалните мрежи между тези физически маршрутизатори.	Използвайте Cisco Easy Virtual Networking (EVN).

Таблица 1-4 Интересни въпроси към тази глава, които можете да вземете предвид по време на преглед на плана за реализация на колега

Въпрос	Отговори
Планът изисква дезактивирането на Split Horizon за маршрутизатора в главина при топологията главина и спици. Опишете предназначението на Split Horizon.	Split Horizon е свойство, което пречи на обявяването на маршрут, научен по един интерфейс, обратно в същия интерфейс.
Планът изисква използването на EIGRP като протокол за маршрутизация. Осигурете кратко описание на EIGRP.	Enhanced Interior Gateway Routing Protocol (EIGRP) се класифицира като усъвършенстван протокол за маршрутизация с вектор на разстояние. Той беше собственост на Cisco до началото на 2013, но сега е отворен за други производители. EIGRP използва Diffusing Update Algorithm (DUAL) за вземане на решения по селектирането на пътя си.

Въпрос	Отговори
Планът изисква едновременно използване на IPv4 и на IPv6. Какви типове мрежов трафик са общи за IPv4 и на IPv6 и кои типове се различават?	И IPv4, и IPv6 имат единични предавания и множествени предавания. Но IPv4 използва и общи предавания, докато IPv6 не може. Освен това, IPv6 поддържа предавания до всеки, докато IPv4 не го прави.
Планът изисква използването на Hot Standby Router Protocol (HSRP). Какво можете да направите за предотвратяване на проблема с асиметричното маршрутизиране, при което трафикът се предава от подмрежа с използването на активния HSRP маршрутизатор, а част от връщания трафик се връща, като използва изчакващия HSRP маршрутизатор (поради балансиране на натоварването)?	В идеалният случай не би трябвало да разпростирате VLAN върху повече от един комутатор от слой за достъп. Но ако трябва да разтегнете VLAN върху няколко комутатора от слоя за достъп, можете да настроите ARP таймера на маршрутизатора за HSRP, така че да е равен или по-малък на времето на стареене на CAM.
Конструкцията изисква предаване на интерактивен глас и видео по мрежа. Кои протоколи от Слой 4 се използват обикновено за предаване на гласов и видео носител? (2)	Real-time Transport Protocol (RTP) е протокол от Слой 4, който пренася глас и видео носители. RTP е капсулиран вътре в User Datagram Protocol (UDP), който е още един протокол от Слой 4.
Планът изисква мрежата да премине от IPv4 към IPv6. Идентифицирайте три стратегии за успешно мигриране на IPv6. (3)	Проверка на съществуващата апаратура за съвместимост с IPv6. Едновременна работа на IPv4 и IPv6. Проверка на поддържането за IPv6 от страна на ISP.
Планът изисква използването на виртуално маршрутизиране и предаване (VRF). Идентифицирайте два подхода към конфигурирането на VRF. (2)	Традиционен начин за конфигуриране на VRF в маршрутизатори Cisco е подход, наречен VRF-Lite. Един по-нов подход към виртуализираната мрежова конфигурация, наречен Cisco Easy Virtual Network (EVN) значително опростява относително сложната конфигурация, изисквана от VRF-Lite.

Глава 2

Таблица 2.2 Преглед на конструкцията

Цел на дизайна	Възможни избори за реализация, разгледани в тази глава
Конструкцията изисква маршрутизаторите в отделените сайтове да се появят като съседни един на друг, и те са свързани взаимно по мрежа MPLS.	Използвайте MPLS VPN от Слой 2.
Конструкцията изисква маршрутизатори, гранични за потребителя (CE) във всеки сайт на фирмата, които да комуникират по мрежа MPLS и да образуват съседство с маршрутизаторите, гранични за доставчика (PE), към които се свързват.	Използвайте MPLS VPN от Слой 3.
Конструкцията изисква IP трафикът за множество предаване, общо предаване и единично предаване между сайтовете да бъде защитен с VPN.	Капсулирайте IP трафика за множество предаване, общо предаване и единично предаване вътре в GRE тунел, и след това капсулирайте GRE пакетите вътре в IPsec тунел.
Конструкцията изисква спиците в една топология VPN главина и спици да могат динамично да образуват тунели GRE между тях.	Използвайте Dynamic Multipoint VPN (DMVPN).
Конструкцията изисква един тунелен интерфейс GRE да поддържа няколко GRE тунела.	Използвайте многоточков GRE (mGRE).
Конструкцията изисква маршрутизаторите в спиците при конструкция главина и спици да могат да отправят заявки към главината за определяне на IP адреса на физически адрес, отговарящ на далечната страна на тунела.	Използвайте NHRP.
Конструкцията изисква да осигурите конфиденциалност, цялост на данните, удостоверяване и защита против повторение за трафик за единично предаване, преминаващ по VPN.	Използвайте IPsec.

Таблица 2-3 Интересни въпроси към тази глава, които можете да вземете предвид по време на преглед на плана за реализация на колега

Въпрос	Отговори
Планът изисква използването на технология MPLS VPN за взаимна връзка на отдалечени сайтове. От кои общи категории на MPLS VPN бихте могли да избирате? (Изберете две.)	MPLS VPN Слой 2, MPLS VPN Слой 3.
Планът задължава използването на MPLS VPN от Слой 3. Кой протокол за маршрутизация вероятно ще използва доставчикът на услуги за размножаване на информацията за маршрута от маршрутизатор в покрайнините на клиента (CE) от единия сайт към маршрутизатор CE в другия край?	Многопротоколен BGP (MP-BGP).
Планът изисква използването на тунел GRE. Кои протоколи можете да изпращате по GRE тунел?	Тунелът GRE поддържа всички протоколи от Слой 3 (включително IP трафик от единично, общо и множествено предаване).
Планът изисква използването на Dynamic Multipoint VPN (DMVPN). Какви технологии за VPN са нужни за поддържането на DMVPN? (Изберете три.)	Multipoint GRE (mGRE), Next Hop Resolution Protocol (NHRP), IPsec
Планът изисква един маршрутизатор в главината при топология главина и спици да има четири GRE тунела към отдалечените сайтове. Ако използвате mGRE, колко на брой интерфейси трябва да бъдат конфигурирани в маршрутизатора в главината за поддържане на четирите тунела GRE?	Един
Планът изисква използването на NHRP в топология главина и спици за VPN. Кой маршрутизатор, или маршрутизатори, в тази топология ще съдържа базата данни NHRP?	Маршрутизаторът в главината.
Планът изисква използването на IPsec. Какви са режимите на работа на IPsec? (Изберете два.)	Транспортен режим, тунелен режим

Таблица 2-4 Тренировка на паметта за план за реализация на конфигурацията

План	Команди за конфигурация/Бележки
Създайте интерфейс за виртуален тунел GRE (в глобален режим на конфигуриране).	interface tunnel <i>id</i>
Задайте IP адрес на тунела GRE (в режим конфигуриране на интерфейса).	ip address <i>ip_address subnet_mask</i>
Посочете източника на тунела GRE (в режим на конфигуриране на интерфейса).	tunnel source <i>{interface_id ip_address}</i>
Посочете получателя на тунела GRE (в режим на конфигуриране на интерфейса).	tunnel destination <i>ip_address</i>

Таблица 2-5 Тренировка на паметта за план за потвърждаване

Необходима информация	Команда(и)
Потвърдете състоянието на интерфейса и капсулирането на един GRE тунел.	show interface tunnel <i>id</i>
Потвърдете, че маршрутизаторът вижда далечния край на тунела GRE като разположен на един скок разстояние, въпреки че може да се преминава през няколко маршрутизатора за достигане на другия край на тунела.	traceroute <i>ip_address_of_far_side_of_tunnel</i>

Глава 3

Таблица 3-14 Преглед на конструкцията

Цел на дизайна	Възможни избори за реализация, разгледани в тази глава
Една конструкция за IPv6 предлага всички хостове клиенти да научават динамично своите IPv6 адреси. Кои инструменти може да се използват? (2)	ДНСР с пълно състояние Автоматична конфигурация без състояние

Цел на дизайна	Възможни избори за реализация, разгледани в тази глава
Един план показва използването на автоматична конфигурация без състояние. Изпълнението на коя функция трябва да очакваме от DHCP IPv6 сървъра?	Да бъдат предоставени IPv6 адресите на DNSv6 сървъра.

Таблица 3-15 Интересни въпроси към тази глава, които можете да вземете предвид по време на преглед на плана за реализация на колега

Въпрос	Отговори
План за реализация посочва, че IPv6 адресите на един маршрутизатор трябва да имат присвоени очевидни стойности, като се използват най-ниските числа в интервала за всяка присвоена представка. Какви методи за конфигурация биха могли да бъдат използвани за конфигурирането на тези ниски стойности на адресите?	Статично конфигуриране на целия адрес с командата ipv6 address . Конфигуриране на MAC адреса като нисък номер, и конфигуриране на адреса с командата ipv6 address eui-64 .
Един план изисква използването на автоматична конфигурация без състояние за хостовите клиенти. Какво трябва да бъде конфигурирано в маршрутизаторите за поддържането на този процес?	Маршрутизаторите трябва да отговарят на съобщенията Router Solicitation с Router Advertisement (RA). За да го направи, един маршрутизатор трябва да има активирано маршрутизиране IPv6 и конфигуриран IPv6 адрес за единично предаване в интерфейса, в който е получено RS.
Един план за реализация на RIPng извежда два съседни маршрутизатора с IPv6 адреси за единично предаване 2000::1/64 и 2001::2/64, съответно. Ще предизвика ли това проблеми в съседството?	Не; IPv6 не използва концепцията за съседни, но освен това и не пречи на размяната на маршрути.

Таблица 3-16 Тренировка на паметта за план за реализация на конфигурацията

Свойство	Команди за конфигурация/ Бележки
Глобално активиране на маршрутизирането за трафик IPv6 за единично предаване.	ipv6 unicast-routing

10 CCNP Routing and Switching ROUTE 300-101 Официално ръководство за...

Свойство	Команди за конфигурация/ Бележки
Глобално активиране на Cisco Express Forwarding (CEF) за IPv6.	<code>ipv6 cef</code>
Конфигуриране на маркировка с етикет на потока в пакети от 1280 и повече байта, изпратени от маршрутизатора.	<code>ipv6 flowset</code>
Конфигуриране на целия глобален адрес за единично предаване в интерфейс.	interface <i>type-number</i> ipv6 address <i>address/prefix length</i>
Конфигуриране на представката IPv6 за единично предаване в интерфейс, и оставяне на маршрутизатора да добави идентификатор на интерфейса.	interface <i>type-number</i> ipv6 address <i>address/prefix length eui-64</i>
Конфигуриране на интерфейс, така че да намери своя IPv6 адрес за единично предаване с използване на автоматично конфигуриране без състояния.	interface <i>type-number</i> ipv6 address autoconfig
Конфигуриране на интерфейс за активиране на IPv6 и използване на IPv6 адреса на друг интерфейс при нужда.	interface <i>type-number</i> ipv6 unnumbered <i>type number</i>
Активиране на IPv6 в интерфейс, като не се конфигурира IPv6 адрес за единично предаване.	interface <i>type-number</i> ipv6 enable
Конфигуриране на локален за връзката адрес в интерфейс.	interface <i>type-number</i> ipv6 address <i>address link-local</i>
Като се приеме, че вече са конфигурирани маршрутизиране IPv6 и адреси IPv6, конфигуриране на RIPng.	ipv6 router rip <i>process-name</i> interface <i>type number</i> ipv6 rip <i>process-name enable</i> (Повторете горните две команди за всеки интерфейс.)

Таблица 3-17 Тренировка на паметта за план за потвърждаване

Необходима информация	Команда(и)
Всички маршрути IPv6	show ipv6 route
По един ред за всеки IPv6 адрес	show ipv6 interface brief
Подробна информация за IPv6 в интерфейс, включително адресите за множество предаване.	show ipv6 interface [type number]
Адресите MAC, използвани от интерфейс.	show interfaces [type number]
Адресите MAC на съседните IPv6 хостове.	show ipv6 neighbors
Информацията, научена от друг маршрутизатор в съобщение RA.	show ipv6 router
Всички IPv6 маршрути, научени от RIP.	show ipv6 route rip
Всички адреси IPv6 на следващ скок, използвани от маршрути RIP	show ipv6 rip next-hops
Интерфейсите, в които е активиран RIP.	show ipv6 protocols

Глава 4

Таблица 4-5 Преглед на конструкцията

Цел на дизайна	Възможни избори за реализация, разглеждани в тази глава
Подобрейте конвергенцията на EIGRP.	Настройване на таймерите EIGRP Hold и Hello така, че отказите на съседите се разпознават по-бързо.
Реализирайте EIGRP на всеки маршрутизатор, така че да се образуват съседства (2).	Откриване на съседи с използване на множествени предавания като резултат на съпоставянето на интерфейс с командата EIGRP network , в режим за конфигуриране на EIGRP в маршрутизатора. Позволяване само на конкретни съседи в интерфейс чрез конфигурирането на командата neighbor в режим за конфигуриране на EIGRP в маршрутизатора.

Цел на дизайна	Възможни избори за реализация, разглеждани в тази глава
Ограничете образуването на съседства в интерфейси, съпоставени с командата network на EIGRP (3)	<p>Използване на удостоверяване EIGRP за позволяване само на съседи с правилни ключове.</p> <p>Предотвратяване на всички съседства в един интерфейс чрез превръщане на интерфейса в пасивен.</p> <p>Позволяване само на конкретни съседи в интерфейс чрез конфигуриране на статичен съсед.</p>

Таблица 4-6 Интересни въпроси към тази глава, които можете да вземете предвид по време на преглед на плана за реализация на колега

Въпрос	Отговор
Какво се случва в интерфейс на комутатор, в който командата network на EIGRP съвпада с интерфейса? (2)	<p>EIGRP се опитва да открие съседите EIGRP чрез изпращане и получаване на EIGRP Hello с множествени предавания.</p> <p>EIGRP обявява подмрежата в свързания интерфейс.</p>
Какви настройки на конфигурацията пречат на откриването на съседи в EIGRP при интерфейс с активиран EIGRP? (2)	<p>Статична конфигурация на поне един съсед в този интерфейс.</p> <p>Конфигуриране на интерфейса като пасивен.</p>
Кои настройки на конфигурацията пречат на всички съседства в интерфейс с активиран EIGRP?	<p>Конфигуриране на интерфейса като пасивен.</p>
Какви настройки проверяват потенциалните съседи преди да станат съседи по EIGRP? (5)	<p>Дали IP адресът на съседа е в същата първична подмрежа, както локалния маршрутизатор.</p> <p>Отказ на удостоверяване за EIGRP.</p> <p>ASN в командите router eigrp asn трябва да съвпадат.</p> <p>Интерфейсите не могат да бъдат пасивни.</p> <p>Конфигурираните K-стойности трябва да съвпадат.</p>

Въпрос	Отговор
Какви настройки, които по ваше мнение биха могли да се отразят върху съседските отношения EIGRP, в действителност не предотвратяват съседство? (3)	Несъвпадащи настройки на таймерите Hello и Hold. Дублирани идентификатори на маршрутизатори. Несъвпадение на IP MTU.

Таблица 4-7 Тренировка на паметта за план за реализация на конфигурацията

План	Команди за конфигурация/Бележки
Активиране на EIGRP в интерфейси	router eigrp <i>autonomous-system</i> network <i>network-number [wildcard-mask]</i>
Настройка на таймери Hello и Hold	ip hello-interval eigrp <i>as-number timer-value</i> ip hold-time eigrp <i>as-number timer-value</i>
Пасивни интерфейси	passive-interface <i>type number</i> passive-interface default no passive-interface <i>type number</i>
Статични EIGRP съседни	neighbor <i>a.b.c.d interface</i>
K-стойности	metric weight 0 <i>k1 k2 k3 k4 k5</i>
Идентификатор на маршрутизатор EIGRP	eigrp router-id <i>a.b.c.d</i>

Таблица 4-8 Тренировка на паметта за план за потвърждаване

Необходима информация	Команда(и)
Маршрути, които са били добавени към таблицата за IP маршрути от EIGRP.	show ip route eigrp
Всички маршрути в таблицата за маршрутите на маршрутизатор.	show ip route
Конкретен маршрут за един адрес на получател или подмрежа.	show ip route <i>ip-address [mask]</i>

14 CCNP Routing and Switching ROUTE 300-101 Официално ръководство за...

Необходима информация	Команда(и)
Списък на всички (и статично конфигурирани, и динамично открити) съседни на EIGRP.	show ip eigrp neighbors show ip eigrp neighbors detail
Маркиране дали един съсед е бил динамично открит или статично конфигуриран.	show ip eigrp neighbors detail
Списък на статистиките по отношение на броя на EIGRP съобщенията, изпратени и получени от маршрутизатор.	show ip eigrp interfaces show ip eigrp interfaces detail
Списък на интерфейсите, в които EIGRP е бил активиран (благодарение на командата EIGRP network).	show ip eigrp interfaces show ip eigrp interfaces detail show ip eigrp interfaces type number
Списък на броя на EIGRP колеги, познати през даден интерфейс.	show ip protocols show ip eigrp neighbors [detail]
Времето, изтекло след образуването на съседство.	show ip protocols
Конфигурираният таймер Hello за интерфейс.	show ip eigrp interfaces detail [type number]
Конфигурираният таймер Hold за интерфейс.	show running-config
Текущият действителен таймер Hold за съсед.	show ip eigrp neighbors [detail]
EIGRP ASN на маршрутизатор.	show ip protocols show ip eigrp traffic show ip eigrp accounting
Списък на пасивните интерфейси на EIGRP.	show ip protocols
Списък на непасивните интерфейси на EIGRP.	show ip eigrp interfaces [detail]
Списък на K-стойностите на EIGRP.	show ip protocols
Списък на статистиката за трафика за EIGRP.	show ip eigrp traffic
EIGRP идентификатор на маршрутизатор.	show ip eigrp topology show ip eigrp accounting

Глава 5

Таблица 5-8 Преглед на конструкцията

Цел на дизайна	Възможни избори за реализация, разгледани в тази глава
Ограничава консумацията на IP подмрежи в конструкция WAN Frame Relay.	Използвайте многоточкови подинтерфейси, с повече от два маршрутизатора, които поделят една и съща WAN подмрежа.
При относително бавна WAN Frame Relay, защитава срещу консумиране на прекалено много широчина на лентата с претоварен трафик EIGRP.	Използвайте EIGRP WAN свойството за контрол на широчината на лентата за ограничаване на количеството широчина на лентата, консумирано от EIGRP.
Планира промяна на широчината на лентата от 1X CIR в 2X CIR във всички подинтерфейси на Frame Relay.	Променете метриците и със закъснение, за да гарантирате избирането на правилните най-добри пътеки плюс резервни пътеки, които са вероятни наследници там, където е възможно.
Планира да зададе широчината на лентата като стойности, различни от действителните скорости на интерфейса, за да манипулира метриците EIGRP.	Попитайте дали конструкцията не би могла да използва закъснение вместо това.
Тази цел за гарантиране на вторични маршрути EIGRP за всички отдалечени маршрутизатори не изисква Query за конвергенция.	Променете метриците с използване на закъснение или списъци за отместване, така че вторичните маршрути да са маршрути FS.
Какви инструменти можем да използваме, за да отговорим на целта за бърза конвергенция на конструкцията? (Четири елемента)	<p>Променете метриците така, че да съществуват маршрути вероятни наследници.</p> <p>Промяна на подходящи маршрути в крайни EIGRP маршрути.</p> <p>Използване на многопътност с различна цена за добавяне на множество маршрути към таблицата за маршрутите.</p> <p>Използване на обобщаване на маршрутите за ограничаване на обхвата на заявката.</p>
R1 и R2 ще обявят един и същи обобщен маршрут; гарантирайте, че R1 е предпочитаната EIGRP пътека за това обобщение.	Промяна на метриката на EIGRP така, че всички метрики на R2 за подчинените маршрути са по-високи от метриката на най-добрия подчинен маршрут на R1.

Цел на дизайна	Възможни избори за реализация, разгледани в тази глава
Попречете на крайните маршрутизатори по местата за един отдел в компанията да научат маршрутите към подмрежи в друг отдел.	Използвайте филтриране на маршрута по EIGRP (списъци на разпределение).
Винаги гарантирайте, че с всеки маршрут се поема по най-късия път.	Избягвайте използване на обобщаващи маршрути.

Таблица 5-9 Интересни въпроси към тази глава, които можете да вземете предвид по време на преглед на плана за реализация на колега

Въпрос	Отговори
Многоточков интерфейс Frame Relay, с присъединени 20 PVC, има конфигурация за 10 процента от широчината на лентата, която ще бъде използвана за EIGRP. Какво количество е отделено за всяка PVC?	Cisco IOS първо разделя широчината на лентата на подинтерфейса на 20 (броят на PVC) и след това отнема 10% (според конфигурацията).
Конфигурация посочва командата no ip split-horizon . Кога това би имало значение?	Тази команда засяга използването на Split Horizon от RIP, и не е за EIGRP, така че вземете предвид използвания протокол за маршрутизиране.
Планът изисква задаване на всички K-стойности на EIGRP като 1. Какъв отрицателен ефект би имало това върху маршрутите в IP таблицата на маршрути?	Хлопане на маршрут.
Конфигурацията използва списъци за отместване. Ще повлияе ли това на изчисляването на FD и/или RD?	И на двете.
Планът показва примерна конфигурация, мигрираща интерфейс от закъснение 20 към закъснение 200. С колко ще се повиши метриката?	Подкомандата от интерфейса delay и формулата за метриките използват единица десетки микросекунди. В този случай, закъснението е с още 180, и след това е умножено по 256, за общ резултат 4608. (Забележка: Не се притеснявайте, ако отговорът ви в този случай не е бил толкова подробен.)

Въпрос	Отговори
Планът посочва изключително използване на частни мрежи от Клас C вътре в голяма фирма. Какъв ефект би могло да има авто-обобщаването на EIGRP?	Автоматичното обобщаване ще накара EIGRP да обяви обобщение за мрежа от Клас C, когато се обявява от интерфейс в различна мрежа от Клас C, което ще доведе до множество обобщаващи маршрути.
Планът показва примерна конфигурация с командата ip summary-address eigrp 1 10.10.0.0 255.255.192.0 5 в маршрутизатор R1. Какви маршрути би трябвало да видят в R1? Какво би било тяхното административно разстояние?	R1 ще посочи 10.10.0.0/22 като обобщен маршрут с AD 5, изходящ интерфейс null0, ако съществува поне един подчинен маршрут. Освен това R1 ще има маршрути за всички подчинени подмрежи в този обхват. Другите маршрутизатори просто ще видят обобщения маршрут, със същото EIGRP AD (90), както останалите вътрешни маршрути.
Планът показва използването на командата <code>variance 4</code> . Какво трябва да бъде конфигурирано за добавяне на други маршрути към таблицата за маршрутите? (два елемента)	Проверете дали броят на максималните пътеки е достатъчно голям за всички маршрути, които искате да включите. Конфигурирайте метриците така, че алтернативните маршрути да бъдат вероятни наследници.
Планът изисква филтрирането на 10.10.10.0/26 и 10.10.12.0/26, но не и на 10.10.11.0/24. Какви инструменти могат да бъдат използвани?	Списъците за разпределение на EIGRP, с представка-списък или маршрут-карта, която сочи към представка-списък за съпоставяне. Може да се използва и ACL, като явно се съпоставя всяка представка.

Таблица 5-10 Тренировка на паметта за план за реализация на конфигурацията

План	Команди за конфигурация/Бележки
Активиране на EIGRP в интерфейси	router eigrp <i>autonomous-system</i> network <i>network-number</i> [<i>wildcard-mask</i>]
Активиране или деактивиране на Split Horizon за EIGRP	[no] ip split-horizon eigrp <i>asn</i>
Задаване на широчина на лентата, консумирана от EIGRP в един интерфейс	ip bandwidth-percent eigrp <i>asn percent</i>

План	Команди за конфигурация/Бележки
Задаване на логическата ширина на лентата на един интерфейс	bandwidth <i>value</i>
Задаване на логическото закъснение на интерфейс	delay <i>value</i>
К-стойности	metric weights <i>tos k1 k2 k3 k4 k5</i>
Конфигуриране на EIGRP списък с отмествания, който съвпада с представка	1. Създаване на IP ACL за съпоставяне на маршрути (различни; разглеждат се като предпоставки). В режим за конфигуриране на EIGRP, конфигурирайте: offset-list <i>{access-list-number access-list-name} {in out} offset [interface-type interface-number]</i>
Конфигуриране на EIGRP списък с отмествания, който съвпада с представка и дължина на представка	Същото както предишния ред от таблицата, но създавате разширен IP ACL, който съпоставя представката с параметъра за ACL IP адрес на източника, и маската с полето за IP адрес на получателя.
Конфигуриране на обобщен маршрут	В интерфейсен режим: ip summary-address eigrp <i>asn prefix subnet-mask [admin-distance]</i>
Активиране и деактивиране на авто-обобщаване	(режим на конфигуриране на EIGRP.) [no] auto-summary
Конфигуриране на балансиране на натоварването с неравна цена	maximum-paths <i>value</i> variance <i>value</i> Промяна на метриците за гарантиране на маршрути вероятни наследници.
Конфигуриране на краен маршрутизатор EIGRP	eigrp stub <i>[[connected] [summary] [static] [redistributed]] [receive-only]</i>
Филтриране на EIGRP маршрути с използване на номерирани ACL	access-list {1-99} {permit deny} subnet-number wildcard-mask router eigrp <i>asn</i> distribute-list <i>acl-number{in out} [interface-type number]</i>

План	Команди за конфигурация/Бележки
Филтриране на EIGRP маршрути с използване на списъци с представки	ip prefix-list [seq <i>sequence-no</i>] <i>list-name</i> [seq <i>seq-value</i>] { deny permit <i>prefix/prefix-length</i> } [ge <i>ge-value</i>] [le <i>le-value</i>] router eigrp <i>asn</i> distribute-list prefix <i>prefix-list-name</i> { in out } [<i>interface-type number</i>]
Активиране на филтрирането на EIGRP маршрути с използване на карти на маршрути	(Създаване на карта на маршрут.) router eigrp <i>asn</i> distribute-list prefix <i>prefix-mdp-name</i> { in out } [<i>interface-type number</i>]
Конфигуриране на маршрут по подразбиране с използването на ip default-network	ip default-network <i>net-id</i>
Конфигуриране на маршрут по подразбиране с използване на статични маршрути	ip route 0.0.0.0 0.0.0.0 <i>outgoing-interface</i>

Таблица 5-11 Тренировка на паметта за план за потвърждаване

Необходима информация	Команда(и)
Съставни стойности на метриките за всички представки на EIGRP.	show ip eigrp topology <i>prefix/length</i>
Извеждане на настройките на EIGRP Split Horizon.	show running-config
Изчисляване на максималната широчина на лентата, която EIGRP ще консумира при физически интерфейс или при интерфейс точка-в-точка.	show interfaces за откриване на широчината на лентата на интерфейса show running-config за откриване на процентната стойност от широчината на лентата за EIGRP

Необходима информация	Команда(и)
Изчисляване на максималната широчина на лентата, която EIGRP ще консумира за всяка PVC в многоточков подинтерфейс Frame Relay.	<p>show interfaces за откриване на широчината на лентата на интерфейса</p> <p>show running-config за откриване на процентната стойност от широчината на лентата за EIGRP</p> <p>show frame-relay pvc interface number-type за откриване на броя на активните PVC, асоциирани с този интерфейс</p> <p>Изчисляване на (широчина на лента на интерфейса/брой PVC) * процентна стойност</p>
Извеждане на увеличаването в RD след реализиране на списък с отмествате EIGRP.	<p>show ip route</p> <p>show ip eigrp topology</p> <p>show ip eigrp topology prefix/length</p>
Извеждане на настройките за широчина на лентата и закъснение на интерфейса.	<p>show ip eigrp topology prefix/length</p>
Извеждане на K-стойностите на EIGRP.	<p>show ip protocols</p>
Откриване на броя на маршрутите наследници и вероятни наследници.	<p>show ip eigrp topology</p> <p>show ip eigrp topology prefix/length</p>
Откриване на всички маршрути, включително и ненаследяващите.	<p>show ip eigrp topology all-links</p> <p>show ip eigrp topology all-links prefix/length</p>
Определяне дали един локален маршрутизатор е краен маршрутизатор.	<p>show running-config</p> <p>show ip protocols</p>
Определяне дали един съседен маршрутизатор е краен маршрутизатор.	<p>show ip eigrp neighbors detail</p>
Извеждане на обобщен IP маршрут.	<p>show ip route</p>
В обобщаващ маршрутизатор, извеждане на EIGRP топологията в обобщен маршрут.	<p>show ip eigrp topology prefix/length</p>
В обобщаващ маршрутизатор извеждане на IP маршрутите за обобщен маршрут и подчинените му маршрути.	<p>show ip route prefix mask longer-prefix</p>

Необходима информация	Команда(и)
В обобщаващ маршрутизатор извеждане на административното разстояние на нулевия маршрут.	show ip route <i>prefix mask</i>
Извеждане на текущата настройка авто-обобщаване.	show ip protocols
Откриване на текущите настройки на променливост и максимални пътеки.	show ip protocols
Извеждане на съобщения всеки път, когато EIGRP отмени обява на представка заради Split Horizon.	debug eigrp packet
Извеждане на списъци на представки.	show ip prefix-list
Извеждане на карти на маршрути.	show route-maps
Определяне дали една представка в таблицата на топологията на EIGRP е била маркирана като кандидат за маршрут по подразбиране.	show ip eigrp topology <i>prefix/length</i> Потърсете стойността на външния флаг.
Определяне дали един IP маршрут е бил маркиран като кандидат за маршрут по подразбиране.	show ip route Потърсете звездичка до маршрута.
Извеждане на предпочитания маршрут по подразбиране на маршрутизатор.	show ip route Потърсете настройката на шлюза за краен случай.

Глава 6

Таблица 6-5 Преглед на конструкцията

Цел на дизайна	Възможни избори за реализация, разгледани в тази глава
Поддържа маршрутизирането на маршрути IPv6 в мрежа, която в момента използва EIGRP за IPv4.	Конфигуриране на EIGRP за IPv6, което позволява на мрежата да продължава да използва EIGRP.

Цел на дизайна	Възможни избори за реализация, разгледани в тази глава
Маршрутизатор в момента има сложна EIGRP конфигурация, с множество свързани с EIGRP команди под различни интерфейси, в допълнение към множество команди за EIGRP под режим за конфигуриране на маршрутизатора. Тази конфигурация трябва да бъде опростена, за да стане по-лесна за разбиране и отстраняване на неизправности.	Заместване на традиционната конфигурация на EIGRP с конфигурация за именуван EIGRP, което обединява всички команди за EIGRP на маршрутизатора под една йерархична структура.

Таблица 6-6 Интересни въпроси към тази глава, които можете да вземете предвид по време на преглед на плана за реализация на колега

Въпрос	Отговори
Част от документацията означава EIGRP за IPv4 като EIGRPv4 и EIGRP за IPv6 като EIGRPv6. Означава ли това, че има „версия 5“ за EIGRP?	Не. Документацията, която означава <i>EIGRP</i> за <i>IPv6</i> като <i>EIGRPv6</i> прави това поради отношенията с IPv6, а не защото това е шесто поколение на EIGRP.
Ако конфигурацията на EIGRP във фирмените маршрутизатори е мигрирала от традиционна конфигурация на EIGRP към конфигурация на Именуван EIGRP, дали мрежовите техници и персонала от техническото обслужване трябва да научат ново множество от команди за потвърждаване и отстраняване на неизправности?	Не. Въпреки че именуваният EIGRP има значително по-различна конфигурация от традиционната конфигурация на EIGRP, командите за удостоверяване (например, командата show) остават едни и същи.

Таблица 6-7 Тренировка на паметта за план за реализация на конфигурацията

План	Команди за конфигурация/Бележки
Активиране на маршрутизиране IPv6.	ipv6 unicast-routing
Активиране на EIGRP за IPv6.	ipv6 router eigrp {1 – 65535}
Активиране на IPv6 в интерфейс, което кара маршрутизатора да извлече локален за връзката адрес за интерфейс.	ipv6 enable

План	Команди за конфигурация/Бележки
Конфигуриране на IPv6 адрес в интерфейс.	ipv6 address <i>address/prefix-length</i> [eui-64]
Активиране на EIGRP за IPv6 в интерфейс.	ipv6 eigrp <i>asn</i>
Конфигуриране на идентификатор на маршрутизатор за EIGRP за IPv6.	eigrp router-id <i>rid</i>
Създаване на виртуален екземпляр за Именуван EIGRP.	router eigrp <i>virtual-instance-name</i>
Посочване на семейство адреси заедно с номер на автономна система.	address-family {ipv4 ipv6} autonomous-system <i>asn</i>
Влизане в режим за конфигуриране Address-Family-Interface.	af-interface {default } <i>interface-id</i>
Влизане в режим за конфигуриране Address-Family-Topology за базова топология.	topology base

Таблица 6-8 Тренировка на паметта за план за потвърждаване

Необходима информация	Команда(и)
Показване на всички IPv4 маршрути, научени от EIGRP.	show ip route
Показване на всички IPv6 маршрути, научени от EIGRP.	show ipv6 route
Показване на променливостта, конфигурирана в EIGRP за автономна система IPv4.	show ip protocols
Показване на променливостта, конфигурирана в EIGRP за автономна система IPv6.	show ipv6 protocols
Показване на интервала Hello за EIGRP за автономна система IPv4.	show ip eigrp interface detail
Показване на интервала Hello за EIGRP за автономна система IPv6.	show ipv6 eigrp interface detail
Извеждане на таблицата за топологията на EIGRP за EIGRP за автономна система IPv4.	show ip eigrp topology [all-links]

Необходима информация	Команда(и)
Извеждане на таблицата за топологията на EIGRP за EIGRP за автономна система IPv6.	show ipv6 eigrp topology [all-links]
Извеждане на изпратени и получени актуализации за EIGRP за автономна система IPv4.	debug ip eigrp notifications
Извеждане на изпратени и получени актуализации за EIGRP за автономна система IPv6.	debug ipv6 eigrp notifications

Глава 7

Таблица 7-7 Преглед на конструкцията

Цел на дизайна	Възможни избори за реализация, разгледани в тази глава
Подобряване на конвергенцията на OSPF.	Променете интервалите Hello и Dead за OSPF така, че отказите на съседите да се разпознават по-бързо.
Реализиране на OSPF във всеки маршрутизатор, така че да се образуват съседства. (2)	Открийте съседите като използвате множествени предавания като резултат на съпоставяне на интерфейс с командата network на OSPF в режим за конфигуриране на маршрутизатор за OSPF Вместо командата network за OSPF, използвайте интерфейлната подкоманда ip ospf process-id area area-id за активиране на OSPF в интерфейс.
Ограничаване на образуването на съседства в интерфейси с активиран OSPF. (2)	Използвайте удостоверяване OSPF, за да позволите само съседите с правилни ключове. Забранете всички съседства в един интерфейс, като направите интерфейса пасивен.

Цел на дизайна	Възможни избори за реализация, разгледани в тази глава
Конструкцията показва клонови маршрутизатори с WAN интерфейси в област 0 и LAN интерфейси в различни области за всеки клон. Каква LSDB информация очаквате да видите в клоновите маршрутизатори?	Клоновите маршрутизатори, които обикновено са по-евтини и не толкова мощни, с по-малко памет, ще трябва да съдържат LSDB за област 0, която може да стане голяма, като се има предвид конструкцията.
План за конструиране на сливане показва две компании с гръбначни области OSPF. Как могат двете области 0 да се свържат? (2)	Физически канали между маршрутизаторите в двете области 0. Виртуален канал.

Таблица 7-8 Интересни въпроси към тази глава, които можете да вземете предвид по време на преглед на плана за реализация на колега

Въпрос	Отговори
Какво става в интерфейс на маршрутизатор, в който командата OSPF network съвпада с интерфейса? (2)	OSPF се опитва да открие съседи OSPF, като изпраща и получава Hello за OSPF с множество предаване. OSPF обявява подмрежата в свързания интерфейс.
Какви настройки на конфигурацията предотвратяват разкриване на съседи OSPF по интерфейс с активиран OSPF?	Конфигуриране на интерфейса като пасивен.
Какви настройки проверяват потенциалните съседи, преди да станат OSPF съседи? (7)	Дали IP адресът на съседа е в същата първична подмрежа, както и локалния маршрутизатор. Отказ на OSPF удостоверяване. Интерфейсът не може да е пасивен. Трябва да бъде в същата област. Интервалите Hello и Dead трябва да съвпадат. Уникални RID. IP MTU трябва да съвпадат.

Въпрос	Отговори
<p>Какви настройки, за които много кандидати за CCNP биха решили, че ще повлияят върху съседските отношения OSPF, в действителност не предотвратяват образуването на съседство?</p>	<p>Несъвпадащи идентификатори на процес в командата router ospf.</p>
<p>Конструкция показва един основен сайт и 100 клона с OSPF и MPLS VPN. Колко на брой OSPF съседства по WAN бихте очаквали да видите в маршрутизатора в централното разположение?</p>	<p>Едно. Всеки маршрутизатор става съсед с маршрутизатора откъм доставчика (PE) вътре в услугата MPLS VPN.</p>
<p>Една конструкция показва основен сайт и 100 клона, с една Frame Relay PVC между основния сайт и всеки от клоновете. Колко на брой OSPF съседства по WAN бихте очаквали да видите в маршрутизатора в централното разположение?</p>	<p>100. Маршрутизаторът от основния сайт образува съседство с всеки клонов маршрутизатор.</p>
<p>Една конструкция показва шест маршрутизатора, свързани в една и съща VLAN и подмрежа. Колко на брой напълно близки съседства OSPF по тази мрежа очаквате да има във всеки маршрутизатор?</p>	<p>DR и BDR ще бъдат напълно близки един с друг и с четирите останали маршрутизатора. Останалите четири маршрутизатора ще бъдат напълно близки само с два маршрутизатора – DR и BDR.</p>
<p>Една конструкция показва един основен сайт и 100 клона, всеки свързан с VPWS услуга. Конфигурацията показва, че маршрутизаторът в централния сайт използва отделен VLAN подинтерфейс за свързване към всеки клон, но клоновите маршрутизатори не разполагат с VLAN, свързваща ги с други клонове. Колко на брой напълно близки OSPF съседства по WAN очаквате да видите в маршрутизатора в централното местоположение?</p>	<p>100. Подинтерфейса за всяка VLAN в основния сайт действа като отделен логически интерфейс. Ще се използват DR и BDR, но в тази конструкция съществуват 100 такива появи, и основният сайт ще стане напълно близък с всичките 100 клона.</p>

Таблица 7-9 Тренировка на паметта за план за реализация на конфигурацията

План	Команди за конфигурация/Бележки
Активиране на OSPF в интерфейс – традиционен метод	router ospf <i>process-id</i> network <i>network-number wildcard-mask area</i> <i>area-id</i>
Активиране на OSPF в интерфейс – с използване на интерфейсни подкоманди	router ospf <i>process-id</i> interface <i>type number</i> ip ospf <i>process-id area area-id</i>
Задаване на интервали Hello и Dead	ip ospf hello-interval <i>timer-value</i> ip ospf dead-interval <i>timer-value</i>
Пасивни интерфейси с подкоманди за маршрутизатор	passive-interface <i>type number</i> passive-interface default no passive-interface <i>type number</i>
OSPF идентификатор на маршрутизатор	router-id <i>a.b.c.d</i>
Създаване на виртуален канал през транзитна област X	router ospf <i>process-id</i> area X virtual-link <i>neighbor-RID</i>

Таблица 7-10 Тренировка на паметта за план за потвърждаване

Необходима информация	Команда(и)
Кои маршрути са добавени към таблицата на IP маршрути от OSPF?	show ip route ospf
Всички маршрути в таблицата за маршрутите на маршрутизатор	show ip route
Конкретният маршрут за един адрес на получател или подмрежа	show ip route <i>ip-address [mask]</i>
Списък на всички (и статични, и динамично открити) OSPF съседни	show ip ospf neighbor show ip ospf neighbor detail

Необходима информация	Команда(и)
Списък на интерфейсите, в които е активиран OSPF	show ip ospf interface show ip ospf interface brief show ip protocols (ако е активиран с интерфейлната подкоманда ip ospf area).
Списък на броя на съседите по OSPF и напълно близките съседни, познати през конкретен интерфейс	show ip ospf interface show ip ospf interface brief show ip ospf interface type number
Времето, изтекло след образуването на съседство	show ip protocols show ip ospf neighbor [detail]
Конфигурираният таймер Hello за интерфейс	show ip ospf interface [type number]
Конфигурираният таймер за интервала Dead за интерфейс	show ip ospf interface [type number]
Текущият действителен таймер Dead за съсед	show ip ospf neighbor [detail]
RID на маршрутизатор	show ip ospf show ip ospf database show ip ospf statistics
Списък на пасивните OSPF интерфейси	show ip protocols
Списък на статистиките за трафика за OSPF	show ip ospf statistics
Извеждане на името и състоянието на виртуален канал	show ip ospf virtual-links show ip ospf neighbor [detail]

Глава 8

Таблица 8-6 Преглед на конструкцията

Цел на дизайна	Възможни избори за реализация, разгледани в тази глава
<p>Конструкцията задава конкретни граници в броя на LSA тип 1 и 2 за всяка област. Опишете как да предскажете броя за всеки тип LSA.</p>	<p>Добавете По Една Тип 1 За Всеки Вътрешен Маршрутизатор В Тази Област.</p> <p>Добавете По Една Тип 1 За Всеки ABR.</p> <p>Добавете по една Тип 2 за всяка подмрежа, в която трябва да бъде избран DR, и за която съществуват два подобни маршрутизатора в тази подмрежа.</p>
<p>Как бихте могли да промените метриките на OSPF така, че да предпочитат канали 10 Gbps вместо 1 Gbps и 1-Gig вместо 100-Mbps? (2)</p>	<p>Конфигурирайте всички маршрутизатори с командата auto-cost reference bandwidth, в режим за конфигуриране на маршрутизатора за OSPF, при поне 10 000.</p> <p>Ръчно конфигурирайте интерфейсите цени за OSPF с интерфейлната подкоманда ip ospf cost cost.</p>
<p>Конструкцията показва една физическа пътека от ABR1 към подмрежа 1 за ядрото вътре в област 0, и една по-дълга пътека през област 1 към същата подмрежа. Какво може да се направи, за да се гарантира възможността за използване и на двете пътеки?</p>	<p>Нищо – ABR1, подобно на всички ABR, игнорира LSA от Тип 3 (подобно на LSA за подмрежа 1), научени в неосновната област (например област 1).</p>

Таблица 8-7 Интересни въпроси към тази глава, които можете да вземете предвид по време на преглед на плана за реализация на колега

Въпрос	Отговори
<p>Какви условия трябва да бъдат верни, за да може един маршрутизатор да създаде/излее LSA тип 2? (2)</p>	<p>Поне два маршрутизатора трябва да бъдат съседи и да са избрали DR.</p> <p>Маршрутизаторът, създаващ LSA, трябва да е DR.</p>

Въпрос	Отговори
Планът показва Frame Relay, при който всички подинтерфейси са точка-в-точка. По подразбиране, ще бъдат ли избрани DR/BDR?	Това е случаят, при който, във Frame Relay, типът по подразбиране точка-в-точка за мрежа OSPF работи отлично. Няма да се избират DR/BDR.
Планът показва планирана промяна на отправната широчина на лентата за всички маршрутизатори с бързи канали, но не и за останалите маршрутизатори. Какви ще са последициите? (2)	Този план нарушава препоръките да се използва една и съща стойност в цялата мрежа. Потенциални последици: <ol style="list-style-type: none"> 1. Настройката на един маршрутизатор променя цената само на този маршрутизатор. 2. Това може да доведе до неправилни избори на маршрут.
Планът показва множество различни скорости на WAN каналите, но широчините на лентите на интерфейса не съвпадат с действителната скорост. Всички промени в цената на OSPF са направени явно с интерфейсната подкоманда ip ospf cost . Дали неправилните широчини на лентата ще причинят някакви проблеми в OSPF?	Няма проблеми за OSPF, който използва интерфейсната цена според ip ospf cost , ако е конфигурирана.

Таблица 8-8 Тренировка на паметта за план за реализация на конфигурацията

План	Команди за конфигурация/Бележки
Променете метриците, като промените формата за изчисляване на цената на OSPF въз основа на широчината на лентата на интерфейса.	router ospf process-id auto-cost reference-bandwidth ref-bw
Променете метриците като промените широчината на лентата на интерфейса.	interface type number bandwidth bandwidth
Променете метриците, като зададете цената директно.	interface type number ip ospf cost cost
Задайте броя на маршрутите с еднаква OSPF цена, позволени в таблицата на маршрутите на един маршрутизатор.	router ospf process-id maximum-paths number

План	Команди за конфигурация/Бележки
Окажете влияние върху избора на DR в LAN. (2)	<p>Конфигурирайте ip ospf priority value в интерфейса.</p> <p>Задайте идентификатор на маршрутизатора в OSPF, като използвайте или подкомандата за маршрутизатор router-id value, като създадете интерфейс за обратна връзка с висок IP адрес или друг интерфейс с висок IP адрес.</p>

Таблица 8-9 Тренировка на паметта за план за потвърждаване

Необходима информация	Команда(и)
Изведете обобщение на базата данни OSPF.	show ip ospf database
Изведете всички LSA тип 1 Маршрутизатор, познати за даден маршрутизатор.	show ip ospf database router
Изведете подробности за конкретна LSA тип 1 Маршрутизатор.	show ip ospf database router <i>lsid</i>
Изведете всички LSA тип 2 Мрежа, познати за даден маршрутизатор.	show ip ospf database network
Изведете подробностите за дадена LSA тип 2 Маршрутизатор.	show ip ospf database network <i>lsid</i>
Изведете всички LSA тип 3 Обобщение, познати за даден маршрутизатор.	show ip ospf database summary
Изведете подробностите за дадена LSA тип 3 Обобщение.	show ip ospf database summary <i>lsid</i>
Изведете списък на OSPF-активираните интерфейси в един маршрутизатор.	show ip ospf interface show ip ospf interface brief show ip ospf interface <i>type number</i> show ip protocols
Определете в кои интерфейси един маршрутизатор е образувал поне едно съседство OSPF.	show ip ospf interface show ip ospf interface brief show ip ospf interface <i>type number</i>

32 CCNP Routing and Switching ROUTE 300-101 Официално ръководство за...

Необходима информация	Команда(и)
Определете броя на напълно близките съседи в един интерфейс.	show ip ospf interface show ip ospf interface brief show ip ospf interface <i>type number</i> show ip ospf neighbor show ip ospf neighbor detail
Определете кои транзитни мрежи се свързват към LSA тип 1.	show ip ospf database router [<i>lsid</i>]
Определете маршрутизатора, който е създаден и излял LSA тип 3.	show ip ospf database show ip ospf database summary
Определете маршрутизатора, който е създаден и излял LSA тип 2.	show ip ospf database show ip ospf database network
Определете маршрутизатора, който е създаден и излял LSA тип 1.	show ip ospf database show ip ospf database router
Изведете IP адреса на текущите DR и BDR в една LAN.	show ip ospf neighbor [detail] show ip ospf interface <i>type number</i>
Изведете цената на интерфейса OSPF (метрика).	show ip ospf database router show ip ospf interface [brief]
Изведете всички маршрути, научени от OSPF.	show ip route ospf
Изведете статистическите данни за броя на изпълненията на алгоритъма SPF.	show ip ospf [statistics]

Глава 9

Таблица 9-5 Преглед на конструкцията

Цел на дизайна	Възможни избори за реализация, разгледани в тази глава
<p>При използване на OSPF, поперечете на маршрутизаторите в разположенията на един отдел от компанията да разберат за подмрежите в друг отдел. (3)</p>	<p>Филтриране LSA Тип 3 в ABR. Филтриране LSA Тип 5 в ABR. Филтриране на маршрутите, добавени от OSPF към таблицата за IP маршрути.</p>
<p>Конструкцията показва фирма, използваща само OSPF. Тя посочва цел по запазване на малък размер на LSDB и таблиците за маршрутите във всяка област. (3)</p>	<p>Използване на ръчно обобщаване на маршрутите в ABR. Използване на LSA филтриране Тип 3. Използване на крайни области.</p>
<p>Конструкцията показва цел за изключително малък размер на LSDB и таблиците за IP маршрути в маршрутизаторите в клоновите офиси. Кой типове крайна област работят най-добре? (2)</p>	<p>Изцяло крайни области. Изцяло NSSA области.</p>
<p>Конструкцията иска изливане на маршрут по подразбиране за целия домейн, за да привлече трафик към свързаните към Интернет маршрутизатори.</p>	<p>Използване на командата default-information originate в маршрутизаторите за Интернет.</p>
<p>Конструкцията изисква маршрутизирането и на мрежи IPv4, и на мрежи IPv6. (2)</p>	<p>Бихте могли да конфигурирате два OSPF процеса, един процес OSPFv2 за поддържане на маршрутизирането на мрежите IPv4 и един процес OSPFv3 (конфигуриран по традиционния начин) за поддържане на маршрутизирането на мрежите IPv6. Като алтернатива бихте могли да конфигурирате една йерархия OSPFv3 Address Family, която включва две семейства адреси, едно за IPv4 и едно за IPv6.</p>

Таблица 9-6 Интересни въпроси към тази глава, които можете да вземете предвид по време на преглед на плана за реализация на колега

Въпрос	Отговори
Планът показва конструкция с област 0, като различни ABR свързват област 0 с областите 1, 2 и 3. Конфигурацията показва филтриране на LSA тип 3 към негръбначните области, но не и в обратната посока. Би ли могла тази конфигурация да филтрира подмрежи в област 1, така че да не се виждат в област 2?	Филтрирането LSA Тип 3 филтрира само подмрежи, чиито LSA Тип 3 биха били създадени от този ABR. Така че ако ABR за област 1-област 0 е създал LSA за подмрежа от област 1, изливайки тази LSA в област 01 ABR за област 0-област 2 не би се опитал да филтрира тази подмрежа с филтриране LSA Тип 3.
Конструкцията показва конфигурация на филтриране на LSA тип 3 във вътрешен маршрутизатор в област 1. Би ли могъл филтърът да има някакъв ефект?	Не. Филтрирането има ефект само върху ABR, за LSA Тип 3, създадено върху този ABR.
Планът показва конфигурация на командата area range в ABR. Каква е метриката за обобщаващия маршрут и при какви условия ABR би обявил обобщението?	Метриката, ако не е посочена с параметъра за цена в командата area range , е най-ниската цена между всички подчинени маршрути. ABR обявява само обобщението, ако съществува поне една подчинена мрежа в този вътрешен за областта маршрут.
Планът показва конфигурацията на командата area1 stub в област, която е разположена в по-голямата си част по Западното крайбрежие на САЩ. Компанията току-що е закупила друга компания, чиито адреси също са по Западното крайбрежие. Какви проблеми съществуват, ако добавите канали от придобитата компания към област 1?	Като крайна област, тази област няма да позволи преразпределянето на външни маршрути. Маршрутите на придобитата компания биха могли, поне първоначално, да се нуждаят от преразпределение в OSPF.
Планът показва конфигурация на командата default-information originate always в този маршрутизатор, към който се свързва каналът към Интернет. Какво става с маршрута по подразбиране, когато каналът към Интернет откаже, и какво се случва с пакетите, предназначени за Интернет, през този период от време?	Тази команда кара маршрутизатора винаги да обявява маршрут по подразбиране, даже и ако маршрутът по подразбиране на този маршрутизатор, насочен към Интернет, откаже. Следователно, всички пакети, насочени навън от фирмата, все пак ще преминават през фирмата към този маршрутизатор, и след това ще бъдат отстранявани.

Въпрос	Отговори
Планът изисква маршрутизиране и на мрежи IPv4, и на мрежи IPv6. Какви нови, или преименувани, типове LSA биха могли да се появят в базата данни за канал-състояние?	С OSPFv3 LSA Тип 3 са преименувани като <i>LSA с междуобластни представки за ABR</i> . LSA Тип 4 са преименувани на <i>LSA с междуобластен маршрутизатор за ABR</i> . Освен това, са въведени две нови LSA: <i>Тип 8 LSA за канали</i> и <i>Тип 9 LSA с вътрешни за областта представки</i> .

Таблица 9-7 Тренировка на паметта за план за реализация на конфигурацията

План	Команди за конфигурация/Бележки
Филтрирайте LSA тип 3, така че да не се изпращат в една област.	(Създайте списък с представки IP) Router ospf process-id area area-number filter-list prefix listname {in out}
Филтрирайте маршрутите OSPF, изчислени от един маршрутизатор, така че да не се добавят към таблицата за маршрутите на този маршрутизатор.	(Създайте списък с представки IP) router ospf process-id distribute-list prefix list-name in
Конфигурирайте обобщаване на маршрут за ABR.	router ospf process-id area area-id range ip-address mask [cost cost]
Конфигурирайте обобщаване на маршрут за ASBR.	router ospf process-id summary-address {ip-address mask prefix mask}
Конфигурирайте OSPF обявяване на маршрут по подразбиране в целия домейн.	router ospf process-id default-information originate [always] [cost metric] [metric-type type]
Конфигурирайте крайни или напълно крайни области.	router ospf process-id area area-number stub (крайните области и напълно крайните области, ако не е ABR) area area-number stub no-summary (напълно крайни области само при ABR) area area-num default-cost cost (незадължително)

План	Команди за конфигурация/Бележки
Конфигурирайте NSSA или напълно NSSA.	router ospf process-id area area-number nssa (NSSA и напълно NSSA, ако не е ABR) area area-number nssa no-summary (напълно NSSA само за ABR) area area-num default-cost cost (незадължително)
Стартирайте процес OSPFv3, като използвате традиционния подход за конфигуриране.	ipv6 router ospf process-id
Инструктирайте интерфейс да участва в област OSPFv3, като използвате традиционния подход за конфигуриране.	ipv6 router ospf process-id area area_number
Започнете процес OSPFv3 с използване на подход за конфигуриране Address Family.	router ospfv3 process-id
Инструктирайте интерфейс да участва в област OSPFv3, като използвате подхода за конфигуриране Address Family.	ospfv3 process-id {ip4 ipv6}

Таблица 9-8 Тренировка на паметта за план за потвърждаване

Необходима информация	Команда(и)
Извеждане на всички IP маршрути за подмрежи в интервал, независимо от дължините на представките.	show ip route subnet mask longer-prefixes
Извеждане на съдържанието на списък с IP представки.	show ip prefix-list [name]
Извеждане на подробности за всички LSA тип 3, познати на един маршрутизатор.	show ip ospf database summary
Извеждане на подробности за всички външни LSA тип 5, познати на един маршрутизатор.	show ip ospf database external
Извеждане на метриката, обявена в обобщен маршрут, създаден от командата area range .	show ip ospf database summary [lsid]

Необходима информация	Команда(и)
Извеждане на метриката, обявена в обобщен маршрут, създаден с командата summary-address .	show ip ospf database external [<i>lsid</i>]
Определете дали един маршрутизатор се намира в крайна област, и ако е така, от какъв тип.	show ip ospf
Потвърдете концепциите на крайна област, като погледнете броя на LSA от тип 3 и тип 5, познати на маршрутизатор.	show ip ospf database database-summary
Посочете интерфейсите, участващи в традиционна конфигурация OSPFv3.	show ipv6 ospf interface brief
Изведете съседите в традиционна конфигурация OSPFv3.	show ipv6 ospf neighbors
Изведете съдържанието на базата данни канал-състояние на маршрутизатор, с използване на традиционна конфигурация OSPFv3.	show ipv6 ospf database
Изведете интерфейсите, участващи в процес по маршрутизиране OSPF IPv4 и/или IPv6, конфигуриран с подхода за конфигуриране Address Family.	show ospfv3 interface brief
Изведете съседите IPv4 и/или IPv6, конфигурирани с подхода за конфигуриране Address Family.	show ospfv3 neighbor
Изведете съдържанието на базата данни канал-състояние на маршрутизатор, с използване на подхода за конфигуриране OSPFv3 Address Family.	show ospfv3 database

Глава 10

Таблица 10-12 Преглед на конструкцията

Цел на дизайна	Възможни избори за реализация, разгледани в тази глава
<p>Една конструкция показва маршрутизатор R1 като свързан и към EIGRP, и към OSPF домейн за маршрутизиране, като всички външни EIGRP маршрути използват конкретно множество от компоненти на метриката EIGRP. Как може да зададете тези метрики? (3)</p>	<p>Задаване на метриците с командата redistribute.</p> <p>Използване на командата default-metric.</p> <p>Задаване на метрика вътре в карта на маршрут, извикана от командата redistribute.</p>
<p>Една конструкция показва маршрутизатор R1 като свързан с два различни EIGRP домейна, с планирано преразпределение. Може ли конструкцията да накара маршрутизаторите да изчисляват метриците въз основа и на присвоената при преразпределянето метрика, и на вътрешната EIGRP топология?</p>	<p>Не се изисква специално действие; това поведение се получава при всички маршрути, преразпределени в EIGRP.</p>
<p>Показана е същата конструкция, както на горния ред, с изключение на описанието дали конструкцията може да накара маршрутизаторите да изчисляват метрики въз основа единствено на компонентите на метриката, присвоени при преразпределение .</p>	<p>Това поведение не се поддържа от EIGRP.</p>
<p>Една конструкция показва маршрутизатор R1 като свързан с два различни OSPF домейна, с планирано преразпределение и всички маршрути, изчислени чрез включване на вътрешно и външно разстояние OSPF.</p>	<p>Маршрутите трябва да бъдат разпределени като маршрути E1, с използване на redistribute ... metric-type 1.</p>
<p>Показана е същата конструкция както предишната, но всички метрики за външни маршрути са основани единствено на външни метрики.</p>	<p>Маршрутите трябва да бъдат разпределени като маршрути E2, с използване на redistribute ... metric-type 2, или с изпускане на ключовата дума metric-type в командата redistribute.</p>

Цел на дизайна	Възможни избори за реализация, разгледани в тази глава
Филтриране на маршрути при преразпределение. (2)	Обръщение към карта на маршрут в командата redistribute . Използване на командата distribute-list , която се обръща към източника на маршрута.
Задаване на различни метрики за различни маршрути, преразпределени от един източник на маршрутизиране.	Използване на опцията redistribute ... route-map .
Задаване на някои маршрути OSPF като E1 и някои като E2 при преразпределяне от един източник на маршрут.	Използване на опцията redistribute ... route-map , с командата set metric-type .
Конструкцията показва много точки на преразпределение с два домейна за маршрутизиране, с необходимост от предотвратяване на примки в домейна. (3)	Задаване на високи стойности на метриците при преразпределение. Задаване на административно разстояние (AD) в преразпределящите маршрутизатори, така че вътрешните маршрути да са по-добри от другите външни маршрути на протокола за маршрутизиране.
Конструкцията показва много точки на преразпределение с повече от два домейна за маршрутизиране, и нужда от предотвратяване на примки в домейна. (3)	Задаване на административно разстояние (AD) за всеки маршрут в преразпределящите маршрутизатори. Филтриране по подмрежа при преразпределение. Филтриране по етикет на маршрут с използване на списъци за разпределение.

Таблица 10-13 Интересни въпроси към тази глава, които можете да вземете предвид по време на преглед на плана за реализация на колега

Въпрос	Отговори
Конструкция показва маршрутизатор R1 като свързан и към EIGRP, и към OSPF домейн за маршрутизация. Кои метрики по подразбиране ще се използват от командата redistribute за всеки протокол за маршрутизиране, ако не са зададени в конфигурацията на R1?	EIGRP – няма метрики по подразбиране OSPF – 20

Въпрос	Отговори
План показва преразпределение между два EIGRP домейна. Какво трябва да се направи, за да се използват оригиналните компоненти на метриката на маршрута източник?	Нищо при преразпределение от EIGRP в EIGRP. Действието по подразбиране, ако метриката не е зададена по някакъв друг начин, използва компонентите на метриката на източника на маршрут.
План показва преразпределение между два домейна OSPF. Какво трябва да се направи, за да се използва оригиналната метрика на маршрута източник?	Нищо при преразпределение от OSPF в OSPF. Действието по подразбиране, ако метриката не е зададена по някакъв друг начин, използва метриката на източника на маршрут.
План показва командата redistribute eigrp 2 за преразпределяне от EIGRP 2 в OSPF. Какви други допълнителни параметри се изискват за гарантиране на преразпределение на 10.1.1.0/24 от EIGRP?	10.1.1.0/24 е подмрежа на класова мрежа, и преразпределението в OSPF се извършва само върху класови мрежи, ако (допълнителната) ключова дума subnets е пропусната в командата redistribute .
R1 има два свързани интерфейса в домейна EIGRP 2 и познава дузини EIGRP маршрути. Планът показва командата redistribute eigrp 2 subnets под процес OSPF. Какво друго трябва да се направи за преразпределение на двете свързани подмрежи вътре в домейна EIGRP?	Нищо – командата redistribute приема маршрутите, научени от маршрутизиращия протокол-източник, плюс свързаните маршрути за интерфейсите, активирани от този протокол.
Конструкция показва домейни за маршрутизация OSPF и EIGRP, с множество преразпределящи маршрутизатори, без очевидна конфигурация за предотвратяване на примки в домейни за маршрутизиране. Какви подразбиращи се стойности на AD съществуват, и как те предотвратяват проблемите?	EIGRP: вътрешно 90, външно 170. OSPF: вътрешно 110, външно 110. Примките в домейни се предотвратяват, тъй като вътрешното 90 на EIGRP е по-малко от външното 110 на OSPF, и вътрешното 110 на OSPF е по-малко от външното 170 на EIGRP.
Същият въпрос както в горния ред, но с домейни RIP и OSPF.	RIP: 120 (за всички) OSPF: вътрешно 110, външно 110. Примките в домейни се предотвратяват, тъй като OSPF предпочита вътрешните маршрути пред маршрутите E1, и маршрутите E1 пред маршрутите E2.

Въпрос	Отговори
<p>Същият въпрос както в предишния ред, но с домейни RIP и EIGRP.</p>	<p>RIP: 120 (за всички).</p> <p>EIGRP: вътрешно 90, външно 170.</p> <p>Примките в домейни се предотвратяват, тъй като вътрешното 90 на EIGRP е по-малко от 120 на RIP, и 120 на RIP е по-малко от външното 170 на EIGRP.</p>
<p>План показва преразпределение между EIGRP и OSPF в два маршрутизатора. Конфигурацията за OSPF в единия маршрутизатор посочва redistribute eigrp 1 subnets и distribute-list 1 out. Ще се опита ли тази конфигурация да филтрира маршрути? Задължителна ли е опцията с карта на маршрут за филтриране при преразпределение?</p>	<p>Конфигурацията е непълна за филтриране. Ако беше използвана командата distribute-list 1 out eigrp 1 (например), с обръщение към източника на маршрута, преразпределените маршрути щяха да бъдат филтрирани. Това е алтернатива на филтрирането с използване на опцията route-map за командата redistribute.</p>
<p>Един частично завършен план показва три различни домейна за маршрутизиране, с множество точки за преразпределение между всяка двойка домейни за маршрутизация. Конфигурацията показва големи ACL, съпоставящи различни подмрежи и задаващи AD за отделните маршрути с използване на командата distance. Какъв алтернативен метод би бил по-лесен за поддържане с промяна на мрежата?</p>	<p>Използването на етикети за маршрути не изисква съвпадение в подмрежите, което би могло да намали количеството необходими с времето промени в конфигурацията.</p>
<p>Планът показва EIGRP за IPv6 и OSPFv3 домейни с взаимно преразпределение. Конфигурацията показва команда redistribute eigrp 1 в процеса OSPF. Какви типове маршрути би трябвало да бъдат преразпределени? И какви типове не?</p>	<p>Конфигурацията преразпределя научените от EIGRP маршрути и свързаните маршрути. Тя няма да преразпредели:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Канално-локални адреси <input type="checkbox"/> Локални маршрути

Таблица 10-14 Тренировка на паметта за план за реализация на конфигурацията

План	Команди за конфигурация/Бележки
Конфигуриране на преразпределение в EIGRP от OSPF (Посочете всички параметри, които можете да си спомните.)	<pre> router eigrp <i>asn</i> redistribute <i>protocol</i> [<i>process-id</i>]<i>as-number</i> [metric <i>bw delay reliability load mtu</i>] [match {internal nssa-external external 1 external 2}] [tag <i>tag-value</i>] [route-map <i>name</i>] </pre>
Конфигуриране на преразпределение в OSPF от EIGRP (Посочете всички параметри, които можете да си спомните.)	<pre> router ospf <i>process-id</i> redistribute <i>protocol</i> [<i>process-id</i>]<i>as-number</i> [metric <i>metric-value</i>] [match {internal external 1 external 2 nssa-external}] [tag <i>tag-value</i>] [route-map <i>map-tag</i>][sub- nets] </pre>
Задаване на метрики по подразбиране за всички команди redistribute , при преразпределяне в EIGRP	<pre> router eigrp <i>asn</i> default-metric <i>bw delay reliability load mtu</i> </pre>
Задаване на метрики по подразбиране за всички команди redistribute , при преразпределяне в OSPF	<pre> router ospf <i>process-id</i> default-metric <i>cost</i> </pre>
Филтриране на маршрути при преразпределяне от OSPF в EIGRP	<p>Примери:</p> <pre> router eigrp 1 redistribute ospf 2 metric 1000 10 255 1 1500 route-map fred route-map fred permit 10 match ip address 1 или router eigrp 1 redistribute ospf 2 default-metric 1000 33 255 1 1500 distribute-list 1 out ospf 2 </pre>

План	Команди за конфигурация/Бележки
Филтриране на маршрути при преразпределяне от EIGRP в OSPF	<p>Примери</p> <pre>router ospf 2</pre> <pre>redistribute eigrp 1 subnets route-map fred</pre> <pre>route-map fred permit 10</pre> <pre>match ip prefix-list barney</pre> <p>или</p> <pre>router ospf 2</pre> <pre>redistribute eigrp 1 subnets</pre> <pre>distribute-list prefix barney out eigrp 1</pre>
Конфигуриране на карта на маршрут, която ще зададе метрични компоненти 1000, 200, 255, 1 и 1500, за маршрутите, разрешени от ACL 1 и филтриране на всички останали маршрути	<pre>route-map fred permit 10</pre> <pre>match ip address 1</pre> <pre>set metric 1000 200 255 1 1500</pre>
Задаване на административно разстояние за OSPF за всички вътрешни маршрути със стойност 110 и за всички външни маршрути със стойност 180	<pre>router eigrp process-id</pre> <pre>distance ospf external 180</pre> <p>(AD вътре в областта и между областите по подразбиране е 110)</p>
Задаване на административно разстояние за EIGRP за всички маршрути, научени от съсед 1.1.1.1, на 190, само за подмрежи в интервала 10.1.0.0 – 10.1.255.255	<pre>router eigrp asn</pre> <pre>distance 190 1.1.1.1 0.0.0.0 list 1</pre> <pre>access-list 1 permit 10.1.0.0 0.0.255.255</pre>
Конфигуриране на RIPv6 за преразпределяне на маршрути от OSPF процес 1, включително подмрежи и свързани маршрути	<pre>ipv6 router rip process-name</pre> <pre>redistribute ospf 1 include-connected</pre>

Таблица 10-15 Тренировка на паметта за план за потвърждаване

Необходима информация	Команда(и)
Извеждане на кратка версия на таблицата на топологията на EIGRP, с изброяване на външните маршрути.	<code>show ip eigrp topology</code>

Необходима информация	Команда(и)
Извеждане на таблицата на топологията на EIGRP, включително маркировка, идентифицираща външните маршрути.	show ip eigrp topology <i>prefix/length</i>
За външни EIGRP маршрути, извеждане на източника на маршрута, външната метрика и IP адреса на маршрутизатора, който е преразпределил този маршрут.	show ip eigrp topology <i>prefix/length</i>
Идентифициране на външни IP маршрути, научени от EIGRP.	show ip route show ip route eigrp
Извеждане на кратка версия на таблицата на топологията на OSPF, с използване на външни LSA тип 5.	show ip ospf database
Извеждане на всички OSPF LSA тип 4.	show ip ospf database asbr-summary
Извеждане на всички OSPF LSA тип 5.	show ip ospf database external
Извеждане на всички OSPF LSA тип 7.	show ip ospf database nssa-external
Извеждане на типа на външния маршрут за OSPF външен маршрут.	show ip ospf database external show ip route ospf
Извеждане на цената на OSPF за всеки интерфейс, накратко.	show ip ospf interface brief
Във вътрешен маршрутизатор, извеждане на цените на всеки ABR от същата област за достигане до някой ASBR.	show ip ospf database asbr-summary
Във вътрешен маршрутизатор, извеждане на най-добрата цена на този маршрутизатор за достигане до ASBR.	show ip ospf border-routers
Извеждане на метриката за всички най-добри в момента външни OSPF маршрути.	show ip route show ip route ospf
Потвърждаване че маршрутите OSPF са били преразпределени от таблица на IP маршрути в таблицата на топологията за EIGRP на същия маршрутизатор.	show ip eigrp topology
Извеждане на броя на съвпаденията в един ACL, използван за филтриране на преразпределението.	show ip access-lists [<i>number-or-name</i>] show access-lists [<i>number-or-name</i>]

Необходима информация	Команда(и)
Извеждане на броя на съвпаденията в списък с IP представки, използван за филтриране на преразпределението.	show ip prefix-list detail [name]
Извеждане на конфигурацията на карта на маршрут.	show route-map [name]
Извеждане на компонентите на метриката за маршрут, преразпределен в EIGRP.	show ip eigrp topology prefix/length
Потвърждаване на отсъствието или наличието на маршрут, който би могъл да бъде преразпределен от OSPF в EIGRP.	show ip eigrp topology prefix/length show ip eigrp topology
Потвърждаване на отсъствието или наличието на маршрут, който би могъл да бъде преразпределен от EIGRP в OSPF.	show ip ospf database prefix/length show ip ospf database
Извеждане на административното разстояние на IP маршрут.	show ip route [subnets]
Извеждане на настройка на административното разстояние за EIGRP.	show ip protocols
Извеждане на настройка на административното разстояние за OSPF.	show ip protocols

Глава 11

Таблица 11-5 Преглед на конструкцията

Цел на дизайна	Възможни избори за реализация, разгледани в тази глава
Дизайнът изисква маршрутизаторите да използват най-ефикасния достъпен метод за комутиране на пакети.	Използване на CEF.
Конструкцията изисква трафикът, предназначен за един от сървърите в подмрежа 10.1.1.0/24, за бъде изпратен по различен маршрут от научения през IGP маршрут за 10.1.1.0/24. (2)	Използване на Policy-Based Routing. Конфигуриране на статичен режим за пакети, изпращани към този отделен сървър.

Цел на дизайна	Възможни избори за реализация, разгледани в тази глава
Същите изисквания, както в горния ред, но само една от подмрежите в хостовите източници би трябвало да има пакети, пренасочени по маршрут, различен от научения през IGP маршрут.	Използване на PBR.
Конструкцията изисква използването на статичен маршрут, но само когато е достъпен конкретен сървър на база данни.	Използване на IP SLA с проследяване на обекти за статичния маршрут.
Конструкцията изисква маршрутизатор на доставчика на услуги да се свързва и да може да комуникира с три маршрута за потребители. (2)	VRF-Lite Сиско EVN

Таблица 11-6 Интересни въпроси към тази глава, които можете да вземете предвид по време на преглед на плана за реализация на колега

Въпрос	Отговори
Планът показва актуализация от по-стар маршрутизатор, който използва Fast Switching с нов маршрутизатор, използващ CEF. Каква е фундаменталната разлика в тези технологии за комутиране на пакети?	При Fast Switching, първият пакет на всеки поток се насочва от процесора на маршрутизатора. Следващите пакети в същия поток след това могат да бъдат предавани въз основа на информацията, научена във Fast Cache. При CEF, всички пакети в потока за данни могат да бъдат насочвани независимо от процесора на маршрутизатора.
План посочва две карти на маршрути PBR – една, която използва ключовата дума default в своята команда set , и друга, която не я използва. Каква е фундаменталната разлика?	Картата на маршрута с ключова дума default ще накара Cisco IOS да опита маршрута за пакета първо както обикновено, и ако не бъде намерен съвпадащ неподразбиращ се маршрут, да използва маршрута в командата set . Без ключовата дума default , Cisco IOS опитва първо маршрута PBR.

Въпрос	Отговори
<p>Един план посочва карта на маршрут, активирана за маршрутизиране с политика, и картата на маршрута съвпада някои пакети с условие deny от картата на маршрута. Какво прави с тези пакети Cisco IOS?</p>	<p>Cisco IOS не насочва тези пакети с PBR и пропуска пакетите през нормалната логика за предаване на пакетите на Cisco IOS. Пакетите не се филтрират.</p>
<p>Документацията на плана показва карта на маршрут PBR с командата set ip dscp ef. Дали PBR поддържа маркиране? И може ли да маркира DSCP?</p>	<p>PBR може да маркира битовете IP Precedence и целия байт ToS, но не може да маркира с използването на стойности DSCP.</p> <p>В наши дни за маркиране на QoS се предпочитат маркировка въз основа на класа.</p>
<p>Планът показва операция IP SLA номер 5, със статичен маршрут, конфигуриран с параметъра track 5. Какви проблеми биха могли да съществуват при свързването между тези команди?</p>	<p>За проследяване на състоянието на операция IP SLA, командата ip route трябва да посочва номер на обекта за проследяване, който на свой ред сочи към номера на операцията на IP SLA.</p>
<p>Конфигурацията IP SLA показва операция IP SLA, използваща ICMP Echo, като IP адрес на получателя е сървър. Какво трябва да се направи в сървъра за поддържане на тази операция?</p>	<p>Нищо – сървърът естествено реагира на ICMP Echo.</p>
<p>Същия сценарий както предишния ред, с изключение на това, че адресът на получателя е в маршрутизатор.</p>	<p>Нищо – маршрутизаторът също така реагира естествено на ICMP Echo.</p>
<p>Същият сценарий като предишния ред, но операцията генерира пакети RTP за измерване на гласовото трептене.</p>	<p>Отдалеченият маршрутизатор трябва да бъде конфигуриран като реагиращ по IP SLA.</p>
<p>Как би могла една конфигурация VRF-Lite в маршрутизатор (конфигурирана с подинтерфейс за всяка VRF) да се свърже към комутатор Cisco Catalyst, докато поддържа изолиран трафика от всяка VRF?</p>	<p>За свързване на интерфейса на маршрутизатора (който е бил разделен на множество подинтерфейси) към комутатора Cisco Catalyst ще се използва канал 802.1Q. Трафикът за всяка VRF ще преминава по отделна VLAN в канала 802.1Q.</p>

Таблица 8-8 Тренировка на паметта за план за реализация на конфигурацията

План	Команди за конфигурация/Бележки
Глобално активиран CEF.	<code>ip cef</code>
Активиране на CEF в интерфейс (ако CEF е глобално активиран).	<code>ip route-cache cef</code>
Конфигуриране на съвпадаща логика в карта на маршрут PBR (2).	route-map name [number] permit match ip address {acl-number acl-name} или match length min max
Конфигуриране на IP адрес на следващ скок в карта на маршрут PBR (2).	route-map name [number] permit set ip next-hop ip-address [... ip-address] или set ip default next-hop ip-address [...ip-address]
Конфигуриране на изходящия интерфейс в една карта на маршрут PBR(2).	route-map name [number] permit set interface type number [... type number] или set default interface type number [... type number]
Активиране на PBR в интерфейс.	interface type number ip policy route-map route-map-name
Активиране на PBR за пакети, създадени от маршрутизатор.	ip local policy route-map route-map-name (глобална команда)
Създаване на VRF.	ip vrf vrf-name
Присвояване на интерфейс или подинтерфейс към VRF.	ip vrf forwarding vrf-name
Влизане в режим за конфигуриране OSPF на маршрутизатор за конкретен екземпляр на VRF.	router ospf process-id vrf vrf-name

Таблица 11-8 Тренировка на паметта за план за потвърждаване-

Необходима информация	Команда(и)
Извеждане на множество статистически данни за интерфейсите, включително информация за режима за комутиране на пакети на интерфейса.	show ip interface <i>interface-id</i>
Извеждане на съдържанието на FIB на маршрутизатори.	show ip cef
Показване на информацията, съдържаща се в таблицата на близост на маршрутизатор, включително информация за протоколите и таймерите.	show adjacency [detail]
Извеждане на интерфейси, в които PBR е активирана и е използвана карта на маршрут.	show ip policy
Извеждане на конфигурацията на карта на маршрут.	show route-map
Генериране на съобщения за отстраняване на бъгове за всеки пакет, който съвпада с PBR.	debug ip policy
Извеждане на конфигурацията на операция SLA.	show ip sla configuration
Извеждане на измерването от операция SLA.	show ip sla statistics
Извеждане на състоянието на проследяващ обект.	show track
Извеждане на изброяване на конфигурирани VRF.	show ip vrf
Извеждане на таблица за IP маршрути за конкретна VRF.	show ip route vrf <i>vrf-name</i>
Използване на ping до IP адрес, намиращ се в конкретна VRF.	ping vrf <i>vrf-name ip address</i>

Глава 12

Таблица 12-4 Преглед на конструкцията

Цел на дизайна	Възможни избори за реализация, разгледани в тази глава
Конструкцията посочва, че интерфейс на маршрутизатор, свързващ се с ISP, ще получи IP адрес, определен от ISP. (2)	Присвояване на статичен IP адрес. DHCP.
Конструкцията посочва, че на устройствата в офис ще бъдат присвоени частни IP адреси, и че тези частни IP адреси ще бъдат транслирани в публично маршрутизирани IP адреси от група адреси, осигурени от ISP. (2)	Динамична NAT (DNAR). Статична NAT (SNAT).
Конструкцията посочва, че на устройствата вътре в офис ще бъдат присвоени частни IP адреси, и че тези частни IP адреси ще бъдат транслирани в един публично маршрутизиран IP адрес, осигурен от ISP.	Транслация на адреси на портове (PAT).

Таблица 12-5 Интересни въпроси към тази глава, които можете да вземете предвид по време на преглед на плана за реализация на колега

Въпрос	Отговори
Планът изисква насоченият към Интернет маршрутизатор на отдалечено местоположение автоматично да бъде конфигуриран със статичен маршрут по подразбиране, насочен към маршрутизатора на ISP. Какъв подход за адресиране би поддържал подобно изискване?	DHCP
NAT има множество описания за различни типове IP адреси. Какъв термин се използва за описание на частните IP адреси, присвоени на устройствата вътре в една мрежа?	Вътрешен локален

Въпрос	Отговори
Една мрежа, използваща NAT, е конфигурирана с множество вътрешни интерфейси. Но планът изисква NAT да се изпълнява върху трафик, който е насочен между вътрешни интерфейси NAT. Кое свойство на NAT би осъществило това?	Виртуален интерфейс на NAT (NVI)

Таблица 12-6 Тренировка на паметта за план за реализация на конфигурацията

План	Команди за конфигурация/Бележки
Присвояване на IP адрес на интерфейс на маршрутизатор, свързан към ISP (в режим за конфигуриране на интерфейс).	ip address <i>ip_address subnet_mask</i>
Конфигуриране на маршрут по подразбиране, сочещ към ISP (в глобален режим за конфигуриране).	ip route 0.0.0.0 0.0.0.0 <i>ip_address_of_isp_router</i>
Инструктиране на интерфейс от Ethernet маршрутизатор да получи IP адрес чрез DHCP (в режим за конфигуриране на интерфейс).	ip address dhcp
Инструктиране на маршрутизатор да не инсталира статичен маршрут по подразбиране въз основа на информацията за шлюза по подразбиране, научена чрез DHCP.	no ip dhcp client request
Създаване на съпоставяна на един или повече вътрешни локални адреси към вътрешен глобален адрес (в глобален режим на конфигуриране).	ip nat inside source static <i>inside_local_address inside_global_address</i>
Заделяне на интерфейс като вътрешен NAT интерфейс (в режим на конфигуриране на интерфейс).	ip nat inside
Заделяне на интерфейс като външен NAT интерфейс (в режим на конфигуриране на интерфейс).	ip nat outside

План	Команди за конфигурация/Бележки
Създаване на ACL за съпоставяне на вътрешни локални адреси, които да бъдат транслирани през NAT (в глобален режим на конфигуриране).	access-list {1-99} epermit network_address wildcard_mask
Дефиниране на NAT група, съдържаща колекция от вътрешни глобални адреси (в глобален режим на конфигуриране).	ip nat pool pool_name starting_ip ending_ip netmask subnet_mask
Асоцииране на ACL, идентифициращ NAT вътрешни локални адреси с група NAT, идентифицираща NAT вътрешни глобални адреси (в глобален режим на конфигуриране).	ip nat inside source list acl pool nat_pool
Асоцииране на ACL, идентифициращ NAT вътрешни локални адреси с външен интерфейс на маршрутизатор и активиране на прехвърляне (в глобален режим на конфигуриране).	ip nat inside source list acl interface outside_interface overload
Конфигуриране на интерфейс за използване на свойството NAT Virtual Interface (NVI) (в режим за конфигуриране на интерфейса).	ip nat enable

Таблица 12-7 Тренировка на паметта за план за потвърждаване

Необходима информация	Команда(и)
Изброяване на интерфейсите на маршрутизатор и техните IP адреси, заедно с индикация дали IP, присвоен на даден интерфейс, е присвоен през DHCP.	show ip interface brief
Извеждане на активните NAT трансляции.	show ip nat translations

Глава 13

Таблица 13-9 Преглед на конструкцията

Цел на дизайна	Възможни избори за реализация, разгледани в тази глава
<p>Конструкцията показва един маршрутизатор, свързан към Интернет, като част от еднодомна конструкция за Интернет. Той посочва раздели за маршрутизиране на фирмата към насочен към Интернет маршрутизатор(и) във фирмата, и друг раздел за избор на маршрути в насочения към Интернет маршрутизатор към Интернет. Посочете опциите, които имат смисъл.</p>	<p>За фирмени маршрутизатори към насочен към Интернет маршрутизатор във фирмата:</p> <ul style="list-style-type: none"> ■ Интернет маршрутизатор за вкарване/изливане на маршрут по подразбиране с IGP. Може да се разположи върху статичен по подразбиране или научен от BGP по подразбиране. <p>За маршрути в насочения към Интернет маршрутизатор, използвайте или</p> <ul style="list-style-type: none"> ■ Статичен по подразбиране ■ Научен от BGP по подразбиране
<p>Използвайте същите критерии, както горната точка в тази таблица, но единичният фирмен маршрутизатор, свързан към Интернет, сега има два канала към един и същи ISP (двудомна).</p>	<p>Същото като горния ред от таблицата за фирмения маршрутизатор към Интернет.</p> <p>За маршрути в насочения към Интернет маршрутизатор:</p> <ul style="list-style-type: none"> ■ Използвайте статични по подразбиране. ■ Използвайте научени от BGP по подразбиране. ■ Приемайте частични или пълни таблици и избирайте най-добрата пътека за всеки получател.

Цел на дизайна	Възможни избори за реализация, разгледани в тази глава
Използвайте същите критерии, както горния елемент, но използвайте два маршрутизатора с по един канал всеки към един и същи ISP (двудомна).	<p>За фирмени маршрутизатори, насочени към обърнатите към Интернет маршрутизатори във фирмата, излизайте маршрутите по подразбиране с IGP от всеки насочен към Интернет маршрутизатор.</p> <p>Същите три опции както предишния ред от тази таблица за маршрути към Интернет. Но ако конструкцията изисква възможност за избор за някои пътеки (маршрути) като по-добри от други с BGP, използвайте iBGP между свързаните към Интернет маршрутизатори, и евентуално с други фирмени маршрутизатори.</p>
Използвайте същите критерии както горния ред, но с единично-многодомна връзка с два маршрутизатора.	Същото като горния ред.
Планът показва използването на публична представка 200.1.1.0/26 от една фирма. Какви методи би трябвало да решите да добавите към плана на реализацията си за обявяване на тази представка към вашите ISP с използване на BGP? (2)	<p>Използвайте командата network за BGP.</p> <p>Преразпределяйте от IGP в BGP.</p>

Таблица 13-10 Интересни въпроси към тази глава, които можете да вземете предвид по време на преглед на плана за реализация на колега

Въпрос	Отговори
Планът показва един маршрутизатор в двудомна конструкция за Интернет, като маршрутизаторът използва BGP във всеки канал към същия ISP. Какви критерии биха се отразили на избора ви за приемане само на маршрути по подразбиране, или на частични актуализации, или на пълни актуализации, с използване на BGP в този случай? (3)	<p>По подразбиране: Ако целта е да се използва една пътека като основна, но да се използва другата пътека, ако първата откаже.</p> <p>Частична: Ако ISP може да определи всеки канал като по-добър канал, като изпраща RA, но за по-малък брой представки.</p> <p>Пълна: Ако всеки канал може да се разглежда като по-добър за повечето от маршрутите BGP.</p>

Въпрос	Отговори
Планът показва четири фирмени маршрутизатора с конфигурация BGP, като два от тези маршрутизатора са с връзки към два различни ISP. Кои връзки са eBGP? Кои са iBGP?	Съседството по BGP между четирите маршрутизатора на фирмата би било iBGP. Всички съседства с маршрутизаторите на ISP биха били eBGP.
Планът показва фирмен маршрутизатор R1 с две паралелни пътеки в Слой 3 към маршрутизатор R2 в ISP, и необходимост за BGP. Какви опции съществуват за високо надеждни колеги по eBGP? (2) Коя е по-добрата?	<p>1. Използвайте интерфейс за обратна връзка като източник на актуализация и конфигурирайте многоскоков eBGP с един BGP колега.</p> <p>2. Използвайте IP адресите на интерфейса за създаване на BGP колеги, но с две съседски отношения с един и същи съседски маршрутизатор.</p> <p>Първата опция намалява количеството на претоварването, като при това дава същата по-голяма достъпност.</p>
Планът за реализация показва фирмен маршрутизатор с връзка eBGP към маршрутизатор на ISP, който използва интерфейс за обратна връзка като източник за Update. Какви други свойства трябва да бъдат конфигурирани, за да работи връзката eBGP?	Многоскоков eBGP.
Маршрутизатор R1 се свързва през eBGP към маршрутизатор I1 в ISP1. R1 има маршрути за 130.1.1.0/24 и 130.1.2.0/24 в своята таблица за маршрути. Конструкцията твърди, че компанията използва като публичен интервал 130.1.0.0/21. Кои методи могат да бъдат използвани за обявяване на един маршрут за целия интервал на колегата по eBGP? (2)	<p>1. Причинява създаването на маршрут в R1 чрез статична конфигурация или обобщаване на маршрута IGP, за 130.1.0.0/21, комбинирано с командата network 130.1.0.0 mask 255.255.248.0 за BGP.</p> <p>2. Преразпределя от IGP в BGP, и след това конфигурира обобщаване на маршрут с ключовата дума summary-only без обявяване на подчинени маршрути.</p>

Таблица 13-11 Тренировка на паметта за план за реализация на конфигурацията

План	Команди за конфигурация/Бележки
Конфигурирайте множество статични маршрути, всеки с различни настройки на административното разстояние.	ip route subnet mask next-hop-ip ad-value (Конфигурирайте два различни маршрута, всеки с различна стойност за AD.)
Конфигурирайте eBGP връзка както следва: локална AS 1, отдалечена AS 2, отдалеченият маршрутизатор използва 1.1.1.1 за колеги по BGP, като 1.1.1.1 е IP адрес в общ канал между маршрутизаторите.	router bgp 1 neighbor 1.1.1.1 remote-as 2
Конфигурирайте връзка eBGP както следва: локална AS 1, отдалечена AS 2, локалната използва loopback1 (1.1.1.1), отдалечената използва loopback2 (2.2.2.2).	router bgp 1 neighbor 2.2.2.2 remote-as 2 neighbor 2.2.2.2 update-source loopback 1 neighbor 2.2.2.2 ebgp-multihop
Деактивирайте административно съседа, конфигуриран в предишните два елемента от тази таблица.	router bgp 1 neighbor 2.2.2.2 shutdown
Активирайте отново съседа, който беше деактивиран в предишния ред от таблицата.	router bgp 1 no neighbor 2.2.2.2 shutdown
Създайте обява на научената по IGP представка 130.1.1.0/24 към съседа, конфигуриран в тази таблица, без преразпределение.	router bgp 1 network 130.1.1.0 mask 255.255.255.0
Повторете задачата от горния ред в тази таблица, но този път с преразпределение на маршрут, като приемете, че за IGP се използва OSPF процес 1.	router bgp 1 redistribute ospf 1

Таблица 13-12 Тренировка на паметта за план за потвърждаване

Необходима информация	Команда(и)
Изведете едноредово състояние на съсед за всеки съсед iBGP.	show ip bgp summary

Необходима информация	Команда(и)
Изведете броя на представките, научени от съсед. (Посочете къде се намира информацията.)	show ip bgp [summary] (Потърсете заглавието „State/PfxRcd“ вядно.) show ip bgp neighbors [neighbor-id] (Потърсете „prefix activity“.)
Изведете броя на представките, обявени към съсед. (Посочете къде се намира информацията.)	show ip bgp neighbors [neighbor-id] (Потърсете „prefix activity“.) show ip bgp neighbors neighbor-id advertised-routes (Потърсете „Total number of prefixes“.)
Изведете локалния и съседния ASN.	show ip bgp summary (Потърсете „Local AS Number“ в горната част.)
Изведете броя на разрешените eBGP скокове.	show ip bgp neighbors [neighbor-id]
Посочете текущите TCP портове, използвани за връзки BGP.	show ip bgp neighbors [neighbor-id] show tcp brief
Изброете всички представки в таблицата BGP.	show ip bgp
Изброете всички най-добри маршрути в таблицата BGP.	show ip bgp
Намерете AS_PATH за всеки елемент от таблицата BGP. (Опишете как.)	show ip bgp (Потърсете заглавието “Path” вядно.)
Определете дали даден елемент от BGP таблицата е научен с iBGP. (Опишете как.)	show ip bgp (Потърсете кода „i“ вляво.) show ip bgp prefix/length (Потърсете „internal“.)
Изведете едноредови елементи за всички елементи от таблицата BGP с дадена представка/дължина, плюс всички подмрежи вътре в този интервал.	show ip bgp prefix/length longer-prefixes
Изброете възможните маршрути по подразбиране.	show ip bgp 0.0.0.0 0.0.0.0

Необходима информация	Команда(и)
Изброете възможните маршрути за пред-ставка.	show ip bgp prefix [subnet-mask]
Изброете маршрутите, научени от един съсед, които са преминали през входящите филтри.	show ip bgp neighbors ip-address routes
Изброете маршрутите, научени от един съсед, преди да бъде приложено някакво входящо филтриране.	show ip bgp neighbors ip-address received-routes
Изведете маршрутите, които са потиснати и добавени към BGP таблицата поради обобщаването (обединяването) на BGP маршрут.	show ip bgp

Глава 14

Таблица 14-10 Преглед на конструкцията

Цел на дизайна	Възможни избори за реализация, разгледани в тази глава
Планът показва типично единично-много-домна конструкция с два маршрутизатора, свързани към два ISP. Как ще гарантирате достигането до следващия скок? (2)	<ol style="list-style-type: none"> 1. Конфигурирайте фирмените маршрутизатори с next-hop-self. 2. Проверете дали и двата BGP маршрутизатора на фирмата имат маршрути за достигане до всички eBGP колеги.
Планът показва същата конструкция както в последния елемент. Двата фирмени маршрутизатора, свързани към Интернет, не разполагат с директна връзка помежду си. Какви методи, разгледани в тази глава, може да се използват за предотвратяване на примки на пакети в ядрото на фирмата? (2)	<ol style="list-style-type: none"> 1. Пуснете мрежа iBGP с основните маршрутизатори на фирмата между свързаните към Интернет маршрутизатори. 2. Преразпределете BGP във вашия IGP, и активирайте синхронизация.

Цел на дизайна	Възможни избори за реализация, разгледани в тази глава
Планът показва същата конструкция както горните елементи, но публичният интервал 200.1.1.0/24 е единственият публичен адресен интервал, използван от фирмата. Как може фирмата да избегне превръщането си в транзитна AS?	Използвайте филтриране за обявяване само на представката 200.1.1.0/24 към ISP.
Окажете влияние върху изходящия маршрут от фирма към представки в Интернет (3).	Задайте административни стойности на Weight, Local Preference и дължина на AS_Path (с използване на предварително добавяне към AS_Path).
Окажете влияние върху изходящия маршрут от фирма към представки в Интернет, така че множество свързани с Интернет фирмени маршрутизатори да правят еднакъв избор въз основа на една и съща информация (2).	Задайте Local Preference и дължина на AS_Path (с използване на предварително добавяне към AS_Path).
Окажете влияние върху входящите маршрути във фирма въз основа на съседни AS (2).	Задайте MED и дължина на AS_Path (с използване на предварително добавяне към AS_Path).

Таблица 14-11 Интересни въпроси към тази глава, които можете да вземете предвид по време на преглед на плана за реализация на колега

Въпрос	Отговори
Планът показва типична единично-многодомна конструкция с два маршрутизатора (R1 и R2), свързани към два ISP. Ще бъдат ли R1 и R2 съседи по BGP? Защо?	R1 може да използва R2 като най-добър маршрутизатор за следващ скок за достигането на определени получатели и обратно, но само ако двата маршрутизатора обменят BGP маршрути, като станат съседи по iBGP.
Планът показва същата конструкция както горния елемент. Каква настройка на конфигурацията трябва да се използва, за да се гарантира, че маршрутизаторите са iBGP, а eBGP колеги?	Командата neighbor remote-as на всеки маршрутизатор се отнася до собствения му ASN, както е конфигуриран в командата router bgp .

Въпрос	Отговори
<p>Планът изисква филтриране на всички представки с изключение на интервала от публични адреси 200.1.1.0/24, когато се обявяват някакви колеги eBGP. Какви опции на командата neighbor съществуват за филтриране въз основа на представката/дължината ? (3)</p>	<ol style="list-style-type: none"> 1. neighbor prefix-list 2. neighbor distribute-list 3. neighbor route-map
<p>Планът показва два фирмени маршрутизатора, R1 и R2, свързани към два различни ISP, с iBGP между R1 и R2. Планът показва задаване на Weight от R1 за маршрути, научени от ISP. Ще реагира ли R2 на тези настройки? Защо да или защо не?</p>	<p>Не. Weight е локално за единичен маршрутизатор и не се обявява към съседните маршрутизатори.</p>
<p>Планът показва два фирмени маршрутизатора, R1 и R2, свързани към два различни ISP, с iBGP между R1 и R2. Планът показва задаване на Local_Pref от R1 за маршрути, научени от ISP. Ще реагира ли R2 на тези настройки? Защо да или защо не?</p>	<p>Да. Local_Pref се обявява за колегите iBGP, така че и R1, и R2 ще направят еднакъв избор въз основа на Local_Pref.</p>
<p>Планът изисква използване на BGP Weight, но непълният план все още не посочва конфигурации. Какви алтернативни конфигурации съществуват? (2)</p>	<ol style="list-style-type: none"> 1. Задаване на Weight за маршрути, съвпадащи в условието на карта на маршрут. 2. Задаване на Weight за всички маршрути, научени от съсед с командата neighbor weight.
<p>Планът изисква използване на BGP Local Preference, но непълният план все още не посочва конфигурации. Каква алтернативна конфигурация съществува?</p>	<p>Задаване на Local Preference за маршрути, съвпадащи в условието на карта на маршрут.</p>
<p>Планът показва два фирмени маршрутизатора, R1 и R2, свързани към различни ISP. Планът изисква използване на MED за повлияване на входящите маршрути. Какви опции за конфигуриране съществуват?</p>	<p>Задаване на MED за маршрути, съвпадащи в условието на карта на маршрут, или изходящи от фирмата, или входящи за ISP.</p>
<p>Планът показва използването на BGP Weight, Local Preference, предварително добавяне към AS_Path и MED за оказване на влияние върху алгоритъма за най-добра пътека. Кое от тях може да бъде зададено и обявено към колеги eBGP?</p>	<p>AS_Path може да бъде с предварително добавяне, и MED може да бъде зададено преди изпращането към съседите eBGP в BGP Updates.</p>

Таблица 14-12 Тренировка на паметта за план за реализация на конфигурацията

План	Команди за конфигурация/Бележки
Конфигуриране на колега iBG	router bgp <i>asn</i> neighbor <i>neighbor-ip remote-as</i> <i>asn</i>
Обявяване на IP адреса на източника на Update за локалния маршрутизатор като адрес за следващ скок за колегите iBGP.	router bgp <i>asn</i> neighbor <i>neighbor-ip next-hop-self</i>
Конфигуриране на мрежа iBGP с колеги 1.1.1.1, 2.2.2.2 и 3.3.3.3.	router bgp <i>asn</i> neighbor 1.1.1.1 remote-as <i>same-as</i> neighbor 2.2.2.2 remote-as <i>same-as</i> neighbor 3.3.3.3 remote-as <i>same-as</i>
Активиране на BGP синхронизация.	router bgp <i>asn</i> synchronization
Конфигуриране на филтриране на маршрути, изпратени към колега eBGP 9.9.9.9, с използването на представка за позволяване само на 200.1.1.0/24.	ip prefix-list <i>plist-name permit</i> 200.1.1.0/24 router bgp <i>asn</i> neighbor 9.9.9.9 prefix-list <i>plist-name out</i>
Конфигуриране на филтриране на маршрути, изпратени към колега eBGP 9.9.9.9, с използването на ACL за позволяване само на 200.1.1.0/24.	access-list 101 permit ip host 200.1.1.0 host 255.255.255.0 router bgp <i>asn</i> neighbor 9.9.9.9 distribute-list 101 out
Конфигуриране на карта на маршрут, която задава Weight.	route-map <i>name permit</i> match ... set weight <i>value</i>
Позволяване на карта на маршрут да зададе BGP Weight.	router bgp <i>asn</i> neighbor <i>neighbor-ip route-map</i> <i>name in</i>
Позволяване на маршрутизатор да зададе BGP Weight за всички маршрути, получени от съсед.	router bgp <i>asn</i> neighbor <i>neighbor-ip weight</i> <i>value</i>
Конфигуриране на карта на маршрут, която задава BGP Local Preference.	route-map <i>name permit</i> match ... set local-preference <i>value</i>

План	Команди за конфигурация/Бележки
Активиране на карта на маршрут за задаване на BGP Local Preference.	router bgp <i>asn</i> neighbor <i>neighbor-ip route-map name in</i>
Конфигуриране на карта на маршрут, която добавя предварително ASN към AS_Path.	route-map name permit match ... set as-path prepend <i>asn1 [asn2] ...</i>
Позволяване на карта на маршрут да извърши предварително добавяне към AS_PATH.	router bgp <i>asn</i> neighbor <i>neighbor-ip route-map name [in out]</i>
Конфигуриране на карта на маршрут, която задава MED.	route-map name permit match ... set metric <i>value</i>
Позволяване на карта на маршрут да задава MED.	router bgp <i>asn</i> neighbor <i>neighbor-ip route-map name [in out]</i>

Таблица 14-13 Тренировка на паметта за план за потвърждаване

Необходима информация	Команда(и)
Извеждане на едноредово състояние на съседни за всички съседни по iBGP.	show ip bgp summary
Определяне дали даден елемент в таблица BGP е научен по iBGP.	show ip bgp (Потърсете код „i“ вляво.) show ip bgp prefix/length (Потърсете “internal”.)
Определяне на IP адреса на следващия скок в научен по iBGP маршрут.	show ip bgp show ip bgp prefix/length
Идентифициране на съсед, от който е научен маршрут BGP.	show ip bgp prefix/length (Потърсете фразата „from ip-address”.)

Необходима информация	Команда(и)
Извеждане на едноредови елементи за всички елементи от BGP таблица с дадена представка/дължина, плюс всички подмрежи вътре в този интервал.	show ip bgp prefix/length longer-prefixes
Извеждане на маршрути BGP, научени от съсед, преди да бъдат обработени от входящ филтър.	show ip bgp neighbors neighbor-ip received-routes
Същото както горния елемент, но след прилагането на входящия филтър.	show ip bgp neighbors neighbor-ip routes
Извеждане на BGP маршрутите, изпратени към съсед, но след прилагането на изходящия филтър.	show ip bgp neighbors neighbor-ip advertised-routes
Извеждане дали съсед може да изпълни опресняване на маршрута BGP.	show ip bgp neighbors [neighbor-ip]
Извеждане на BGP таблица, включително избраната най-добра пътека за всяка представка. (Посочете как да идентифицирате най-добрите пътеки.)	show ip bgp (Потърсете > като втори символ.)
Извеждане по един ред за маршрут BGP, но за представките в даден интервал.	show ip bgp prefix/length longer-prefixes
Идентифициране на BGP Weight за елемент от BGP таблица. (Посочете къде да откриете изходния резултат.)	show ip bgp (Потърсете заглавието "Weight".)
Идентифицирайте BGP Local Preference за елемент от BGP таблица. (Посочете къде да откриете изходния резултат.)	show ip bgp (Потърсете заглавието "LocPrf".) show ip bgp prefix/length (Потърсете "localpref".)
Идентифицирайте BGP дължината на AS_Path за елемент от BGP таблица. (Посочете къде да откриете изходния резултат.)	show ip bgp (Пребройте ASN под заглавието "Path".) show ip bgp prefix/length (Пребройте количеството ASN.)

Необходима информация	Команда(и)
Идентифицирайте MED за елемент от BGP таблица. (Посочете къде да откриете изходния резултат.) (4 метода)	<p>show ip bgp (Потърсете заглавието "Metric".)</p> <p>show ip bgp prefix/length (Потърсете "metric".)</p> <p>show ip route (Потърсете второто число в квадратни скоби.)</p> <p>show ip route prefix-mask (Потърсете "route metric".)</p>
Изведете маршрути, получени от съсед, преди да бъдат обработени от входящ филтър.	show ip bgp neighbors neighbor-ip received-routes
Същото като горния елемент, но след прилагане на изходящ филтър.	show ip bgp neighbors neighbor-ip routes
Изведете BGP маршрутите, изпратени към съсед, но след прилагането на изходящ филтър.	show ip bgp neighbors neighbor-ip advertised-routes
Изведете най-добрите BGP пътеки, които не са добавени в таблицата на IP маршрутите.	show ip bgp rib-failures

Глава 15

Таблица 15-2 Преглед на конструкцията

Цел на дизайна	Възможни избори за реализация, разгледани в тази глава
Конструкцията посочва, че насоченият към Интернет маршрутизатор на клиента трябва динамично да получава IPv6 адрес за своя насочен към Интернет интерфейс от ISP. (4)	<p>Автоматична конфигурация на адреса без състояние (SLAAC)</p> <p>DCHPv6 без състояние</p> <p>DCHPv6 с пълно състояние</p> <p>DHCPv6 Prefix Delegation (DHCPv6-PD)</p>

Цел на дизайна	Възможни избори за реализация, разгледани в тази глава
Конструкцията посочва, че насоченият към Интернет маршрутизатор на клиента обменя маршрути IPv4 и IPv6 с ISP.	Многопротоколен BGP (MP-BGP)
Конструкцията изисква да филтрирате конкретни IPv6 маршрути, изпратени към или получени от ISP.	Списъци с представки (Забележка: Въпреки че при филтрирането на маршрути съществуват и други опции, фокусът на материала за ROUTE е върху използването на списъци с представки.)
Конструкцията има двудомна връзка с Интернет, която използва MP-BGP, с изискване да повлияете върху селектирането на изходящата пътека.	Local Preference (Забележка: Въпреки че за оказване на влияние върху селекцията на изходяща пътека за MP-BGP съществуват и други опции, фокусът на материала за ROUTE е използването на атрибута Local Preference.)

Таблица 15-3 Интересни въпроси към тази глава, които можете да вземете предвид по време на преглед на плана за реализация на колега

Въпрос	Отговори
Планът изисква насоченият към Интернет маршрутизатор на клиента да получи IPv6 адрес от ISP на клиента. Какъв подход към динамично присвояване на IPv6 адреси позволява на насочен към Интернет маршрутизатор да получи един IP адрес от DHCP сървъра на ISP?	DHCPv6 с пълно състояние
Планът изисква използване на IPv6 ACL. Какви два типа трафик са явно позволени от IPv6 ACL? (2)	Neighbor Discovery – Neighbor Advertisements Neighbor Discovery – Neighbor Solicitations

Въпрос	Отговори
<p>Планът изисква използването на MP-BGP. Посочете поне три от новите елементи, въведени от MP-BGP. (3)</p>	<p>Address Family Identifier (AFI)</p> <p>Subsequent Address Family Identifier (SAFI)</p> <p>Multiprotocol Reachable Network Layer Reachability Information (MP_REACH_NLRI)</p> <p>Multiprotocol Unreachable Network Layer Reachability Information (MP_UNREACH_NLRI)</p> <p>BGP Capabilities Advertisement</p>
<p>Планът изисква маршрутизиране и на мрежа IPv4, и на мрежа IPv6 с един ISP. Какъв вариант на BGP поддържа това изискване?</p>	<p>MP-BGP</p>
<p>Планът изисква използване на MP-BGP, конфигуриран по такъв начин, че и маршрутите IPv4, и маршрутите IPv6 могат да бъдат обявявани върху една сесия IPv4 BGP. Какъв допълнителен конфигурационен елемент се изисква за поддържане на този тип конструкция, за разлика от конструкцията, при която маршрутите IPv6 са обявени върху сесия IPv6 BGP?</p>	<p>Карта на маршрут, която описва IPv6 адреса на интерфейса на локалния маршрутизатор като атрибут за следващия скок, който да се обяви към съседа по MP-BGP</p>
<p>Планът изисква използването на атрибута Local Preference за оказване на влияние върху селекцията на изходящи пътеки за мрежа MP-BGP. Предпочитани са по-високите или по-ниските стойности на Local Preference?</p>	<p>По-високи стойности за Local Preference</p>

Таблица 15-4 Тренировка на паметта за план за реализация на конфигурацията

План	Команди за конфигурация/Бележки
Задайте IPv6 адрес на интерфейс на маршрутизатор, свързващ се към ISP (в режим за конфигуриране на интерфейс).	ipv6 address <i>ipv6_address/prefix_length</i>
Конфигурирайте маршрут по подразбиране IPv6, който сочи към ISP (в глобален режим на конфигуриране).	ipv6 route <i>::0 ipv6_address_of_isp_router</i>
Създайте IPv6 ACL (в глобален режим на конфигуриране).	ipv6 access-list <i>name</i>
Приложете IPv6 ACL към интерфейс (в режим на конфигуриране на интерфейса).	ipv6 traffic-filter <i>name [in out]</i>
Активирайте IPv6 маршрутизиране за единично предаване (в глобален режим на конфигуриране).	ipv6 unicast-routing
Създайте карта на маршрут (в глобален режим на конфигуриране).	route-map <i>route_map_name</i>
Посочете IPv6 адреса на интерфейса на маршрутизатор, свързващ се към съсед, като IPv6 адрес на следващия скок (в режим на конфигуриране на карта на маршрут).	set ipv6 next-hop <i>ipv6_address</i>
Дефинирайте автономна система BGP (в глобален режим на конфигуриране).	router bgp <i>as-number</i>
Дефинирайте съсед IPv4 (в режим на конфигуриране на маршрутизатор за BGP).	neighbor <i>neighbor's_ipv4_address remote-as</i>
Влезте в режим на конфигуриране на семейство IPv4 адреси (в режим на конфигуриране на маршрутизатор за BGP).	address-family <i>ipv4</i>
Посочете кой интерфейс(и) ще участва в семейството IPv4 адреси (в режим на конфигуриране на семейство адреси).	network <i>ipv4_address[mask subnet_mask]</i>
Влезте в режим на конфигуриране на семейство IPv6 адреси (в режим на конфигуриране на маршрутизатор за BGP).	address-family <i>ipv6</i>
Посочете кой интерфейс(и) ще участва в семейството IPv6 адреси (в режим на конфигуриране на семейство адреси).	network <i>ipv6_network_address/prefix-length</i>

План	Команди за конфигурация/Бележки
Активирайте BGP съседа за семейство IPv6 адреси (в режим за конфигуриране на семейство адреси).	neighbor <i>neighbor's_ip_address</i> activate
Асоциирайте карта на маршрут със съсед, за да обявите подходящия IPv6 адрес за следващ скок към този адрес (в режим на конфигуриране на семейство адреси).	neighbor <i>neighbor's_ip_address</i> route-map <i>route_map_name</i> out
Дефинирайте съсед IPv6 BGP (в режим на конфигуриране на маршрутизатор за BGP).	neighbor <i>neighbor's_ipv6_address</i> remote-as <i>remote-as</i>
Създайте списък с IPv6 представки (в глобален режим на конфигуриране).	ipv6 prefix-list <i>name seq number</i> [permit deny] <i>ippv6_network/prefix-length</i> { ge le } <i>bits</i>
Приложете списък с IPv6 представки (в режим на конфигуриране на семейство адреси).	neighbor <i>neighbor's_ip_address</i> prefix-list <i>name</i> { in out }
Посочете Local Preference (в режим на конфигуриране на карта на маршрут).	set local-preference <i>value</i>

Таблица 15-5 Тренировка на паметта за план за потвърждаване

Необходима информация	Команда(и)
Изведете ACL (ACL и за IPv4, и за IPv6)	<code>show access-list</code>
Изведете маршрутите IPv6.	<code>show ipv6 route</code>
Изведете мрежите IPv6, познати на BGP.	<code>show bgp ipv6 unicast</code>
Изведете идентификатор на маршрутизатор, локален номер на AS и списък със съседите и номерата на техните AS за BGP в конфигурация MP-BGP.	<code>show bgp ipv6 unicast summary</code>

Глава 16

Таблица 16-7 Преглед на конструкцията

Цел на дизайна	Възможни избори за реализация, разгледани в тази глава
Конструкцията изисква документирана защитна политика на маршрутизатора. (Посочете пет или повече теми за защитата, които обикновено се решават в политиката за защита на маршрутизатор.) (11)	Политиката за защита на маршрутизатор обикновено решава теми за защитата като пароли, удостоверяване, достъп, услуги, филтриране, протоколи за маршрутизиране, архивиране, документация, излишък, наблюдение и актуализация.
Конструкцията изисква сървър за счетоводство (разположен в подмрежа на центъра за данни) да е достъпен само през работно време.	Използвайте почасови ACL.
Конструкцията изисква криптиране на трафика за управление на маршрутизатора.	Използвайте SSH вместо Telnet. Използвайте SNMPv3 вместо SNMPv1 или SNMPv2c.
Конструкцията изисква линейната парола на маршрутизатор да бъде криптирана, така че някой, който е мернал работната конфигурация на маршрутизатора, да няма възможност да прочете някоя от паролите.	Активирайте услугата password-encryption .
Конструкцията изисква насоченият към Интернет интерфейс на маршрутизатора да провери IP адреса на източника на входящ пакет, и да разреши този пакет само ако маршрутът обратно към IP адреса на източника на този пакет се намира във FIB на маршрутизатора, и ако FIB посочва, че изходящият интерфейс за връщане в IP адреса на този източник е същият интерфейс, в който е пристигнал пакета.	Активирайте uRPF в стриктен режим.
Конструкцията изисква удостоверяването на маршрутизатор да бъде обработено от външен сървър. Но ако този външен сървър е недостъпен, заявките за удостоверяване от маршрутизатора трябва да се обработват от базата данни с локални потребители на маршрутизатора.	Активирайте AAA в маршрутизатор. Като част от конфигурацията на AAA, използвайте списък с методи, който посочва сървър TACACS+ или RADIUS като първи избор за удостоверяване и базата данни с локалните потребители на маршрутизатор като резервен механизъм за удостоверяване.

Цел на дизайна	Възможни избори за реализация, разгледани в тази глава
Искате да попречите на нападател да повлияе върху времето на маршрутизатора, в усилие да прекара трафик през почасови ACL.	Накарайте маршрутизаторите да настроят времето си с използване на NTP, и активирайте удостоверяване NTP във всички тези маршрутизатори.

Таблица 16-8 Интересни въпроси към тази глава, които можете да вземете предвид по време на преглед на плана за реализация на колега

Въпрос	Отговори
Планът използва почасови ACL за защита на конкретни сървъри. Какви почасови ACL могат да бъдат конфигурирани в Cisco IOS? (2)	Интервалът от време може да е <i>периодичен</i> , когато се активира или деактивира в определен час или в определени дни от седмицата. Като алтернатива, интервалът от време може да е <i>абсолютен</i> , при което има фиксирана начални и крайни дата и час, през които ACL е активен.
Планът изисква използването на SSH вместо Telnet. Кои два параметъра на маршрутизатора с възможност за конфигуриране се използват при генерирането на ключовата двойка RSA, използвана от SSH?	Името на хоста и името на домейна на маршрутизатора се използват в генерирането на ключовата двойка RSA.
Планът показва използването на различни типове пароли, включително Тип 0, Тип 4, Тип 5 и Тип 7. Каква е разликата в тези типове пароли?	Тип 0 не е криптиран. Парола от Тип 4 е представена със раздробена стойност SHA-256. Парола от Тип 5 е представена с раздробена стойност MD5. Парола Тип 7 е криптирана с използване на шифър на Виженер.
Планът изисква конфигурирането на uRPF. Какви са трите работни режима на uRPF?	uRPF може да работи в <i>стриктен режим</i> , <i>свободен режим</i> или <i>режим VRF</i> .
Планът изисква използването на AAA с външен сървър, който работи с протокол с отворен стандарт. Кой протокол на AAA бихте избрали?	Двата протокола AAA, поддържани от Cisco IOS, включват TACACS+ и RADIUS. Но TACACS+ е фирмен за Cisco, докато RADIUS е протокол с отворен стандарт. Следователно в този случай трябва да бъде избран RADIUS.

Въпрос	Отговори
Въпреки че знаете, че SNMPv3 е по-безопасен от SNMPv2с, планът изисква използването на SNMPv2с в маршрутизаторите ви. Какво можете да направите за по-добра защита на този протокол за мрежово управление? (2)	Ако използвате SNMPv2с в маршрутизатор, вземете предвид настройка на общи нисове само за четене и за четене и запис със стойности, които не са лесни за отгатване. Освен това можете да посочите ACL, който да контролира на кои IP адреси е позволено да комуникират с маршрутизатора с използването на SNMP.
Планът изисква един мрежов маршрутизатор да получава точно време от разположен в Интернет цезиев часовник. Този маршрутизатор след това ще осигури точно време за всички маршрутизатори вътре във фирмата. Ще има ли нужда от конфигурирането на командата ntp master в този маршрутизатор?	Не. Командата ntp master е необходима само ако маршрутизаторът ще осигурява точно време за други устройства, и той използва вътрешния си часовник като свой източник на точно време.

Таблица 16-9 Тренировка на паметта за план за реализация на конфигурацията

План	Команди за конфигурация/Бележки
Създайте именуван часови интервал за ACL (в глобален режим на конфигуриране).	time-range <i>name</i>
Дефинирайте периодичен времеви интервал (в режим за конфигуриране на интервал от време).	periodic <i>days-of-week hh:mm to hh:mm</i>
Дефинирайте абсолютен времеви интервал (в режим за конфигуриране на интервал от време).	absolute [start <i>hh:mm day_of_month month year</i>] end <i>hh:mm day_of_month month year</i>
Приложете интервал от време към номериран ACL (в глобален режим за конфигуриране).	access-list <i>ACL_number</i> < <i>matching_parameters</i> > time-range <i>name_of_time_range</i>
Приложете интервал от време към именуван ACL (в режим на конфигуриране на именуван списък за достъп).	< <i>matching_parameters</i> > time-range <i>name_of_time_range</i>
Посочете име на хост за маршрутизатор.	hostname <i>name</i>

План	Команди за конфигурация/Бележки
Посочете име на домейн за маршрутизатор.	ip domain-name <i>domain_name</i>
Създайте потребител с ниво на привилегии 15 и раздробена парола.	username <i>username</i> privilege 15 secret <i>password</i>
Генерирайте ключова двойка RSA.	crypto key generate rsa modulus <i>size_of_modulus</i>
В режим за конфигуриране на VTY линия, разрешете само връзки по SSH.	transport input ssh
В режим за конфигуриране на VTY линия, инструктирайте SSH да използва базата данни за локални потребители на маршрутизатора за удостоверяване.	login local
Активирайте услугата за криптиране на пароли, за да криптирате линейни пароли.	service password-encryption
Активирайте uRPF в режим за конфигуриране на интерфейса.	ip verify unicast source reachable-via {rx any} [allow-default] [allow-self-ping] [acl]
Активирайте услугите AAA в маршрутизатор.	aaa new-model
Създайте списък с методи AAA, наречен TEST, който се опитва да използва сървъра TACACS+ за удостоверяване, но ще се върне обратно към базата данни с локални потребители, ако сървърът TACACS+ е недостъпен.	aaa authentication login TEST group tacacs+ local
Конфигурирайте общ низ само за четене или за четене и запис в маршрутизатор, и посочете ACL, който дефинира доверени IP адреси.	snmp-server community <i>community-string</i> {ro rw} <i>acl</i>
Посочете ключ за удостоверяване NTP, заедно с идентификатор на ключа.	ntp authentication-key <i>key-id</i> md5 <i>key</i>
Инструктирайте маршрутизатора да идентифицира източници на точно време.	ntp authenticate
Посочете ключов идентификатор за доверен NTP.	ntp trusted-key <i>key-id</i>

План	Команди за конфигурация/Бележки
Инструктирайте маршрутизатор да осигури точно време за други устройства, разбиращи NTP, като използва вътрешния си часовник като източник на точно време, и посочете класовата стойност на маршрутизатора.	ntp master <i>stratum-number</i>
Посочете IP адрес за NTP сървър, от който маршрутизатор трябва да получи точно време, заедно с идентификатор на ключа, който би трябвало да бъде използван за удостоверяване с този NTP сървър.	ntp server <i>ip-address-of-ntp-server</i> key <i>key-id</i>

Таблица 16-10 Тренировка на паметта за план за потвърждаване

Необходима информация	Команда(и)
Извеждане на съдържанието на FIB на маршрутизатор.	show ip cef
Определяне дали един интерфейс е с активиран uRPF.	show cef interface <i>interface_id</i>
Изведете NTP класовата стойност на маршрутизатор.	show ntp status
Изведете класовата стойност на NTP обръщение към маршрутизатор.	show ntp associations detail

Глава 17

Таблица 17-3 Преглед на конструкцията

Цел на дизайна	Възможни избори за реализация, разгледани в тази глава
Предотвратяване на вкарването на неправилно управляем маршрутизатор от злонамерен потребител в автономна система EIGRP и образуване на съседство.	Конфигурирайте EIGRP удостоверяване, което използва удостоверяване MD5.

Цел на дизайна	Възможни избори за реализация, разгледани в тази глава
Конфигуриране на удостоверяване OSPFv2, така че злонамерен потребител да не може да извърши улавяне на пакет в трафика за удостоверяване и да определи ключа за удостоверяване.	Въпреки че OSPFv2 може да бъде конфигуриран за удостоверяване с открит текст (удостоверяване от Тип 1), тази цел може да бъде изпълнена с конфигуриране на удостоверяване с раздробяване (удостоверяване от Тип 2).
Предотвратяване на отвличането на съществуваща BGP сесия от неуправляем маршрутизатор, причинено от злонамерен потребител.	Конфигурирайте удостоверяване BGP, което използва удостоверяване MD5.

Таблица 17-4 Интересни въпроси към тази глава, които можете да вземете предвид по време на преглед на плана за реализация на колега

Въпрос	Отговори
Разговарящ на EIGRP маршрутизатор е конфигуриран с верига ключове, която съдържа множество ключове. Кой ключ ще бъде използван?	При изпращане на EIGRP съобщение, се използва най-ниският номер на ключ (от всички валидни ключове). Но при приемането на EIGRP съобщение и проверка на извадката MD5 се проверяват всички валидни в момента ключове.
Какви типове удостоверяване са достъпни за OSPFv3?	OSPFv3 няма вградени свойства за удостоверяване; но той може да се възползва от свойствата за удостоверяване, достъпни в IPsec. Следователно можете да използвате удостоверяване MD5 или SHA с OSPFv3.
Защо бихте искали да удостоверите съседите BGP, след като BGP изисква един маршрутизатор да притежава статично конфигуриране на IP адреса на съседа му?	Един злонамерен потребител би могъл да се опита да отвлече съществуваща сесия между два BGP съседа и след това да манипулира информацията за маршрутизиране.

Таблица 17-5 Тренировка на паметта за план за реализация на конфигурацията

План	Команди за конфигурация/Бележки
За EIGRP създайте верига от ключове и ѝ задайте име.	key chain <i>name</i>
За EIGRP създайте един или няколко номера за ключове.	key <i>number</i>
За EIGRP дефинирайте стойност на ключ за удостоверяване.	key-string <i>value</i>
Активирайте удостоверяване EIGRP за IPv4 MD5 в интерфейс за конкретна автономна система EIGRP.	ip authentication mode eigrp <i>asn md5</i>
За EIGRP за IPv4, посочете верига от ключове, която да се използва в интерфейс.	ipv6 authentication key-chain eigrp <i>asn name-of-chain</i>
Активирайте удостоверяване EIGRP за IPv6 в интерфейс за конкретна автономна система EIGRP.	ip authentication key-chain eigrp <i>asn md5</i>
За EIGRP за IPv6, посочете верига от ключове, която да се използва в интерфейс.	ipv6 authentication key-chain eigrp <i>asn name-of-chain</i>
Активирайте удостоверяване с Именуван EIGRP за интерфейс.	authentication mode [mg5 hmac-sha-256]
За именуван EIGRP, посочете верига от ключове, която да се използва в интерфейс.	authentication key-chain <i>name-of-chain</i>
Активирайте удостоверяване OSPFv2 за интерфейс.	ip ospf authentication [message-digest]
Активирайте удостоверяване OSPFv2 за всички интерфейси в дадена област, като конфигурирате удостоверяване в област.	area <i>area-number authentication</i>
Посочете ключ, който да се използва с удостоверяване OSPFv2 с открит текст.	ip ospf authentication key <i>key-string</i>
Посочете ключ, който да се използва с удостоверяване OSPFv2 MD5.	ip ospf message-digest-key <i>key-id md5 key-string</i>
Активирайте удостоверяване OSPFv3 в интерфейс.	area <i>area-number authentication ipsec spi security_policy_index</i> [md5 sha1] {0 7} <i>key-string</i>

План	Команди за конфигурация/Бележки
Активирайте удостоверяване OSPFv3 във всички интерфейси в дадена област, като конфигурирате удостоверяването в област.	ipv6 ospf authentication ipsec spi security_policy_index [md5 sha1] {0 7} key-string
Посочете ключ за удостоверяване, който да се използва с BGP съсед.	neighbor neighbor_ip password key

Таблица 17-6 Тренировка на паметта за план за потвърждаване

Необходима информация	Команда(и)
Потвърдете дали е включено съседство EIGRP за IPv4.	show ip cef
Потвърдете дали е включено съседство EIGRP за IPv6.	show ipv6 eigrp neighbors
Съберете информация за конфигурирана верига от ключове.	show key chain
Потвърдете дали е активирано удостоверяване OSPFv2.	show ip ospf interface interface_id
Потвърдете дали е активирано удостоверяване OSPFv3.	show crypto ipsec sa interface interface_id
Потвърдете дали е включено съседство OSPF.	show ip[v6] ospf neighbor
Потвърдете дали е включено съседство BGP за IPv4.	show ip bgp neighbors
Потвърдете дали е включено съседство BGP за IPv6.	show bgp ipv6 unicast summary

