



# Динамические многоточечные виртуальные частные сети IPsec (с применением протокола GRE/NHRP для масштабирования сети VPN IPsec)

---

Автор: Майк Суленбергер (Mike Sullenberger)

## Содержание

### Введение

### Общие сведения

### Решение DMVPN

- Запуск автоматического шифрования IPsec

- Динамическое создание туннелей для каналов с топологией "звезда"

- Создание динамического туннеля для трафика между краевыми маршрутизаторами

- Поддержка протоколов динамической маршрутизации

- Быстрая коммутация Cisco Express Forwarding для mGRE

### Использование динамической маршрутизации в виртуальных частных сетях (VPN), защищенных спецификацией IPsec

### Базовая настройка

- Примеры таблиц маршрутизации концентраторов и лучей

### Уменьшение размера настройки маршрутизатора концентратора

### Поддержка динамических адресов на лучах

### Динамическая многоточечная сеть типа "звезда"

### Динамические многоточечные виртуальные частные сети IPsec

- RIP

- EIGRP

- OSPF

- Начальные условия

- Условия после установки динамического канала между лучами 1 и 2

### VPN с динамическим многоточечным IPsec с двумя концентраторами

### Схема "Двойной концентратор – одинарный DMVPN"

- Начальные условия и изменения

### Системы с двумя концентраторами – топология двойной динамической многоточечной виртуальной частной сети (DMVPN)

- Начальные условия и изменения

### Заключение

### Дополнительные сведения

---

## Введение

В документе описаны динамические многоточечные виртуальные частные сети IPsec (DMVPN) и причины, побуждающие компании проектировать или переходить на новое решение IPsec VPN в ПО Cisco IOS®.

## Общие сведения

При шифровании трафика для его защиты компаниям бывает нужно связывать много узлов с основным узлом, а также друг с другом, через Интернет. Например, системе розничной продажи, которой нужно подключиться к штаб-квартире компании для инвентаризации и подачи заказов, может также потребоваться подключение к другим магазинам компании, чтобы проверить наличие продукта. Раньше единственным способом установить соединение было использование сети уровня 2, такой как ISDN или Frame Relay, для объединения всех компонентов. Настройка и себестоимость этих жестко проложенных каналов для внутреннего IP-трафика может быть трудоемка и дорога. Если все узлы (включая основной) уже имеют доступ к недорогому Интернет-трафику, его можно использовать для передачи внутреннего IP-трафика между магазинами и головным офисом с применением туннелей IPsec для обеспечения конфиденциальности и

целостности данных.

Для построения больших сетей IPsec с взаимодействием узлов через Интернет для различных компаний, нужна возможность масштабирования сети IPsec. IPsec шифрует трафик между двумя адресуемыми конечными точками вызова, и шифрование выполняется между этими двумя конечными точками с использованием общего "секрета". Так как секрет разделен только между этими двумя конечными точками, шифрованные сети изначально являются набором двухточечных каналов связи. Поэтому IPsec, в сущности, является двухточечной туннельной сетью. Наиболее подходящим способом является масштабирование больших двухточечных сетей для организации их в сеть с топологией "звезда" или полную (частичную) объединенную сеть. В большинстве сетей почти весь трафик IP приходится на обмен данными между конечными узлами и концентратором, и лишь самая малая его часть - на трафик между самими конечными узлами, поэтому звездообразная топология, как правило, оказывается оптимальным вариантом. Кроме того, такая архитектура соответствует топологии старых сетей Frame Relay, в которых ее применение объяснялось недопустимо высокой стоимостью установки прямых линий между всеми узлами сетей.

При использовании Интернета в качестве посредника между концентратором и лучами, лучи также имеют прямой доступ друг к другу без дополнительных материальных затрат, но до настоящего времени было практически невозможно установить и/или управлять полной (частичной) объединенной сетью. Сети с полностью или частично ячеистой структурой часто являются более предпочтительными, так как они позволяют сэкономить средства, если трафик между двумя лучами можно передать напрямую, а не через концентратор. Трафик между двумя лучами, проходящий через концентратор, использует ресурсы концентратора и может вызвать дополнительную задержку, особенно при использовании шифрования IPsec, т.к. концентратору придется расшифровывать входящие пакеты от посылающих лучей, а затем вновь шифровать трафик для передачи его на получающий луч. Еще один пример, когда прямой трафик между лучами более предпочтителен, - ситуация, когда два конца луча находятся в одном городе, а концентратор - на другом конце страны.

Из-за развертывания и увеличения в размерах звездообразных сетей IPsec все чаще возникает необходимость в максимально динамичной маршрутизации IP-пакетов. В старых звездообразных сетях Frame Relay это достигалось с помощью протоколов динамической маршрутизации, таких как OSPF или EIGRP, работающих через каналы Frame Relay. Это использовалось для динамического объявления доступности конечных сетей и обеспечения резервирования сетей с IP-маршрутизацией. Если в сети потерян центральный маршрутизатор, резервный центральный маршрутизатор может автоматически занять его место, чтобы сохранить сетевые подключения к конечным сетям.

Это основная проблема с туннелями IPsec и протоколами динамической маршрутизации. Протоколы динамической маршрутизации рассчитаны на использование многоадресных или широковещательных пакетов, но IPsec не поддерживает шифрование этих пакетов. В настоящее время эта проблема решается с помощью использования туннелей общей маршрутной инкапсуляции GRE в комбинации с шифрованием IPsec.

Туннели GRE поддерживают передачу многоадресных и широковещательных IP-пакетов на другой конец туннеля GRE. Туннельный пакет GRE представляет собой однонаправленный пакет IP, поэтому пакет GRE может шифроваться посредством IPsec. В этом сценарии для поддержки сети VPN GRE выполняет туннелирование, а IPsec - шифрование. Когда туннели GRE настроены, IP-адреса для конечных точек туннеля (**tunnel source ...**, **tunnel destination ...**) должны быть известны на другом конце туннеля и иметь возможность передачи через Интернет. Это означает, что концентратор и маршрутизаторы всех лучей в этой сети должны иметь статические, а не частные IP-адреса.

Для подсоединения к Интернету небольших узлов внешний IP-адрес луча обычно меняется при каждом подключении к Интернету, т.к. каждый раз, когда в канале появляется луч (асимметричная цифровая абонентская линия (ADSL) и абонентский кабельный ввод), поставщик Интернет-услуг (ISP) динамично предоставляет адрес внешнего интерфейса (через протокол динамической настройки узла (DHCP)). Такое динамическое выделение "внешнего адреса" маршрутизатора позволяет ISP реализовывать избыточную подписку для адресного пространства в Интернете, так как одновременно не все пользователи будут подключены к сети. Выделение статического адреса для конечного маршрутизатора может стоить значительно дороже. Для использования протокола динамической маршрутизации поверх IPsec VPN необходимы туннели GRE, однако при этом теряется возможность использования периферийных серверов с динамически выделяемыми IP-адресами на внешних физических интерфейсах.

Все упомянутые, а также дополнительные ограничения, сводятся к следующим пунктам:

- IPsec использует список контроля доступа (ACL) для определения данных, которые должны быть зашифрованы. Каждый раз, когда добавляется новая сеть (подсеть) после луча или концентратора, необходимо изменить список управления доступом и на центральном маршрутизаторе и на маршрутизаторе на конце луча. Если SP управляет маршрутизатором, то пользователь должен уведомить SP, чтобы получить список ACL IPsec. Это список изменен таким образом, чтобы новый трафик стал зашифрованным.
- В больших звездообразных сетях размер настройки на маршрутизаторе концентратора может достигнуть такой величины, что его уже нельзя будет использовать. Например, центральному маршрутизатору понадобится около 3900 строк настройки для поддержки 300 конечных маршрутизаторов. При таком большом количестве трудно отобразить всю настройку и найти ее раздел, относящийся к текущей проблеме, отладка которой выполняется. Кроме того, это настройка размера может быть слишком большой, чтобы уместиться в энергонезависимом ЗУПВ, поэтому ее следует сохранить во флеш-памяти.

- GRE + IPsec должен знать адрес однорангового узла конечной точки. IP-адреса маршрутизаторов на конце луча подключены напрямую к Интернету через собственного ISP, и они зачастую настроены так, что адреса их внешних интерфейсов не являются фиксированными. IP-адреса могут изменяться каждый раз, когда узел подключается к сети (по DHCP).
- Если необходимо прямое соединение между лучами через IPsec VPN, тогда звездообразная сеть должна стать полностью объединенной сетью. Так как еще неизвестно, между какими лучами необходимо установить соединение, то требуется полная объединенная сеть, даже если соединение всех лучей друг с другом не понадобится. Также, невозможно настроить IPsec на маленьком маршрутизаторе луча так, чтобы он имел прямое соединение со всеми другими маршрутизаторами лучей в сети; для этого необходимо иметь более мощные маршрутизаторы лучей.

## Решение для сети DMVPN

Чтобы исправить перечисленные проблемы методом масштабирования, решение DMVPN использует Multipoint GRE (mGRE) и протокол разрешения последующего узла (NHRP) с IPsec и некоторыми новыми расширениями.

### Запуск автоматического шифрования IPsec

Без использования решения для сети DMVPN, туннель шифрования IPsec не будет активен до тех пор, пока не появится трафик, требующий использования этого туннеля IPsec. Для запуска туннеля IPsec и отбрасывания трафика требуется от 1 до 10 секунд. При использовании GRE с IPsec настройка туннеля GRE уже содержит адрес однорангового узла туннеля GRE (**tunnel destination ...**), который одновременно является адресом однорангового узла IPsec. Оба адреса настраиваются предварительно.

Если вы используете алгоритм обнаружения конечной точки туннеля (TED) и динамические криптокарты на маршрутизаторе концентратора, то вы можете избежать необходимости предварительной настройки адресов однорангового узла IPsec на концентраторе, но перед началом работы протокола ISAKMP необходимо провести тестовую отправку и получение TED. Это необязательно, так как при использовании GRE одноранговые адреса источника и назначения известны заранее. Они либо внесены в настройку, либо приведены в NHRP (для многоточечных туннелей GRE).

При использовании решения для сетей DMVPN, IPsec запускается одновременно для двухточечных и многоточечных туннелей GRE. Также, нет необходимости настраивать любой криптографический ACL, так как они будут автоматически поставлены от туннельных адресов GRE источника и назначения. Для определения параметров шифрования IPsec используются следующие команды. Обратите внимание на то, что команды **set peer ...** или **match address ...** не требуются, так как данная информация поступает прямо из связанного туннеля GRE или сопоставлений NHRP.

```
crypto ipsec profile <profile-name>
set transform-set <transform-name>
```

Следующая команда связывает интерфейс туннеля с профилем IPsec.

```
interface tunnel<number>
...
tunnel protection ipsec profile <profile-name>
```

### Создание динамического туннеля для каналов типа "звезда"

В сети DMVPN на маршрутизаторе концентратора не настроена информация GRE или IPsec о луче. Туннель GRE маршрутизатора луча содержит (посредством команд NHRP) информацию о маршрутизаторе концентратора. Когда маршрутизатор луча запускается, он автоматически устанавливает туннель IPsec с маршрутизатором концентратора, как описано выше. Затем он использует NHRP, чтобы сообщить маршрутизатору концентратора текущий IP-адрес физического интерфейса. Это полезно по трем причинам:

- Если IP-адрес физического интерфейса конечного маршрутизатора был присвоен динамически (например, с помощью ADSL или кабельного модема), то для маршрутизатора концентратора нельзя использовать эти данные, так как при каждой перезагрузке конечный маршрутизатор будет получать новый IP-адрес физического интерфейса.

- Настройка центрального маршрутизатора сокращается и упрощается, поскольку ему не нужна информация GRE или IPsec о маршрутизаторах одноранговых узлов. Вся информация постоянно запоминается посредством NHRP.
- Изменять настройку на концентраторе или других текущих маршрутизаторах луча при добавлении в сеть DMVPN нового маршрутизатора луча не потребуется. Новый маршрутизатор луча настраивается на основе информации концентратора, и при включении маршрутизатор концентратора автоматически его регистрирует. Протокол динамической маршрутизации передает маршрутную информацию для этого луча на концентратор. Концентратор передает эти новые данные маршрутизации другим периферийным устройствам. Кроме этого, он передает маршрутную информацию всех остальных лучей на этот новый луч.

## Создание динамического туннеля для трафика между "лучевыми" маршрутизаторами

Как отмечалось выше, сейчас в объединенной сети все двухточечные туннели IPsec (или IPsec+GRE) должны быть настроены на все маршрутизаторы, даже если некоторые или большинство из них действуют не все время. Используя решение DMVPN, один маршрутизатор становится концентратором, а другие маршрутизаторы (лучи) настраиваются на концентратор с помощью туннелей. Туннели с топологией "звезда" постоянно включены, и настройка прямого туннеля между какими-либо лучами не требуется. Напротив, когда один луч хочет передать пакет на другой луч (как подсеть за другим лучом), он использует NHRP для динамического определения необходимого адреса луча назначения. Маршрутизатор концентратора действует в качестве сервера NHRP и обрабатывает этот запрос для исходного луча. Затем два луча динамически создают между собой туннель IPsec (через единый интерфейс mGRE), обеспечивающий прямую передачу данных. Данный динамический туннель между двумя лучами будет автоматически разорван после окончания (настроенного) периода бездействия.

## Поддержка протоколов динамической маршрутизации

Решение DMVPN основано на туннелях GRE, поддерживающих тоннелирование многоадресных/широковещательных IP-пакетов, поэтому решение DMVPN также поддерживает протоколы динамической маршрутизации, которые работают через туннели IPsec+mGRE. Ранее протокол NHRP требовал явной настройки широковещательного/многоадресного сопоставления для IP-адресов назначения туннеля для поддержки GRE-тоннелирования многоадресных и широковещательных IP-пакетов. Например, на концентраторе вам потребуется строка настройки **ip nhrp map multicast <spoke-n-addr>** для каждого луча. Для решения DMVPN адреса на конце лучей заранее неизвестны, поэтому эта настройка невозможна. NHRP можно настроить на автоматическое добавление каждого луча в список многоадресного назначения на концентраторе с помощью команды **ip nhrp map multicast dynamic**. При помощи этой команды, когда маршрутизаторы лучей регистрируют одноадресное сопоставление NHRP при помощи сервера NHRP (концентратора), NHRP также создаст многоадресное сопоставление для этого луча. Это освобождает от необходимости заранее знать адреса лучей.

## Быстрая коммутация Cisco Express Forwarding для mGRE

В настоящий момент трафик в интерфейсе mGRE коммутируется процессом, что приводит к снижению производительности. Решение DMVPN обеспечивает коммутацию с механизмом переадресации Cisco для трафика mGRE, увеличивая быстродействие. Необязательно использовать команды настройки для включения этой функции. Если коммутация Cisco Express Forwarding разрешена на интерфейсе туннеля GRE и входящих/исходящих физических интерфейсах, то многоточечные туннельные пакеты GRE будут переключаться с помощью Cisco Express Forwarding.

## Использование динамической маршрутизации в виртуальных частных сетях (VPN), защищенных спецификацией IPsec

В данном разделе рассматривается текущее положение дел (до решения DMVPN). IPsec устанавливается на маршрутизаторы Cisco с помощью нескольких команд для определения шифрования, а затем команды **crypto map <map-name>** на внешний интерфейс маршрутизатора. Из-за такой архитектуры и отсутствия стандарта, описывающего порядок использования IPsec для шифрования многоадресных/широковещательных IP-пакетов, пакеты протокола IP маршрутизации невозможно передать через туннель IPsec, и информация о любых изменениях маршрутизации достигнет другого конца туннеля IPsec не сразу.

**Примечание.** Все протоколы динамической маршрутизации, кроме BGP, используют широковещательные и многоадресные IP пакеты. Для решения этой проблемы используются туннели GRE в комбинации с IPsec.

Туннели GRE устанавливаются на маршрутизаторы Cisco с помощью виртуального интерфейса туннеля (**interface tunnel<#>**). Протокол тоннелирования GRE разработан для многоадресных/широковещательных IP пакетов, поэтому протокол динамической маршрутизации можно "запустить" через туннель GRE. Туннельные пакеты GRE являются одноадресными пакетами IP, инкапсулирующими исходный много- или одноадресный пакет IP. Затем можно использовать IPsec для шифрования туннельного

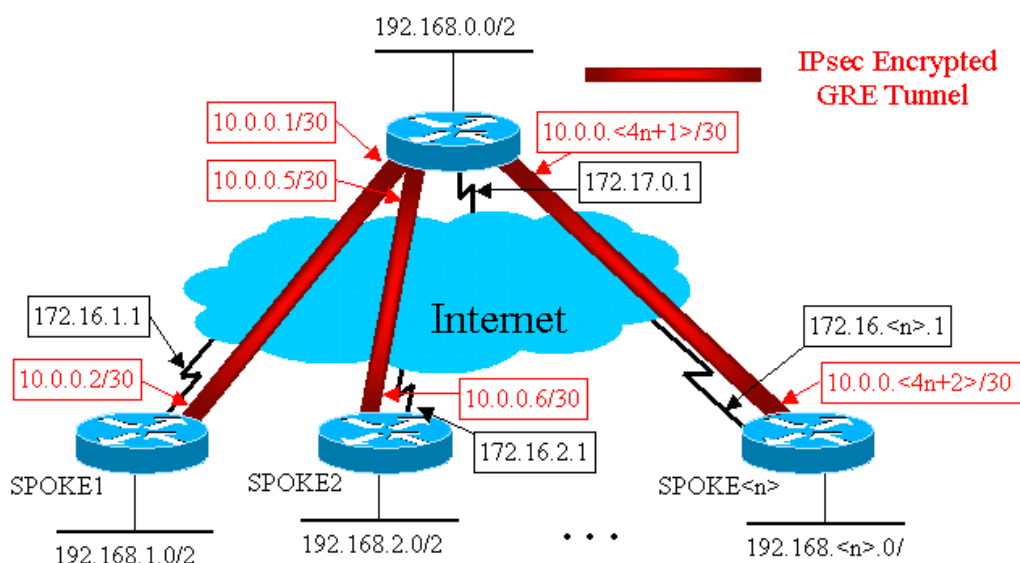
пакета GRE. Можно запустить IPsec в режиме передачи и сэкономить 20 байт, т. к. GRE уже инкапсулировал исходный пакет данных и IPsec нет необходимости инкапсулировать IP-пакет GRE в другом IP-заголовке.

При использовании IPsec в транспортном режиме предусмотрено следующее ограничение: подлежащие шифрованию IP-адреса источника и назначения пакета должны соответствовать одноранговым адресам IPsec (самого маршрутизатора). В данном случае это означает, что конечная точка GRE-туннеля и адрес узла IPsec должны совпадать. Это не представляет трудности, т. к. одни и те же маршрутизаторы являются конечными точками туннелей IPsec и GRE. Совмещая туннели GRE с шифрованием IPsec, можно использовать протокол динамической IP маршрутизации для обновления таблиц маршрутизации на обоих концах зашифрованного туннеля. Элементы таблицы IP маршрутизации для сетей, которые были записаны через зашифрованный туннель, будут воспринимать противоположный конец туннеля (IP-адрес интерфейса туннеля GRE) как IP следующего перехода. Таким образом, если на каком-либо конце туннеля меняются параметры сети, то на другом конце эти изменения динамически отразятся; соединение при этом не будет нарушено, и дополнительные настройки маршрутизаторов не понадобятся.

## Базовая настройка

Ниже представлена стандартная двухточечная настройка IPsec+GRE. Затем приведено несколько примеров настроек, в которых отдельные элементы решения DMVPN добавлены в выполняемые действия, чтобы показать различные возможности DMVPN. Каждый пример построен на предыдущих примерах для демонстрации использования решения DMVPN в усложняющихся структурах сети. Эту серию примеров можно использовать в качестве шаблона для переноса текущей сети VPN IPsec+GRE в DMVPN. В любой момент "перенос" можно остановить, если конкретный пример настройки соответствует требованиям к вашей сети.

### Звезда IPsec + GRE (n = 1,2,3,...)



#### ● Маршрутизатор концентратора ●

```
version 12.3
!
hostname Hub
!
crypto isakmp policy 1
 authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
 crypto map vpnmap1 local-address Ethernet0
 crypto map vpnmap1 10 ipsec-isakmp
  set peer 172.16.1.1
  set transform-set trans2
 match address 101
 crypto map vpnmap1 20 ipsec-isakmp
  set peer 172.16.2.1
  set transform-set trans2
```

```

match address 102
. . .
crypto map vpnmap1 <10*n> ipsec-isakmp
set peer 172.16.<n>.1
set transform-set trans2
match address <n+100>
!
interface Tunnel1
bandwidth 1000
ip address 10.0.0.1 255.255.255.252
ip mtu 1400
delay 1000
tunnel source Ethernet0
tunnel destination 172.16.1.1
!
interface Tunnel2
bandwidth 1000
ip address 10.0.0.5 255.255.255.252
ip mtu 1400
delay 1000
tunnel source Ethernet0
tunnel destination 172.16.2.1
!
. . .
!
interface Tunnel<n>
bandwidth 1000
ip address 10.0.0.<4n-3> 255.255.255.252
ip mtu 1400
delay 1000
tunnel source Ethernet0
tunnel destination 172.16.<n>.1
!
interface Ethernet0
ip address 172.17.0.1 255.255.255.0
crypto map vpnmap1
!
interface Ethernet1
ip address 192.168.0.1 255.255.255.0
!
router eigrp 1
network 10.0.0.0 0.0.0.255
network 192.168.0.0 0.0.0.255
no auto-summary
!
access-list 101 permit gre host 172.17.0.1 host 172.16.1.1
access-list 102 permit gre host 172.17.0.1 host 172.16.2.1
...
access-list <n+100> permit gre host 172.17.0.1 host 172.16.<n>.1

```

## ● Маршрутизатор луча 1 ●

```

version 12.3
!
hostname Spoke1
!
crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
mode transport
!
crypto map vpnmap1 local-address Ethernet0
crypto map vpnmap1 10 ipsec-isakmp
set peer 172.17.0.1
set transform-set trans2
match address 101
!
interface Tunnel0
bandwidth 1000
ip address 10.0.0.2 255.255.255.252
ip mtu 1400
delay 1000
tunnel source Ethernet0
tunnel destination 172.17.0.1
!

```

```
interface Ethernet0
 ip address 172.16.1.1 255.255.255.252
 crypto map vpnmap1
!
interface Ethernet1
 ip address 192.168.1.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.1.0 0.0.0.255
 no auto-summary
!
access-list 101 permit gre host 172.16.1.1 host 172.17.0.1
```

## ● Маршрутизатор луча 2 ●

```
version 12.3
!
hostname Spoke2
!
crypto isakmp policy 1
 authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
 crypto map vpnmap1 local-address Ethernet0
 crypto map vpnmap1 10 ipsec-isakmp
 set peer 172.17.0.1
 set transform-set trans2
 match address 101
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.6 255.255.255.252
 ip mtu 1400
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.1
!
interface Ethernet0
 ip address 172.16.2.1 255.255.255.252
 crypto map vpnmap1
!
interface Ethernet1
 ip address 192.168.2.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.2.0 0.0.0.255
 no auto-summary
!
access-list 101 permit gre host 172.16.2.1 host 172.17.0.1
```

## ● Маршрутизатор луча<n> ●

```
version 12.3
!
hostname Spoke<n>
!
crypto isakmp policy 1
 authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
!
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
 crypto map vpnmap1 local-address Ethernet0
 crypto map vpnmap1 10 ipsec-isakmp
 set peer 172.17.0.1
```

```

set transform-set trans2
match address 101
!
interface Tunnel0
bandwidth 1000
ip address 10.0.0.<4n-2> 255.255.255.252
ip mtu 1400
delay 1000
tunnel source Ethernet0
tunnel destination 172.17.0.1
!
interface Ethernet0
ip address 172.16.<n>.1 255.255.255.252
crypto map vpnmap1
!
interface Ethernet1
ip address 192.168.<n>.1 255.255.255.0
!
router eigrp 1
network 10.0.0.0 0.0.0.255
network 192.168.<n>.0 0.0.0.255
no auto-summary
!
access-list 101 permit gre host 172.16.<n>.1 host 172.17.0.1

```

В приведенной выше настройке списки ACL используются для определения трафика, который должен быть зашифрован. На маршрутизаторах концентратора и луча список управления доступом должен соответствовать только IP пакетам туннеля GRE. Не важно, как меняются сети на концах туннеля, IP пакеты туннеля GRE не изменятся, т.е. этот список ACL не требует изменений.

**Примечание.** При использовании ПО Cisco IOS версии до 12.2(13)T, необходимо выполнить команду настройки **crypto map vpnmap1** на интерфейсе туннеля GRE (Tunnel<x>) и физическом интерфейсе (Ethernet0). При использовании Cisco IOS версии 12.2(13)T и выше команда **crypto map vpnmap1** применяется только к физическому интерфейсу (Ethernet0).

## Примеры таблиц маршрутизации концентраторов и лучей

### ● Таблицы маршрутизации на концентраторе ●

```

172.17.0.0/24 is subnetted, 1 subnets
C    172.17.0.0 is directly connected, Ethernet0
10.0.0.0/30 is subnetted, <n> subnets
C    10.0.0.0 is directly connected, Tunnel1
C    10.0.0.4 is directly connected, Tunnel2
...
C    10.0.0.<4n-4> is directly connected, Tunnel<n>
C    192.168.0.0/24 is directly connected, Ethernet1
D    192.168.1.0/24 [90/2841600] via 10.0.0.2, 18:28:19, Tunnel1
D    192.168.2.0/24 [90/2841600] via 10.0.0.6, 2d05h, Tunnel2
...
D    192.168.<n>.0/24 [90/2841600] via 10.0.0.<4n-2>, 2d05h, Tunnel<n>

```

### ● Таблица маршрутизации для маршрутизатора луча 1 ●

```

172.16.0.0/24 is subnetted, 1 subnets
C    172.16.1.0 is directly connected, Ethernet0
10.0.0.0/30 is subnetted, <n> subnets
C    10.0.0.0 is directly connected, Tunnel1
D    10.0.0.4 [90/2841600] via 10.0.0.1, 23:00:58, Tunnel0
...
D    10.0.0.<4n-4> [90/2841600] via 10.0.0.1, 23:00:58, Tunnel0
D    192.168.0.0/24 [90/2841600] via 10.0.0.1, 23:00:58, Tunnel0
C    192.168.1.0/24 is directly connected, Loopback0
D    192.168.2.0/24 [90/3097600] via 10.0.0.1, 23:00:58, Tunnel0
...
D    192.168.<n>.0/24 [90/3097600] via 10.0.0.1, 23:00:58, Tunnel0

```



## ● Таблица маршрутизации для маршрутизатора луча<n> ●

```
172.16.0.0/24 is subnetted, 1 subnets
C    172.16.<n>.0 is directly connected, Ethernet0
    10.0.0.0/30 is subnetted, <n> subnets
D    10.0.0.0 [90/2841600] via 10.0.0.1, 22:01:21, Tunnel0
D    10.0.0.4 [90/2841600] via 10.0.0.1, 22:01:21, Tunnel0
...
C    10.0.0.<4n-4> is directly connected, Tunnel0
D    192.168.0.0/24 [90/2841600] via 10.0.0.1, 22:01:21, Tunnel0
D    192.168.1.0/24 [90/3097600] via 10.0.0.1, 22:01:21, Tunnel0
D    192.168.2.0/24 [90/3097600] via 10.0.0.1, 22:01:21, Tunnel0
...
C    192.168.<n>.0/24 is directly connected, Ethernet0
```

Это базовая работающая настройка, которая используется в качестве отправной точки для сравнения с более сложными настройками с возможностью использования решения DMVPN. Первое изменение уменьшит размер настройки на маршрутизаторе концентратора. Это не имеет значения при небольшом количестве маршрутизаторов лучей, и становится важным, если количество маршрутизаторов составляет 50–100 устройств.

## Уменьшение размера настройки маршрутизатора концентратора

В следующем примере настройка маршрутизатора концентратора изменена минимально: с многоканального двухточечного туннельного интерфейса GRE на одноканальный многоточечный туннельный интерфейс. Это первый шаг к решению DMVPN.

Маршрутизатор концентратора содержит уникальный блок строк настройки, необходимый для определения характеристик криптокарты для каждого маршрутизатора луча. Данная часть настройки определяет зашифрованный ACL и интерфейс туннеля GRE для этого маршрутизатора луча. Эти характеристики чаще всего одинаковы для всех лучей, исключения составляют IP-адреса (**set peer ...**, **tunnel destination ...**).

Из приведенной выше настройки маршрутизатора концентратора видно, что для каждого маршрутизатора луча необходимо как минимум 13 строк настройки; четыре для криптокарты, одна для зашифрованного ACL и восемь для интерфейса туннеля GRE. Общее количество строк настройки при 300 маршрутизаторах лучей равно 39000. Необходимо также 300 (/30) подсетей для адресации каждого канала туннеля. Настройкой такого размера сложно управлять, особенно при устранении неполадок в сети VPN. Для уменьшения этого значения можно использовать динамические криптокарты, которые сократят указанное выше значение на 1200 строк, и оставят 2700 строк в сети с 300 лучами.

**Примечание.** При использовании динамических криптокарт зашифрованный туннель IPSec должен быть инициализирован лучевым маршрутизатором. Можно также использовать **ip unnumbered <interface>** для уменьшения количества подсетей, необходимых для туннелей GRE, но это в дальнейшем может усложнить процедуру устранения неполадок.

Решение DMVPN позволяет настроить одиночный многоадресный туннельный интерфейс GRE и одиночный профиль IPsec на маршрутизаторе концентратора для обработки всех лучевых маршрутизаторов. Это позволяет размеру настройки на маршрутизаторе концентратора оставаться постоянным, вне зависимости от количества лучевых маршрутизаторов, добавленных в сеть VPN.

Решение DMVPN предлагает следующие новые команды:

```
crypto ipsec profile <name>
  <ipsec parameters>

tunnel protection ipsec profile <name>

ip nhrp map multicast dynamic
```

Команда **crypto ipsec profile <name>** используется как динамическая криптокарта и разработана специально для туннельных

интерфейсов. Эта команда используется для определения параметров шифрования IPsec в VPN туннелях от луча к концентратору и от одного луча к другому. Единственный необходимый параметр в этом профиле - это набор для преобразования. Адрес однорангового узла IPsec и условие **match address ...** для прокси IPsec автоматически извлекаются из NHRP-сопоставлений для туннеля GRE.

Команда **tunnel protection ipsec profile <name>** настраивается на туннельном интерфейсе GRE и используется для соединения туннельного интерфейса GRE с профилем IPsec. Кроме этого, команда **tunnel protection ipsec profile <name>** может использоваться в двухточечных туннелях GRE. В этом случае получаются данные о сервере и одноранговом узле IPsec из настройки **tunnel source ...** и **tunnel destination ...**. Это позволяет упростить процесс настройки, так как отпадает необходимость использования одноранговых узлов IPsec и зашифрованных списков ACL.

**Примечание.** Команда **tunnel protection** означает, что шифрование IPsec закончится после того, как инкапсуляция GRE будет добавлена к пакету.

Эти две новые команды похожи на настройку криптокарт и назначение криптокарт интерфейсу с помощью команды **crypto map <name>**. Существенное отличие заключается в том, что при использовании новых команд нет необходимости указывать адрес равноправного пользователя протокола IPsec или список ACL, чтобы отобрать пакеты, подлежащие шифрованию. Эти параметры определяются автоматически из отображений NHRP для туннельного интерфейса mGRE.

**Примечание.** При использовании команды **tunnel protection** на туннельном интерфейсе, команда **crypto map ...** не настроена на исходящем физическом интерфейсе.

Последняя новая команда, **ip nhrp map multicast dynamic**, позволяет NHRP автоматически добавлять лучевые маршрутизаторы к многоадресным сопоставлениям NHRP, когда эти маршрутизаторы инициируют туннель mGRE+IPsec и регистрируют их одноадресные соответствия NHRP. Это необходимо для возможности работы протокола динамической маршрутизации в туннелях mGRE+IPsec между концентратором и лучами. Если эта команда недоступна, то маршрутизатор концентратора должен иметь отдельный канал настройки для многоадресного сопоставления с каждым лучом.

**Примечание.** С этой настройкой маршрутизаторы лучей должны инициировать туннельное соединение mGRE+IPsec, поскольку настройка маршрутизатора концентратора не содержит данных о лучах. Однако проблем не возникает, поскольку при использовании DMVPN при запуске маршрутизатора луча туннель mGRE+IPsec автоматически инициируется и постоянно остается активным.

**Примечание.** Следующий пример демонстрирует двухточечный туннельный интерфейс GRE на лучевых маршрутизаторах и каналах настройки NHRP, добавленный на маршрутизаторы концентраторов и лучей для поддержки туннеля mGRE на маршрутизаторе концентратора. Изменения конфигурации изложены ниже.

### ● Маршрутизатор концентратора (старый) ●

```
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.16.1.1
  set transform-set trans2
  match address 101
crypto map vpnmap1 20 IPsec-isakmp
  set peer 172.16.2.1
  set transform-set trans2
  match address 102
. . .
crypto map vpnmap1 <10n> IPsec-isakmp
  set peer 172.16.<n>.1
  set transform-set trans2
  match address <n+100>
!
interface Tunnel1
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.252
  ip mtu 1400
  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.16.1.1
!
interface Tunnel2
  bandwidth 1000
  ip address 10.0.0.5 255.255.255.252
  ip mtu 1400
  delay 1000
  tunnel source Ethernet0
```

```

tunnel destination 172.16.2.1
!
. . .
!
interface Tunnel<n>
bandwidth 1000
ip address 10.0.0.<4n-1> 255.255.255.252
ip mtu 1400
delay 1000
tunnel source Ethernet0
tunnel destination 172.16.<n>.1
!
interface Ethernet0
ip address 172.17.0.1 255.255.255.0
crypto map vpnmap1
!
access-list 101 permit gre host 172.17.0.1 host 172.16.1.1
access-list 102 permit gre host 172.17.0.1 host 172.16.2.1
. . .
access-list <n+100> permit gre host 172.17.0.1 host 172.16.<n>.1

```

### ● Маршрутизатор концентратора (новый) ●

```

crypto ipsec profile vpnprof
set transform-set trans2
!
interface Tunnel0
bandwidth 1000
ip address 10.0.0.1 255.255.255.0
ip mtu 1400
ip nhrp authentication test
ip nhrp map multicast dynamic
ip nhrp network-id 100000
ip nhrp holdtime 600
no ip split-horizon eigrp 1
delay 1000
tunnel source Ethernet0
tunnel mode gre multipoint
tunnel key 100000
tunnel protection ipsec profile vpnprof
!
interface Ethernet0
ip address 172.17.0.1 255.255.255.0

```

### ● Маршрутизатор луча <n> (старый) ●

```

crypto map vpnmap1 10 IPsec-isakmp
set peer 172.17.0.1
set transform-set trans2
match address 101
!
interface Tunnel0
bandwidth 1000
ip address 10.0.0.<4n-2> 255.255.255.252
ip mtu 1400
delay 1000
tunnel source Ethernet0
tunnel destination 172.17.0.1
!
interface Ethernet0
ip address 172.16.<n>.1 255.255.255.252
crypto map vpnmap1
!
. . .
!
access-list 101 permit gre host 172.16.<n>.1 host 172.17.0.1
!

```

## ● Маршрутизатор луча<n> (новый) ●

```
crypto map vpnmap1 10 IPsec-isakmp
set peer 172.17.0.1
set transform-set trans2
match address 101
!
interface Tunnel0
bandwidth 1000
ip address 10.0.0.<n+1> 255.255.255.0
ip mtu 1400
ip nhrp authentication test
ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp network-id 100000
ip nhrp holdtime 300
ip nhrp nhs 10.0.0.1
delay 1000
tunnel source Ethernet0
tunnel destination 172.17.0.1
tunnel key 100000
!
interface Ethernet0
ip address 172.16.<n>.1 255.255.255.252
crypto map vpnmap1
!
. . .
!
access-list 101 permit gre host 172.16.<n>.1 host 172.17.0.1
!
```

На лучевых маршрутизаторах изменилась маска подсети, и на туннельный интерфейс были добавлены команды NHRP. Команды NHRP необходимы, т.к. маршрутизатор концентратора теперь использует NHRP для сопоставления IP-адреса туннельного интерфейса луча с IP-адресом физического интерфейса луча.

```
ip address 10.0.0.<n+1> 255.255.255.0
ip mtu 1400
ip nhrp authentication test
ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp network-id 100000
ip nhrp holdtime 300
ip nhrp nhs 10.0.0.1
...
tunnel key 100000
```

Подсеть теперь /24 вместо /30, поэтому все узлы находятся в одной подсети, а не в разных. Лучевые устройства по-прежнему передают трафик между лучами через концентратор, поскольку они используют двухточечный туннельный интерфейс GRE. Команды **ip nhrp authentication ...**, **ip nhrp network-id ...** и **tunnel key ...** используются для сопоставления туннельных пакетов и пакетов NHRP с правильным ширококошечательным туннельным интерфейсом GRE и сетью NHRP при их получении концентратором. Команды **ip nhrp map ...** и **ip nhrp nhs ...** используются протоколом NHRP на луче для объявления сопоставления NHRP лучей (10.0.0.<n+1> --> 172.16.<n>.1) с концентратором. Адрес 10.0.0.<n+1> извлекается из команды **ip address ...** на туннельном интерфейсе, и адрес 172.16.<n>.1 извлекается из команды **tunnel destination ...** на туннельном интерфейсе.

В случае 300 лучевых маршрутизаторов это изменение уменьшит число строк настройки на концентраторе с 3 900 до 16 (на 3 884 строки). Размер настройки на каждом лучевом маршрутизаторе увеличится на 6 строк.

## Поддержка динамических адресов на лучах

Перед установлением туннельного соединения по протоколу IPSec на маршрутизаторе Cisco для каждого однорангового узла необходимо задать IP-адрес другого однорангового узла. При выполнении этого может возникнуть проблема, если маршрутизатор на конце луча имеет динамический адрес физического интерфейса, как это часто бывает у маршрутизаторов, подключенных через DSL или кабельную линию.

TED позволяет одноранговому пользователю IPsec найти другого однорангового пользователя с помощью отправки специального пакета протокола ISAKMP (Протокол управления ключами Ассоциации безопасности Интернет) на IP-адрес назначения исходного пакета данных, который должен быть зашифрован. Предполагается, что этот пакет пройдет через промежуточную сеть, следуя по тому же пути, что и туннельный пакет IPsec. Этот пакет будет подхвачен одноранговым узлом IPsec на другом конце, о чем он сообщит первому одноранговому узлу. Затем выполняется сопоставление безопасности IPsec и ISAKMP и создание туннеля IPsec. Это работает только в том случае, если пакеты данных, которые необходимо зашифровать, имеют маршрутизируемые IP-адреса.

TED можно использовать в сочетании с GRE туннелями, настройки которых приведены в предыдущем разделе. Это было успешно протестировано, хотя в ранних версиях ПО Cisco IOS возникали большие проблемы, когда TED вынужденно шифровал не только туннельные пакеты GRE, но и весь IP трафик между двумя одноранговыми узлами IPsec. Решение DMVPN предоставляет эту и другие дополнительные возможности, при этом узлам не требуется использовать маршрутизируемые IP-адреса Интернета и отправлять тестовые и ответные пакеты. С небольшими изменениями настройка из последнего раздела может использоваться для поддержки маршрутизаторов луча с динамическими IP-адресами на внешних физических интерфейсах.

### ● Маршрутизатор концентратора (без изменений) ●

```
crypto ipsec profile vpnprof
  set transform-set trans2
!
interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 600
  no ip split-horizon eigrp 1
  delay 1000
  tunnel source Ethernet0
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
!
interface Ethernet0
  ip address 172.17.0.1 255.255.255.0
```

### ● Маршрутизатор луча <n> (старый) ●

```
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set transform-set trans2
  match address 101
!
...
!
access-list 101 permit gre host 172.16.<n>.1 host 172.17.0.1
```

### ● Маршрутизатор луча<n> (новый) ●

```
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set transform-set trans2
set security-association level per-host
  match address 101
!
...
!
access-list 101 permit gre any host 172.17.0.1
```

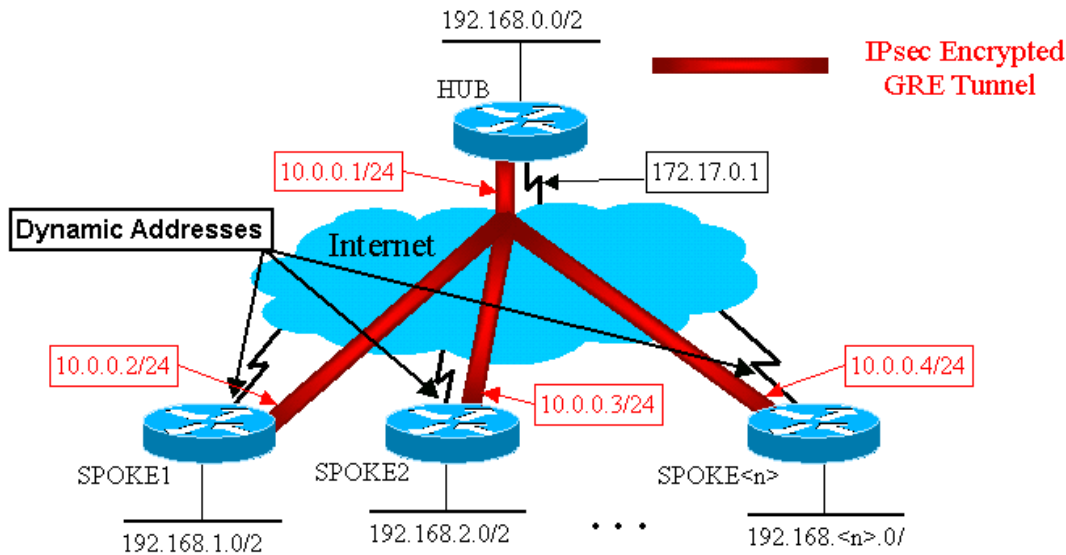
В новой настройке луча поддерживаются следующие функциональные возможности.

- Когда появляется интерфейс туннеля GRE, он запускает отсылку регистрационных пакетов NHRP маршрутизатору концентратора. Эти регистрационные пакеты NHRP инициируют IPsec. На лучевом маршрутизаторе настраиваются команды одноранговых узлов `<peer-address>` и `match ip access-list <ACL>`. ACL определяет GRE как протокол: любой в качестве источника, IP-адрес концентратора в качестве адреса назначения.

**Примечание.** Важно отметить, что в качестве источника в ACL используется любой адрес, т.к. IP-адрес лучевого маршрутизатора динамичен и потому не известен до тех пор, пока физический интерфейс не станет активным. Подсеть IP может использоваться как источник в ACL, если адрес динамического интерфейса "звезды" ограничивается адресом в данной подсети.

- Была использована команда `set security-association level per-host`, благодаря чему источник IP на IPsec прокси периферийного оборудования будет адресом текущего физического интерфейса периферийного оборудования (/32), а не адресом из ACL. Если какие-либо списки ACL использовались в качестве источника в IPsec-прокси, то другой краевой маршрутизатор не сможет настроить с помощью этого концентратора туннель IPsec+GRE. Это объясняется тем, что итоговый прокси IPsec на концентраторе идентичен команде `permit gre host 172.17.0.1 any`. Это означает, что все туннельные пакеты GRE, предназначенные для любого луча, зашифровываются и отправляются на первый луч, установивший туннель с концентратором, так как прокси-сервер IPSEC согласовывает пакеты GRE для каждого луча.
- Как только туннель IPsec настроен, пакет регистрации протокола NHRP передается от лучевого маршрутизатора на заданный сервер следующего узла. NHS является маршрутизатором концентратора в сети с топологией "звезда". Пакет регистрации протокола NHRP содержит данные, позволяющие маршрутизатору концентратора создавать отображение NHRP для лучевого маршрутизатора. С этим отображением маршрутизатор концентратора может пересылать одноадресные IP-пакеты данных для лучевого маршрутизатора через туннель mGRE+IPsec. Кроме этого, концентратор добавляет лучевой маршрутизатор в список многоадресного соответствия NHRP. После этого концентратор начнет отправку групповых пакетов динамической IP маршрутизации лучам (если настроен протокол динамической маршрутизации). Луч затем станет соседом протокола маршрутизации концентратора, и они обмениваются обновлениями маршрутизации.

### Звездообразные IPsec + mGRE



#### Маршрутизатор концентратора

```
version 12.3
!
hostname Hub
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
```

```

mode transport
!
crypto ipsec profile vpnprof
  set transform-set trans2
!
interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 600
  no ip split-horizon eigrp 1
  delay 1000
  tunnel source Ethernet0
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
!
interface Ethernet0
  ip address 172.17.0.1 255.255.255.0
!
interface Ethernet1
  ip address 192.168.0.1 255.255.255.0
!
router eigrp 1
  network 10.0.0.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
  no auto-summary
!

```

Обратите внимание, что в вышеприведенной настройке концентратора IP-адреса оконечных маршрутизаторов не настроены. IP-адреса внешнего физического интерфейса оконечного устройства и туннельного интерфейса сопоставления оконечного устройства определяются концентратором динамически по протоколу NHRP. Это позволяет динамически назначать IP-адрес внешнего физического интерфейс.

### ● Маршрутизатор луча 1 ●

```

version 12.3
!
hostname Spoke1
!
crypto isakmp policy 1
  authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
!
crypto map vpnmap1 local-address Ethernet0
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set security-association level per-host
  set transform-set trans2
  match address 101
!
interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.2 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.17.0.1
  tunnel key 100000
!
interface Ethernet0
  ip address dhcp hostname Spoke1
  crypto map vpnmap1
!

```

```
interface Ethernet1
 ip address 192.168.1.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.1.0 0.0.0.255
 no auto-summary
!
access-list 101 permit gre 172.16.1.0 0.0.0.255 host 172.17.0.1
```

## ● Маршрутизатор луча 2 ●

```
version 12.3
!
hostname Spoke2
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto map vpnmap1 local-address Ethernet0
crypto map vpnmap1 10 IPsec-isakmp
 set peer 172.17.0.1
 set security-association level per-host
 set transform-set trans2
 match address 101
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.3 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.1
 tunnel key 100000
!
interface Ethernet0
 ip address dhcp hostname Spoke2
 crypto map vpnmap1
!
interface Ethernet1
 ip address 192.168.2.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.1.0 0.0.0.255
 no auto-summary
!
access-list 101 permit gre 172.16.2.0 0.0.0.255 host 172.17.0.1
```

Основные параметры настройки, на которые необходимо обратить внимание:

- Внешний физический интерфейс (Ethernet0) использует динамический IP-адрес через DHCP.

**ip address dhcp hostname Spoke2**

- Зашифрованный ACL (101) определяет подсеть как источник для прокси-сервера IPsec.

**access-list 101 permit gre 172.16.2.0 0.0.0.255 host 172.17.0.1**

- Следующая команда в криптокарте IPsec служит для настройки сопоставлений безопасности для отдельных узлов.



## set security-association level per-host

- Все туннели входят в одну подсеть, т. к. все они соединяются через один многоточечный интерфейс GRE концентратора.

**ip address 10.0.0.2 255.255.255.0**

Комбинация этих трех команд делает ненужной настройку IP-адреса внешнего физического интерфейса луча. Используемый прокси-сервер IPsec будет основан скорее на узле, а не подсети.

Настройка на лучевых маршрутизаторах обязательно имеет заданный IP-адрес маршрутизатора концентратора, поскольку он должен инициировать туннель IPsec+GRE. Отметьте подобие настроек Spoke1 и Spoke2. Похожие настройки будут на всех лучевых маршрутизаторах. В большинстве случаев каждому лучу необходимо просто присвоить уникальный IP-адрес для их интерфейсов; остальные настройки будут одинаковы у всех лучей. Такой подход позволяет быстро настраивать и разворачивать много лучевых маршрутизаторов.

Данные NHRP в звездообразной сети выглядят следующим образом:

### Маршрутизатор концентратора

```
Hub#show ip nhrp
10.0.0.2/32 via 10.0.0.2, Tunnel0 created 01:25:18, expire 00:03:51
  Type: dynamic, Flags: authoritative unique registered
  NBMA address: 172.16.1.4
10.0.0.3/32 via 10.0.0.3, Tunnel0 created 00:06:02, expire 00:04:03
  Type: dynamic, Flags: authoritative unique registered
  NBMA address: 172.16.2.10
...
10.0.0.<n>/32 via 10.0.0.<n>, Tunnel0 created 00:06:00, expire 00:04:25
  Type: dynamic, Flags: authoritative unique registered
  NBMA address: 172.16.<n>.41
```

### Маршрутизатор луча 1

```
Spoke1#sho ip nhrp
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 4d08h, never expire
  Type: static, Flags: authoritative
  NBMA address: 172.17.0.1
```

## Динамическая многоточечная сеть типа "звезда"

Настройка на лучевых маршрутизаторах, описанная выше, не основывается на возможностях решения DMVPN, поэтому на них может быть запущено ПО Cisco IOS версий ранее 12.2(13)T. Настройка маршрутизатора концентратора зависит от функций DMVPN, поэтому на нем необходимо использовать Cisco IOS версии 12.2(13)T и выше. Это позволяет более гибко определять время обновления уже развернутых лучевых маршрутизаторов. Если на ваших маршрутизаторах также установлено программное обеспечение Cisco IOS версии 12.2(13)T и выше, тогда вы можете упростить настройку следующим образом.

### Маршрутизатор луча<n> (для версий ПО до Cisco IOS 12.2(13)T)

```
crypto map vpnmap1 10 IPsec-isakmp
set peer 172.17.0.1
set security-association level per-host
set transform-set trans2
match address 101
!
interface Tunnel0
```

```

bandwidth 1000
ip address 10.0.0.<n+1> 255.255.255.0
ip mtu 1400
ip nhrp authentication test
ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp network-id 100000
ip nhrp holdtime 300
ip nhrp nhs 10.0.0.1
delay 1000
tunnel source Ethernet0
tunnel destination 172.17.0.1
tunnel key 100000
!
interface Ethernet0
ip address dhcp hostname Spoke<n>
crypto map vpnmap1
!
. . .
!
access-list 101 permit gre any host 172.17.0.1

```

### ● Маршрутизатор луча<n> (для версий ПО выше Cisco IOS 12.2(13)T) ●

```

crypto ipsec profile vpnprof
set transform-set trans2
!
interface Tunnel0
bandwidth 1000
ip address 10.0.0.<n+1> 255.255.255.0
ip mtu 1400
ip nhrp authentication test
ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp network-id 100000
ip nhrp holdtime 300
ip nhrp nhs 10.0.0.1
delay 1000
tunnel source Ethernet0
tunnel destination 172.17.0.1
tunnel key 100000
tunnel protection ipsec profile vpnprof
!
interface Ethernet0
ip address dhcp hostname Spoke<n>
!

```

Обратите внимание, что было сделано следующее:

1. Команда **crypto map vpnmap1 10 ipsec-isakmp** заменена командой **crypto ipsec profile vpnprof**.
2. Команда **crypto map vpnmap1** была удалена из интерфейса Ethernet0, и команда **tunnel protection ipsec profile vpnprof** добавлена на интерфейс Tunnel0.
3. Удален зашифрованный ACL, **access-list 101 permit gre any host 172.17.0.1**.

В этом случае адреса равноправных пользователей и прокси протокола IPsec автоматически выводятся из настройки **источника ...** и **назначения тунеля ...**. Одноранговые узлы и прокси-серверы (в результате команды **show crypto ipsec sa**):

```

...
local ident (addr/mask/prot/port):    (172.16.1.24/255.255.255.255/47/0)
remote ident (addr/mask/prot/port):   (172.17.0.1/255.255.255.255/47/0)
...
local crypto endpt.: 172.17.1.24, remote crypto endpt.:172.17.0.1
...

```

В общих словах, следующие полные настройки включают все изменения, сделанные в базовой настройке (звездообразные IPsec+GRE).

### ● Маршрутизатор концентратора ●

```
version 12.3
!
hostname Hub
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp holdtime 600
 no ip split-horizon eigrp 1
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address 172.17.0.1 255.255.255.0
!
interface Ethernet1
 ip address 192.168.0.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.0.0 0.0.0.255
 no auto-summary
!
```

Нет изменений настройки концентратора.

### ● Маршрутизатор луча 1 ●

```
version 12.3
!
hostname Spoke1
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.2 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp network-id 100000
```

```

ip nhrp holdtime 300
ip nhrp nhs 10.0.0.1
delay 1000
tunnel source Ethernet0
tunnel destination 172.17.0.1
tunnel key 100000
tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke2
!
interface Ethernet1
 ip address 192.168.1.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.1.0 0.0.0.255
 no auto-summary
!

```

## ● Маршрутизатор луча 2 ●

```

version 12.3
!
hostname Spoke2
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.3 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.1
 tunnel key 100000
tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke2
!
interface Ethernet1
 ip address 192.168.2.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.2.0 0.0.0.255
 no auto-summary
!

```

## Динамическая многоточечная VPN с поддержкой IPsec

В этом разделе концепции и настройки показывают все возможности динамической многоточечной виртуальной частной сети (DMVPN). NHRP дает возможность лучевым маршрутизаторам динамически запоминать адреса внешних физических интерфейсов других лучевых маршрутизаторов в сети VPN. Это означает, что лучевой маршрутизатор получает достаточный объем информации для динамического создания туннеля IPsec+mGRE к другим лучевым маршрутизаторам. Эта возможность является преимуществом, если трафик данных между двумя лучами передается через маршрутизатор концентратора. Затем трафик должен быть

зашифрован/расшифрован, при этом время задержки и нагрузка на маршрутизаторе концентратора увеличиваются вдвое. Для использования этой функции лучевые маршрутизаторы должны быть скомутированы от двухточечных GRE (p-pGRE) до туннельных интерфейсов многоточечной GRE (mGRE). Им тоже нужно знать (под)сети, доступные за другими лучами с помощью IP следующего перехода IP-адреса туннеля другого лучевого маршрутизатора. Лучевые маршрутизаторы запоминают эти (под)сети с помощью динамического протокола IP маршрутизации через туннель IPsec+mGRE с концентратором.

Динамический протокол IP-маршрутизации, запущенный на маршрутизаторе концентратора, можно настроить для отображения маршрутов, обнаруженных на одном лучевом маршрутизаторе, восстанавливая тот же интерфейс на остальных лучевых маршрутизаторах, однако следующим IP-узлом в таких маршрутах, как правило, является центральный, а не лучевой маршрутизатор, на котором был обнаружен этот маршрут.

**Примечание.** Протокол динамической маршрутизации работает только на концентраторе и каналах лучей. Он не работает в динамических каналах между лучами.

Протоколы динамической маршрутизации (RIP, OSPF и EIGRP) должны быть настроены на концентраторе для декларации обратных маршрутов из интерфейса туннеля mGRE и для задания вызывающего лучевого маршрутизатора в качестве следующего IP-узла для маршрутов, полученных от одного луча при декларации маршрута другим.

Это требования для настроек протокола маршрутизации.

## RIP

Нужно отключить разделение горизонтов на туннельном интерфейсе mGRE концентратора, иначе EIGRP не поместит маршруты, полученные по интерфейсу mGRE, обратно в этот интерфейс.

```
no ip split-horizon
```

В других изменениях нет необходимости. RIP автоматически использует оригинальный IP следующего перехода на объявленных маршрутах, на которых он восстанавливает тот же интерфейс, откуда они были получены.

## EIGRP

Нужно отключить разделение горизонтов на туннельном интерфейсе mGRE концентратора, иначе EIGRP не поместит маршруты, полученные по интерфейсу mGRE, обратно в этот интерфейс.

```
no ip split-horizon eigrp <as>
```

По умолчанию EIGRP назначит следующий узел IP маршрутизатором концентратора для маршрутов, которые он объявляет, даже если объявление этих маршрутов восстанавливает тот же интерфейс, откуда они были получены. Поэтому в данном случае необходима следующая команда настройки, чтобы предписать EIGRP использовать исходный IP-адрес следующего перехода при объявлении этих маршрутов.

```
no ip next-hop-self eigrp <as>
```

**Примечание.** Команда `no ip next-hop-self eigrp <as>` доступна в ПО Cisco IOS выпуск 12.3(2) и выше. Для Cisco IOS версий от 12.2(13)T до 12.3(2) выполните следующие действия:

- Если создание динамических туннелей между лучами нежелательно, использовать указанную выше команду нет необходимости.
- Если необходимы динамические туннели между лучами, то необходимо использовать коммутирование туннельного интерфейса

на лучевых маршрутизаторах.

- В противном случае вам придется использовать другой протокол маршрутизации для DMVPN.

## OSPF

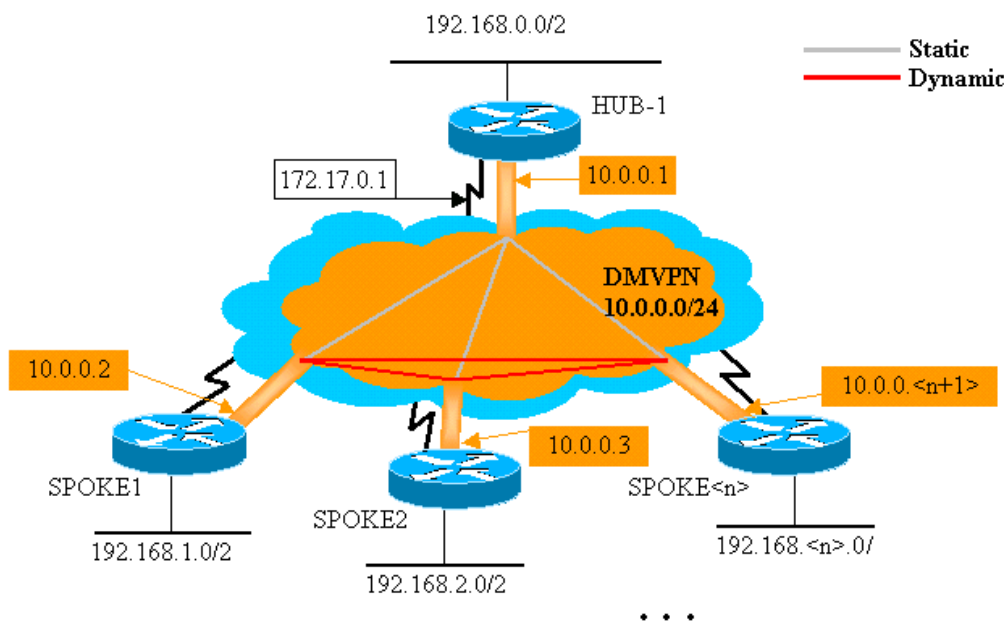
Так как OSPF является протоколом маршрутизации на основе состояния каналов, проблемы с разделением диапазонов не возникают. Обычно при использовании многоточечных интерфейсов для соединений точка-множество точек настраивается сеть типа OSPF, однако это приведет к тому, что OSPF добавит маршруты узла в таблицы маршрутизации на лучевых маршрутизаторах. Маршруты этих узлов являются причиной того, что пакеты, предназначенные для сетей за другими лучевыми маршрутизаторами, будут перенаправлены через концентратор вместо направления непосредственно к другому лучу. Чтобы обойти эту проблему, настройте широковещательный тип сети OSPF с помощью команды.

```
ip ospf network broadcast
```

Необходимо также убедиться, что маршрутизатор концентратора является выделенным маршрутизатором (DR) для сети IPsec+mGRE. Чтобы сделать это, установите для приоритета OSPF такие значения: на концентраторе — больше 1, а на лучах — 0.

- Концентратор: `ip ospf priority 2`
- Луч: `ip ospf priority 0`

## Одиночный концентратор DMVPN



● Маршрутизатор концентратора ●

```
version 12.3
!
hostname Hub
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
```

```

mode transport
!
crypto ipsec profile vpnprof
  set transform-set trans2
!
interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 600
  ip ospf network broadcast
  ip ospf priority 2
  delay 1000
  tunnel source Ethernet0
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
!
interface Ethernet0
  ip address 172.17.0.1 255.255.255.0
!
interface Ethernet1
  ip address 192.168.0.1 255.255.255.0
!
router ospf 1
network 10.0.0.0 0.0.0.255 area 0
network 192.168.0.0 0.0.0.255 area 0
!

```

Единственное изменение настройки концентратора – это использование протокола маршрутизации OSPF вместо EIGRP. Обратите внимание, что тип сети OSPF - широковещательный, уровень приоритета - 2. Установка широковещательного типа сети OSPF вынудит OSPF установить маршруты для сетей за лучевыми маршрутизаторами с помощью IP-адреса следующего перехода как туннельного адреса GRE для данного лучевого маршрутизатора.

### ● Маршрутизатор луча 1 ●

```

version 12.3
!
hostname Spoke1
!
crypto isakmp policy 1
  authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
mode transport
!
crypto ipsec profile vpnprof
  set transform-set trans2
!
interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.2 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast 172.17.0.1
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  ip ospf network broadcast
  ip ospf priority 0
  delay 1000
  tunnel source Ethernet0
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
!
interface Ethernet0
  ip address dhcp hostname Spoke1
!
interface Ethernet1

```

```
ip address 192.168.1.1 255.255.255.0
!
router ospf 1
network 10.0.0.0 0.0.0.255 area 0
network 192.168.1.0 0.0.0.255 area 0
!
```

Настройка для лучевых маршрутизаторов теперь очень похожа на настройку для концентратора. Различия:

- Приоритет OSPF установлен на 0. Маршрутизаторы в топологии "звезда" не могут стать выделенным маршрутизатором для широковещательной сети с множественным доступом (NBMA) на основе протокола mGRE. Прямое статическое соединение со всеми лучевыми маршрутизаторами предусмотрено только для маршрутизатора концентратора. DR должен иметь доступ ко всем участникам сети NBMA.
- Для маршрутизатора концентратора настроены одноадресное и многоадресное сопоставления NHRP.

```
ip nhrp map multicast 172.17.0.1
ip nhrp map 10.0.0.1 172.17.0.1
```

В предыдущей настройке команда **ip nhrp map multicast ...** не использовалась, т. к. туннель GRE был двухточечным. В этом случае многоадресные пакеты автоматически инкапсулируются через туннель в единственно возможное место назначения. Теперь необходимо использовать эту команду, т.к. туннель между лучами GRE стал многоточечным, и однозначного места назначения не существует.

- Когда лучевой маршрутизатор активируется, он должен инициировать туннель с концентратором, поскольку маршрутизатор концентратора не имеет изначально какой-либо информации о лучевых маршрутизаторах, которые могут иметь динамические IP-адреса. Лучевые маршрутизаторы тоже настроены таким образом, что концентратор является их NHRP NHS.

```
ip nhrp nhs 10.0.0.1
```

При использовании вышеуказанной команды лучевой маршрутизатор отправляет пакеты регистрации NHRP через туннель mGRE+IPsec на маршрутизатор концентратора через равные промежутки времени. Эти пакеты регистрации обеспечивают данные отображения NHRP для луча необходимые маршрутизатору концентратора для туннелирования пакетов обратно лучевым маршрутизаторам.

## ● Маршрутизатор луча 2 ●

```
version 12.3
!
hostname Spoke2
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.3 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast 172.17.0.1
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 ip ospf network broadcast
```



```

ip ospf priority 0
delay 1000
tunnel source Ethernet0
tunnel mode gre multipoint
tunnel key 100000
tunnel protection ipsec profile vpnprof
!
interface Ethernet0
ip address dhcp hostname Spokel
!
interface Ethernet1
ip address 192.168.3.1 255.255.255.0
!
router ospf 1
network 10.0.0.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0
!

```

## ● Маршрутизатор луча<n> ●

```

version 12.3
!
hostname Spoke<n>
!
crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
mode transport
!
crypto ipsec profile vpnprof
set transform-set trans2
!
interface Tunnel0
bandwidth 1000
ip address 10.0.0.<n+1> 255.255.255.0
ip mtu 1400
ip nhrp authentication test
ip nhrp map multicast 172.17.0.1
ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp network-id 100000
ip nhrp holdtime 300
ip nhrp nhs 10.0.0.1
ip ospf network broadcast
ip ospf priority 0
delay 1000
tunnel source Ethernet0
tunnel mode gre multipoint
tunnel key 100000
tunnel protection ipsec profile vpnprof
!
interface Ethernet0
ip address dhcp hostname Spoke<n>
!
interface Ethernet1
ip address 192.168.<n>.1 255.255.255.0
!
router ospf 1
network 10.0.0.0 0.0.0.255 area 0
network 192.168.<n>.0 0.0.0.255 area 0
!

```

Обратите внимание, что настройки всех лучевых маршрутизаторов схожи. Единственное различие - это IP-адреса локальных интерфейсов. Это помогает при разворачивании большого количества лучевых маршрутизаторов. Все лучевые маршрутизаторы могут быть настроены одинаково, необходимо только добавить адреса локального IP-интерфейса.

На этом этапе обратите внимание на таблицы маршрутизации и таблицы соответствий NHRP на маршрутизаторах концентратора, луча1 и луча 2 для получения начальных условий (сразу после включения луча 1 и 2), а также условий после установления динамической связи между лучами 1 и 2.

## Начальные условия

### Информация о маршрутизаторе концентратора

```
Hub#show ip route
 172.17.0.0/24 is subnetted, 1 subnets
C    172.17.0.0 is directly connected, Ethernet0
 10.0.0.0/24 is subnetted, 1 subnets
C    10.0.0.0 is directly connected, Tunnel0
C   192.168.0.0/24 is directly connected, Ethernet1
O   192.168.1.0/24 [110/2] via 10.0.0.2, 00:19:53, Tunnel0
O   192.168.2.0/24 [110/2] via 10.0.0.3, 00:19:53, Tunnel0
Hub#show ip nhrp
10.0.0.2/32 via 10.0.0.2, Tunnel0 created 00:57:27, expire    00:04:13
  Type: dynamic, Flags: authoritative unique registered
  NBMA address: 172.16.1.24
10.0.0.3/32 via 10.0.0.3, Tunnel0 created 07:11:25, expire    00:04:33
  Type: dynamic, Flags: authoritative unique registered
  NBMA address: 172.16.2.75
Hub#show crypto engine connection active
ID  Interface  IP-Address  State Algorithm          Encrypt Decrypt
204 Ethernet0  172.17.0.1  set  HMAC_SHA+DES_56_CB    0      0
205 Ethernet0  172.17.0.1  set  HMAC_SHA+DES_56_CB    0      0
2628 Tunnel0    10.0.0.1    set  HMAC_MD5               0     402
2629 Tunnel0    10.0.0.1    set  HMAC_MD5               357    0
2630 Tunnel0    10.0.0.1    set  HMAC_MD5               0     427
2631 Tunnel0    10.0.0.1    set  HMAC_MD5               308    0
```

### Информация о маршрутизаторе луча 1

```
Spoke1#show ip route
 172.16.0.0/24 is subnetted, 1 subnets
C    172.16.1.24 is directly connected, Ethernet0
 10.0.0.0/24 is subnetted, 1 subnets
C    10.0.0.0 is directly connected, Tunnel0
O   192.168.0.0/24 [110/2] via 10.0.0.1, 00:31:46, Tunnel0
C   192.168.1.0/24 is directly connected, Ethernet1
O   192.168.2.0/24 [110/2] via 10.0.0.3, 00:31:46, Tunnel0
Spoke1#show ip nhrp
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 01:42:00, never expire
  Type: static, Flags: authoritative used
  NBMA address: 172.17.0.1
Spoke1#show crypto engine connection active
ID  Interface  IP-Address  State Algorithm          Encrypt Decrypt
  2 Ethernet0  172.16.1.24  set  HMAC_SHA+DES_56_CB    0      0
2064 Tunnel0    10.0.0.2    set  HMAC_MD5               0     244
2065 Tunnel0    10.0.0.2    set  HMAC_MD5               276    0
```

### Информация о маршрутизаторе луча 2

```
Spoke2#show ip route
 172.16.0.0/24 is subnetted, 1 subnets
C    172.16.2.0 is directly connected, Ethernet0
 10.0.0.0/24 is subnetted, 1 subnets
C    10.0.0.0 is directly connected, Tunnel0
O   192.168.0.0/24 [110/2] via 10.0.0.1, 00:38:52, Tunnel0
O   192.168.1.0/24 [110/2] via 10.0.0.2, 00:38:52, Tunnel0
C   192.168.2.0/24 is directly connected, Ethernet1
Spoke2#show ip nhrp
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 01:32:10, never expire
  Type: static, Flags: authoritative used
  NBMA address: 172.17.0.1
Spoke2#show crypto engine connection active
ID  Interface  IP-Address  State Algorithm          Encrypt Decrypt
 17 Ethernet0  172.16.2.75  set  HMAC_SHA+DES_56_CB    0      0
2070 Tunnel0    10.0.0.3    set  HMAC_MD5               0     279
```

```
2071 Tunnel0      10.0.0.3      set  HMAC_MD5      316      0
```

На этом шаге проверяется доступность адресата от 192.168.1.2 на 192.168.2.3. Эти адреса предназначены для узлов за маршрутизаторами луча1 и луча2 соответственно. Приведенная далее последовательность событий обеспечивает организацию прямого туннеля mGRE+IPsec между лучами.

1. Маршрутизатор луча1 получает пакет эхо-запроса с адресом назначения 192.168.2.3. Он ищет место назначения в таблице маршрутизации и обнаруживает, что должен передать этот пакет за пределы интерфейса Tunnel0 на IP-адрес следующего перехода, 10.0.0.3.
2. Лучевой маршрутизатор 1 проверяет таблицу коммутации NHRP для 10.0.0.3 и обнаруживает отсутствие входа. Маршрутизатор луча 1 создаёт ответный пакет разрешения NHRP и посылает его на NHS (маршрутизатор концентратора).
3. Маршрутизатор концентратора проверяет по таблице сопоставления NHRP адрес назначения 10.0.0.3 и обнаруживает, что он сопоставлен с адресом 172.16.2.75. Маршрутизатор концентратора создаёт ответный пакет разрешения NHRP и посылает его на маршрутизатор луча 1.
4. Маршрутизатор луча 1 получает ответ NHRP и вносит соответствие 10.0.0.3 >172.16.2.75 в таблицу маршрутизации NHRP. Включение IPsec-триггеров сопоставления NHRP для инициации туннельного соединения с одноранговым узлом 172.16.2.75.
5. Маршрутизатор луча 1 активизирует ISAKMP с адресом 172.16.2.75 и настраивает связь между ISAKMP и IPsec SAs. Прокси-сервер IPsec выводится из команды Tunnel0 **tunnel source <address>** и соответствий NHRP.

```
local ident (addr/mask/prot/port): (172.16.1.24/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.16.2.75/255.255.255.255/47/0)
```

6. При завершении организации туннеля IPsec все последующие пакеты данных, поступающие к подсети 192.168.2.0/24, будут передаваться напрямую к лучу 2.
7. После пересылки на узел пакета, предназначенного для 192.168.2.3, этот узел вышлет обратный пакет на 192.168.1.2. Когда маршрутизатор луча 2 получает этот пакет, предназначенный для 192.168.1.2, он будет искать этот адрес в таблице маршрутизации и обнаружит, что необходимо переадресовать этот пакет через интерфейс Tunnel0 на следующий IP-адрес пересылки, 10.0.0.2.
8. Маршрутизатор луча 2 проверяет таблицу коммутации NHRP для 10.0.0.2 и обнаруживает отсутствие записи. Маршрутизатор луча 2 создаёт ответный пакет разрешения NHRP и посылает его на NHS (маршрутизатор концентратора).
9. Маршрутизатор концентратора проверяет по таблице сопоставления NHRP адрес назначения 10.0.0.2 и обнаруживает, что он сопоставлен с адресом 172.16.1.24. Маршрутизатор концентратора создаёт ответный пакет разрешения NHRP и посылает его на маршрутизатор луча 2.
10. Маршрутизатор луча 2 получает ответ NHRP и вносит соответствие 10.0.0.2 >172.16.1.24 в таблицу маршрутизации NHRP. Добавление сопоставления NHRP инициирует создание туннеля IPsec с узлом 172.16.1.24, но такой туннель уже существует, поэтому дальнейшие действия не требуются.
11. Лучи 1 и 2 могут теперь пересылать друг другу пакеты напрямую. Если для пересылки пакетов на протяжении периода удержания сопоставление NHRP не используется, сопоставление NHRP будет удалено. Удаление записи сопоставления NHRP инициирует удаление IPsec SA для этого прямого подключения.

## Условия после установки динамического канала между лучами 1 и 2

### ● Информация о маршрутизаторе луча 1 ●

```
Spoke1#show ip nhrp
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 02:34:16, never expire
  Type: static, Flags: authoritative used
  NBMA address: 172.17.0.1
10.0.0.3/32 via 10.0.0.3, Tunnel0 created 00:00:05, expire 00:03:35
  Type: dynamic, Flags: router unique used
  NBMA address: 172.16.2.75
Spoke1#show crypto engine connection active
```

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
2	Ethernet0	172.16.1.24	set	HMAC_SHA+DES_56_CB	0	0
3	Ethernet0	172.16.1.24	set	HMAC_SHA+DES_56_CB	0	0
2064	Tunnel0	10.0.0.2	set	HMAC_MD5	0	375
2065	Tunnel0	10.0.0.2	set	HMAC_MD5	426	0
2066	Tunnel0	10.0.0.2	set	HMAC_MD5	0	20
2067	Tunnel0	10.0.0.2	set	HMAC_MD5	19	0

## ● Информация о маршрутизаторе луча 2 ●

```
Spoke2#show ip nhrp
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 02:18:25, never expire
  Type: static, Flags: authoritative used
  NBMA address: 172.17.0.1
10.0.0.2/32 via 10.0.0.2, Tunnel0 created 00:00:24, expire 00:04:35
  Type: dynamic, Flags: router unique used
  NBMA address: 172.16.1.24
Spoke2#show crypto engine connection active
ID Interface IP-Address State Algorithm Encrypt Decrypt
 17 Ethernet0 172.16.2.75 set HMAC_SHA+DES_56_CB 0 0
 18 Ethernet0 172.16.2.75 set HMAC_SHA+DES_56_CB 0 0
2070 Tunnel0 10.0.0.3 set HMAC_MD5 0 407
2071 Tunnel0 10.0.0.3 set HMAC_MD5 460 0
2072 Tunnel0 10.0.0.3 set HMAC_MD5 0 19
2073 Tunnel0 10.0.0.3 set HMAC_MD5 20 0
```

Из приведенного выше примера видно, что лучи 1 и 2 получили NHRP-сопоставления друг друга от маршрутизатора концентратора, построили туннель mGRE+IPsec и используют его. Срок действия сопоставлений NHRP закончится через пять минут (текущее значение времени хранения NHRP = 300 секунд). Если сопоставления NHRP используются в течение последней минуты, то будет послан запрос и ответ разрешения NHRP для обновления значения до его удаления. Иначе, схема NHRP будет уничтожена и будет инициирована IPsec очистка.

## VPN с динамическим многоточечным IPsec с двумя концентраторами

Добавив несколько строк настройки на лучевые маршрутизаторы, можно установить маршрутизаторы двух (и больше) концентраторов (для избыточности). Существует 2 способа настроить DMVPN с двумя концентраторами.

- Одиночная сеть DMVPN, в которой каждый луч использует одиночный одноточечный интерфейс туннеля GRE и которая указывает на два разных концентратора как на ее сервер следующего перехода (NHS).

На маршрутизаторе концентратора предусмотрен только один многоточечный туннельный интерфейс GRE.

- Двойные сети DMVPN, где у каждого луча есть два туннельных интерфейса GRE (или двухточечный, или многоточечный), а каждый туннель GRE подключен к различным маршрутизаторам концентраторов.

Снова, на маршрутизаторе концентратора предусмотрен только один многоточечный туннельный интерфейс GRE.

В следующих примерах приведены настройки этих двух сценариев для сетей DMVPN с двумя концентраторами.. В обоих случаях выделены отличия от настройки DMVPN с одним концентратором.

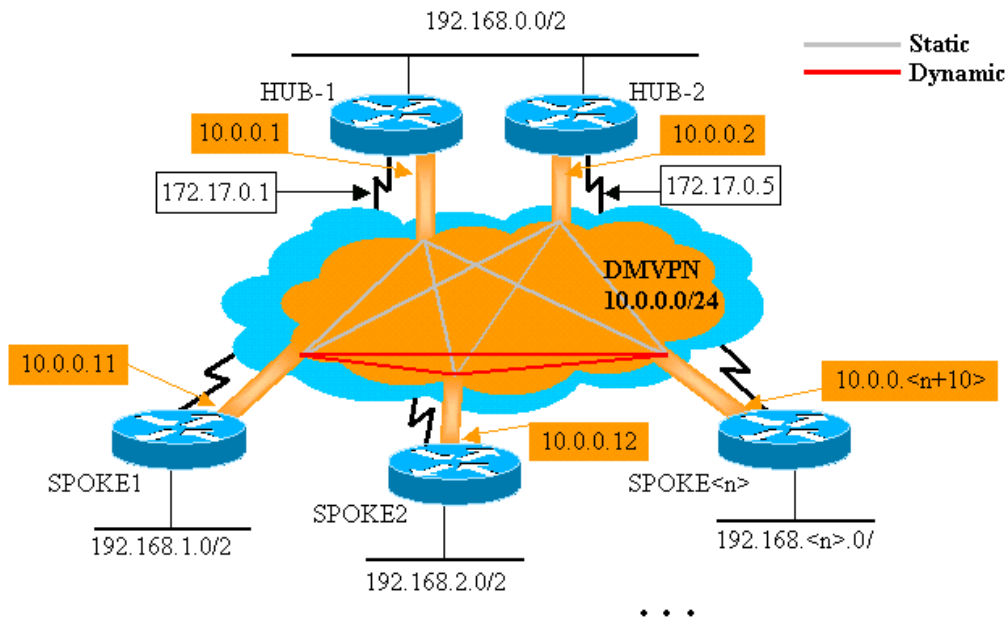
## Схема "Двойной концентратор – одинарный DMVPN"

Система с двумя концентраторами и одной сетью DMVPN достаточно проста в настройке, однако в ней не обеспечивается управление маршрутизацией по сети DMVPN такого уровня, как в системах с двумя концентраторами и двумя сетями DMVPN. Главная идея заключается в том, чтобы иметь единое "облако" DMVPN со всеми концентраторами (в данном случае с двумя) и подключить все лучи к этой одиночной сети ("облаку"). Статическое NHRP-сопоставление лучей и концентраторов определяет статический канал IPsec+mGRE, в котором выполняется протокол динамической маршрутизации. Динамический протокол маршрутизации не будет выполняться в динамической линии связи IPsec+mGRE между лучами. Поскольку лучевые маршрутизаторы маршрутизируют соседей

с маршрутизаторами концентраторов через тот же туннельный интерфейс mGRE, то нельзя использовать различия настройки интерфейсов (такие как полоса пропускания, стоимость и задержка) и канала для изменения метрики протокола динамической маршрутизации, чтобы предпочесть один концентратор другому, когда они работают оба. Если это предпочтение необходимо, следует использовать внутренние методы для настройки протокола маршрутизации. Поэтому в качестве протокола динамической маршрутизации лучше использовать EIGRP или RIP, а не OSPF.

**Примечание.** Эта проблема характерна только для расположенных рядом концентраторов. В противном случае при стандартной динамической маршрутизации будет выбран правильный маршрутизатор концентратора, даже если доступ к сети назначения возможен и через другой маршрутизатор концентратора.

### Dual Hub - Single DMVPN Layout



#### Маршрутизатор концентратора

```

version 12.3
!
hostname Hub1
!
crypto isakmp policy 1
 authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp holdtime 600
 ip ospf network broadcast
 ip ospf priority 2
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0

```

```
ip address 172.17.0.1 255.255.255.0
!
interface Ethernet1
ip address 192.168.0.1 255.255.255.0
!
router ospf 1
network 10.0.0.0 0.0.0.255 area 1
network 192.168.0.0 0.0.0.255 area 0
!
```

## ● Маршрутизатор концентратора 2 ●

```
version 12.3
!
hostname Hub2
!
crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
mode transport
!
crypto ipsec profile vpnprof
set transform-set trans2
!
interface Tunnel0
bandwidth 900
ip address 10.0.0.2 255.255.255.0
ip mtu 1400
ip nhrp authentication test
ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp map multicast 172.17.0.1
ip nhrp map multicast dynamic
ip nhrp network-id 100000
ip nhrp holdtime 600
ip nhrp nhs 10.0.0.1
ip ospf network broadcast
ip ospf priority 1
delay 1000
tunnel source Ethernet0
tunnel mode gre multipoint
tunnel key 100000
tunnel protection ipsec profile vpnprof
!
interface Ethernet0
ip address 172.17.0.5 255.255.255.0
!
interface Ethernet1
ip address 192.168.0.2 255.255.255.0
!
router ospf 1
network 10.0.0.0 0.0.0.255 area 1
network 192.168.0.0 0.0.0.255 area 0
!
```

Единственное различие в настройке концентратора 1 - это использование OSPF двух областей. Область 0 закреплена за сетью, находящейся позади двух концентраторов, а область 1 – за сетью DMVPN и сетями позади лучевых маршрутизаторов. OSPF мог бы использовать одну область, но для демонстрации настройки для нескольких областей OSPF в этом примере использовались две области.

Настройка концентратора 2 в основном совпадает с настройкой концентратора 1 при изменении соответствующего IP-адреса. Главное отличие состоит в том, что концентратор 2 также является лучом (или клиентом) концентратора 1; т.е. концентратор 1 является главным, а концентратор 2 - дополнительным. Это сделано для того, чтобы концентратор 2 стал соседом OSPF, и концентратор 1 работал через туннель mGRE. Поскольку концентратор 1 – это выделенный маршрутизатор OSPF DR, он должен иметь прямое соединение со всеми другими маршрутизаторам OSPF через интерфейс mGRE (сеть NBMA). Без наличия прямой связи между концентраторами 1 и 2 концентратор 2 не сможет участвовать в маршрутизации OSPF при работающем концентраторе 1. Когда отключается концентратор 1, концентратор 2 выступает в роли OSPF DR для DMVPN (сеть NBMA). При повторном включении концентратора 1 он снова станет главным, будучи маршрутизатором назначения OSPF для сети DMVPN.

Маршрутизаторы за концентратором 1 и 2 будут использовать концентратор 1 для передачи пакетов лучевым сетям, поскольку пропускная способность интерфейса туннеля GRE установлена на 1000 Кб/сек, что на 100 Кб/сек больше, чем у концентратора 2. Лучевые маршрутизаторы, напротив, отправляют пакеты, предназначенные для сетей за маршрутизаторами, на Hub1 и Hub2, т. к. на каждом лучевом маршрутизаторе есть только один туннельный интерфейс mGRE и два равноценных маршрута. Использование балансировки нагрузки по пакетам может привести к нарушению последовательности пакетов.

### Маршрутизатор луча 1

```
version 12.3
!
hostname Spoke1
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.11 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast 172.17.0.1
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp map multicast 172.17.0.5
 ip nhrp map 10.0.0.2 172.17.0.5
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 ip nhrp nhs 10.0.0.2
 ip ospf network broadcast
 ip ospf priority 0
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke1
!
interface Ethernet1
 ip address 192.168.1.1 255.255.255.0
!
 router ospf 1
 network 10.0.0.0 0.0.0.255 area 1
 network 192.168.1.0 0.0.0.255 area 1
!
```

Различие в настройке лучевых маршрутизаторов следующее:

- Лучевой маршрутизатор в новой настройке настроен со статическими сопоставлениями NHRP для концентратора 2, и концентратор 2 добавлен как сервер следующего перехода.

Исходный:

```
ip nhrp map multicast 172.17.0.1
ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp nhs 10.0.0.1
```

Новый:

```
ip nhrp map multicast 172.17.0.1
ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp map multicast 172.17.0.5
ip nhrp map 10.0.0.2 172.17.0.5
ip nhrp nhs 10.0.0.1
ip nhrp nhs 10.0.0.2
```

- Области OSPF для лучевых маршрутизаторов были изменены на область 1.

Помните, что определение статического отображения NHRP и сервера NHS на маршрутизаторе луча для концентратора необходимо для того, чтобы обеспечить работу протокола динамической маршрутизации в этом туннеле. Это определяет концентратор и лучевую маршрутизацию или соседнюю сеть. Учтите, что концентратор 2 используется для всех лучей и сам является лучом для концентратора 1. Это облегчает проектирование, настройку и изменение сетей со структурой "звезда" при использовании решений DMVPN (динамических многоотводных виртуальных частных сетей).

### Маршрутизатор луча 2

```
version 12.3
!
hostname Spoke2
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.12 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast 172.17.0.1
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp map multicast 172.17.0.5
 ip nhrp map 10.0.0.2 172.17.0.5
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 ip nhrp nhs 10.0.0.2
 ip ospf network broadcast
 ip ospf priority 0
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke1
!
interface Ethernet1
 ip address 192.168.2.1 255.255.255.0
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
!
```

### Маршрутизатор луча<n>

```
version 12.3
```



```

!
hostname Spoke<n>
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.<n+10> 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast 172.17.0.1
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp map multicast 172.17.0.5
 ip nhrp map 10.0.0.2 172.17.0.5
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 ip nhrp nhs 10.0.0.2
 ip ospf network broadcast
 ip ospf priority 0
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke<x>
!
interface Ethernet1
 ip address 192.168.<n>.1 255.255.255.0
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
 network 192.168.<n>.0 0.0.0.255 area 0
!

```

На этом этапе обратите внимание на таблицы маршрутизации, таблицы соответствий NHRP и соединения IPsec на маршрутизаторах концентратора 1 и 2, луча1 и 2 для получения начальных условий (сразу после включения луча 1 и 2).

## Начальные условия и изменения

### Информация о маршрутизаторе концентратора 1

```

Hub1#show ip route
 172.17.0.0/24 is subnetted, 1 subnets
C    172.17.0.0 is directly connected, Ethernet0
 10.0.0.0/24 is subnetted, 1 subnets
C    10.0.0.0 is directly connected, Tunnel0
C    192.168.0.0/24 is directly connected, Ethernet1
O    192.168.1.0/24 [110/2] via 10.0.0.11, 00:02:17, Tunnel0
O    192.168.2.0/24 [110/2] via 10.0.0.12, 00:02:17, Tunnel0
Hub1#show ip nhrp
10.0.0.2/32 via 10.0.0.2, Tunnel0 created 1w3d, expire 00:03:15
  Type: dynamic, Flags: authoritative unique registered
  NBMA address: 172.17.0.5
10.0.0.11/32 via 10.0.0.11, Tunnel0 created 1w3d, expire 00:03:49
  Type: dynamic, Flags: authoritative unique registered
  NBMA address: 172.16.1.24
10.0.0.12/32 via 10.0.0.12, Tunnel0 created 1w3d, expire 00:04:06
  Type: dynamic, Flags: authoritative unique registered
  NBMA address: 172.16.2.75
Hub1#show crypto engine connection active

```

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
4	Ethernet0	172.17.0.1	set	HMAC_SHA+DES_56_CB	0	0
5	Ethernet0	172.17.0.1	set	HMAC_SHA+DES_56_CB	0	0

6	Ethernet0	172.17.0.1	set	HMAC_SHA+DES_56_CB	0	0
3532	Tunnel0	10.0.0.1	set	HMAC_MD5+DES_56_CB	0	232
3533	Tunnel0	10.0.0.1	set	HMAC_MD5+DES_56_CB	212	0
3534	Tunnel0	10.0.0.1	set	HMAC_MD5+DES_56_CB	0	18
3535	Tunnel0	10.0.0.1	set	HMAC_MD5+DES_56_CB	17	0
3536	Tunnel0	10.0.0.1	set	HMAC_MD5+DES_56_CB	0	7
3537	Tunnel0	10.0.0.1	set	HMAC_MD5+DES_56_CB	7	0

## Информация о маршрутизаторе концентратора 2

```
Hub2#show ip route
 172.17.0.0/24 is subnetted, 1 subnets
C    172.17.0.0 is directly connected, Ethernet0
 10.0.0.0/24 is subnetted, 1 subnets
C    10.0.0.0 is directly connected, Tunnel0
C    192.168.0.0/24 is directly connected, Ethernet1
O    192.168.1.0/24 [110/2] via 10.0.0.11, 00:29:15, Tunnel0
O    192.168.2.0/24 [110/2] via 10.0.0.12, 00:29:15, Tunnel0
Hub2#show ip nhrp
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 1w3d, never expire
  Type: static, Flags: authoritative used
  NBMA address: 172.17.0.1
10.0.0.11/32 via 10.0.0.11, Tunnel0 created 1w3d, expire 00:03:15
  Type: dynamic, Flags: authoritative unique registered
  NBMA address: 172.16.1.24
10.0.0.12/32 via 10.0.0.12, Tunnel0 created 00:46:17, expire 00:03:51
  Type: dynamic, Flags: authoritative unique registered
  NBMA address: 172.16.2.75
Hub2#show crypto engine connection active
ID Interface IP-Address State Algorithm Encrypt Decrypt
 4 Ethernet0 171.17.0.5 set HMAC_SHA+DES_56_CB 0 0
 5 Ethernet0 171.17.0.5 set HMAC_SHA+DES_56_CB 0 0
 6 Ethernet0 171.17.0.5 set HMAC_SHA+DES_56_CB 0 0
3520 Tunnel0 10.0.0.2 set HMAC_MD5+DES_56_CB 0 351
3521 Tunnel0 10.0.0.2 set HMAC_MD5+DES_56_CB 326 0
3522 Tunnel0 10.0.0.2 set HMAC_MD5+DES_56_CB 0 311
3523 Tunnel0 10.0.0.2 set HMAC_MD5+DES_56_CB 339 0
3524 Tunnel0 10.0.0.2 set HMAC_MD5+DES_56_CB 0 25
3525 Tunnel0 10.0.0.2 set HMAC_MD5+DES_56_CB 22 0
```

## Информация о маршрутизаторе луча 1

```
Spoke1#show ip route
 172.16.0.0/24 is subnetted, 1 subnets
C    172.16.1.0 is directly connected, Ethernet0
 10.0.0.0/24 is subnetted, 1 subnets
C    10.0.0.0 is directly connected, Tunnel0
O IA 192.168.0.0/24 [110/11] via 10.0.0.1, 00:39:31, Tunnel0
     [110/11] via 10.0.0.2, 00:39:31, Tunnel0
C    192.168.1.0/24 is directly connected, Ethernet1
O    192.168.2.0/24 [110/2] via 10.0.0.12, 00:37:58, Tunnel0
Spoke1#show ip nhrp
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 00:56:40, never expire
  Type: static, Flags: authoritative used
  NBMA address: 172.17.0.1
10.0.0.2/32 via 10.0.0.2, Tunnel0 created 00:56:40, never expire
  Type: static, Flags: authoritative used
  NBMA address: 172.17.0.5
Spoke1#show crypto engine connection active
ID Interface IP-Address State Algorithm Encrypt Decrypt
 1 Ethernet0 172.16.1.24 set HMAC_SHA+DES_56_CB 0 0
 2 Ethernet0 172.16.1.24 set HMAC_SHA+DES_56_CB 0 0
2010 Tunnel0 10.0.0.11 set HMAC_MD5+DES_56_CB 0 171
2011 Tunnel0 10.0.0.11 set HMAC_MD5+DES_56_CB 185 0
2012 Tunnel0 10.0.0.11 set HMAC_MD5+DES_56_CB 0 12
2013 Tunnel0 10.0.0.11 set HMAC_MD5+DES_56_CB 13 0
```

## Информация о маршрутизаторе луча 2

```
Spoke2#show ip route
 172.16.0.0/24 is subnetted, 1 subnets
C    172.16.2.0 is directly connected, Ethernet0
 10.0.0.0/24 is subnetted, 1 subnets
C    10.0.0.0 is directly connected, Tunnel0
O IA 192.168.0.0/24 [110/11] via 10.0.0.1, 00:57:56, Tunnel0
      [110/11] via 10.0.0.2, 00:57:56, Tunnel0
O    192.168.1.0/24 [110/2] via 10.0.0.11, 00:56:14, Tunnel0
C    192.168.2.0/24 is directly connected, Ethernet1

Spoke2#show ip nhrp
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 5w6d, never expire
  Type: static, Flags: authoritative used
  NBMA address: 172.17.0.1
10.0.0.2/32 via 10.0.0.2, Tunnel0 created 6w6d, never expire
  Type: static, Flags: authoritative used
  NBMA address: 172.17.0.5

Spoke2#show crypto engine connection active
ID  Interface  IP-Address  State Algorithm          Encrypt Decrypt
  2  Ethernet0  172.16.2.75  set  HMAC_SHA+DES_56_CB    0       0
  3  Ethernet0  172.16.2.75  set  HMAC_SHA+DES_56_CB    0       0
3712 Tunnel0    10.0.0.12   set  HMAC_MD5+DES_56_CB    0       302
3713 Tunnel0    10.0.0.12   set  HMAC_MD5+DES_56_CB   331     0
3716 Tunnel0    10.0.0.12   set  HMAC_MD5+DES_56_CB    0       216
3717 Tunnel0    10.0.0.12   set  HMAC_MD5+DES_56_CB   236     0
```

Существует несколько интересных пунктов по таблицам маршрутизации на концентраторах 1 и 2 и лучах 1 и 2:

- У обоих маршрутизаторов концентраторов стоимости маршрутов к сетям после лучевых маршрутизаторов равны.

Концентратор1:

```
O    192.168.1.0/24 [110/2] via 10.0.0.11, 00:02:17, Tunnel0
O    192.168.2.0/24 [110/2] via 10.0.0.12, 00:02:17, Tunnel0
```

Концентратор2:

```
O    192.168.1.0/24 [110/2] via 10.0.0.11, 00:29:15, Tunnel0
O    192.168.2.0/24 [110/2] via 10.0.0.12, 00:29:15, Tunnel0
```

Это означает, что концентраторы 1 и 2 будут объявлять одну и ту же стоимость для сетей с лучевыми маршрутизаторами тем маршрутизаторам, которые входят в сеть с концентраторами. Например, таблица маршрутизации на маршрутизаторе R2, который связан непосредственно с локальной сетью 192.168.0.0/24, выглядит следующим образом:

R2:

```
O    IA 192.168.1.0/24 [110/12] via 192.168.0.1, 00:00:26, Ethernet1/0/3
      [110/12] via 192.168.0.2, 00:00:27, Ethernet1/0/30
O    IA 192.168.2.0/24 [110/12] via 192.168.0.1, 00:00:27, Ethernet1/0/3
      [110/12] via 192.168.0.2, 00:00:27, Ethernet1/0/3
```

- Лучевые маршрутизаторы имеют равные стоимости маршрутов через оба маршрутизатора концентратора к сетям после маршрутизаторов концентраторов.

Луч 1:

```
O    IA 192.168.0.0/24 [110/11] via 10.0.0.1, 00:39:31, Tunnel0
      [110/11] via 10.0.0.2, 00:39:31, Tunnel0
```

Луч 2:

```
O IA 192.168.0.0/24 [110/11] via 10.0.0.1, 00:57:56, Tunnel0
   [110/11] via 10.0.0.2, 00:57:56, Tunnel0
```

Выполнение лучевыми маршрутизаторами по пакетной балансировки нагрузки может привести к появлению поврежденных пакетов.

Чтобы избежать асимметричной маршрутизации или по пакетной балансировки нагрузки через связи к двум концентраторам, нужно так настроить протокол маршрутизации, чтобы был предпочтительным один путь к от луча к концентратору в обоих направлениях. Если необходимо настроить концентратор 1 в качестве основного и концентратор 2 в качестве резервного, необходимо установить различные значения стоимости OSPF для туннельных интерфейсов концентраторов.

Концентратор1:

```
interface tunnel0
...
ip ospf cost 10
...
```

Концентратор2:

```
interface tunnel0
...
ip ospf cost 20
...
```

Теперь маршруты выглядят следующим образом:

Концентратор1:

```
O 192.168.1.0/24 [110/11] via 10.0.0.11, 00:00:28, Tunnel0
O 192.168.2.0/24 [110/11] via 10.0.0.12, 00:00:28, Tunnel0
```

Концентратор2:

```
O 192.168.1.0/24 [110/21] via 10.0.0.11, 00:00:52, Tunnel0
O 192.168.2.0/24 [110/21] via 10.0.0.12, 00:00:52, Tunnel0
```

R2:

```
O IA 192.168.1.0/24 [110/31] via 192.168.0.1, 00:01:06, Ethernet1/0/3
O IA 192.168.2.0/24 [110/31] via 192.168.0.1, 00:01:06, Ethernet1/0/3
```

Два маршрутизатора концентратора имеют различные стоимости на маршрутах для сетей за лучевыми маршрутизаторами. Это означает, что концентратор 1 будет более предпочтительным для передачи трафика на лучевые маршрутизаторы, что видно на маршрутизаторе R2. Это решит описанную выше проблему асимметричной маршрутизации.

Здесь по-прежнему используется асимметричная маршрутизация в другом направлении, как описано во втором пункте выше. При использовании OSPF в качестве динамического протокола маршрутизации, эту проблему можно решить обходным путем, воспользовавшись командой **distance ...** под **router ospf 1** на лучах для оказания предпочтения маршрутам, полученным через концентратор 1, а не маршрутам, полученным через концентратор 2.

Луч 1:

```
router ospf 1
distance 111 10.0.0.2 0.0.0.0 1
access-list 1 permit any
```

Луч 2:

```
router ospf 1
distance 111 10.0.0.2 0.0.0.0 1
access-list 1 permit any
```

Теперь маршруты выглядят следующим образом:

Луч 1:

```
O       192.168.0.0/24 [110/11] via 10.0.0.1, 00:00:06, Tunnel0
```

Луч 2:

```
O       192.168.1.0/24 [110/11] via 10.0.0.1, 00:00:10, Tunnel0
```

Вышеописанная настройка маршрутизатора обеспечивает защиту от асимметричной маршрутизации, при этом разрешая переключение на концентратор 2 при отказе концентратора 1. Это означает, что при двух работающих концентраторах используется только концентратор 1. Если вы хотите использовать оба концентратора путем балансировки лучевых устройств по концентраторам, с функцией обхода отказа и без асимметричной маршрутизации, то настройка маршрутизации может усложниться, особенно при использовании OSPF. Поэтому рекомендуется предпочесть следующий двойной концентратор с двойной DMVPN.

## Системы с двумя концентраторами – топология двойной динамической многоточечной виртуальной частной сети (DMVPN)

Систему с двумя коммутаторами с топологией двойной динамической многоточечной виртуальной частной сети (DMVPN) несколько сложнее настроить, но она дает больший контроль над маршрутизацией через DMVPN. Основная идея заключается в том, чтобы иметь два отдельных "облака" DMVPN. Каждый концентратор (в данном случае два) будет подключен к одной подсети DMVPN ("облаку"), а маршрутизаторы на конце луча будут подключены к обеим подсетям DMVPN ("облакам"). Поскольку лучевые маршрутизаторы маршрутизируют соседей с маршрутизаторами концентраторов через два туннельных интерфейса GRE, можно использовать различия настройки интерфейсов (такие как полоса пропускания, стоимость и задержка), изменяя метрики протокола динамической маршрутизации, чтобы предпочесть один концентратор другому, когда они работают оба.

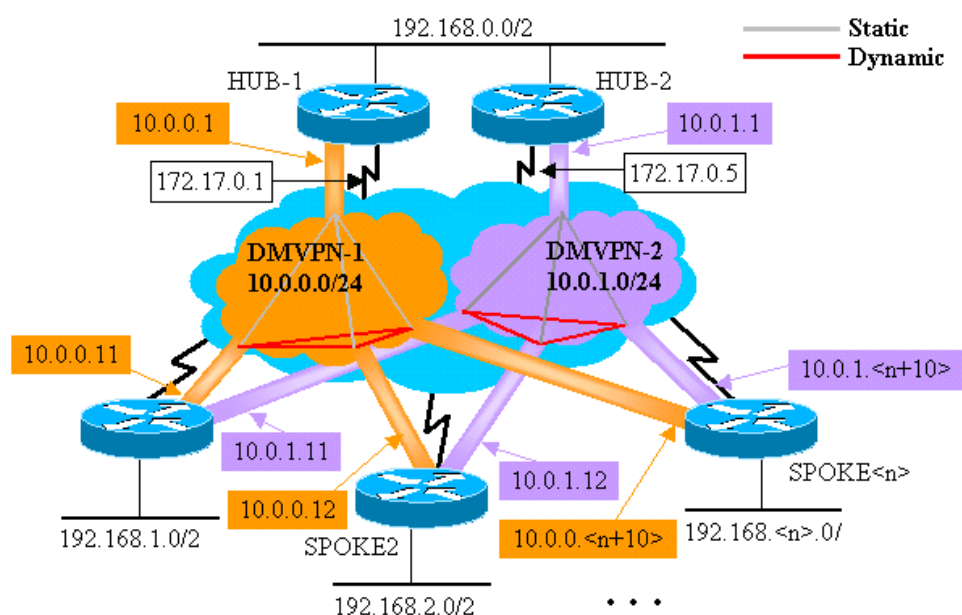
**Примечание.** Вышеуказанная проблема возникает только если маршрутизаторы концентраторов размещены рядом друг с другом. В противном случае при стандартной динамической маршрутизации будет выбран правильный маршрутизатор концентратора, даже если доступ к сети назначения возможен и через другой маршрутизатор концентратора.

На лучевых маршрутизаторах можно использовать туннельные интерфейсы - либо r-pGRE, либо mGRE. Многоточечный интерфейс r-pGRE на лучевом маршрутизаторе может использовать тот же IP-адрес **источника туннеля ...**, но многоточечные интерфейсы mGRE на лучевом маршрутизаторе должны иметь уникальный IP-адрес **источника туннеля ...**. Это связано с тем, что при инициации IPsec

первым передается пакет ISAKMP, который должен быть связан с одним из туннелей mGRE. Пакет ISAKMP имеет только IP-адрес назначения (адрес удаленного однорангового узла IPsec), с которым следует выполнять это сопоставление. Этот адрес сравнивается с адресом **источника туннеля ...**, однако поскольку у обоих туннелей один и тот же адрес **источника туннеля ...**, the first интерфейс первого туннеля mGRE всегда будет ему соответствовать. Это значит, что входящие многоадресные пакеты данных могут быть связаны с неправильным mGRE интерфейсом, разрушая любой протокол динамической маршрутизации.

Сами пакеты GRE лишены этой проблемы, так как используют значение **туннельного ключа ...**, чтобы различать два интерфейса mGRE. Начиная с Cisco IOS выпуск 12.3(5) и 12.3(7)T, в ПО был добавлен новый параметр для преодоления этого ограничения. **защита туннеля...общая**. Слово **общая** означает, что множественные интерфейсы mGRE будут использовать шифрование IPsec с тем же IP-адресом источника. При использовании более ранних версий ПО можно использовать туннели r-pGRE в системе с двумя концентраторами с двойной DMVPN. В случае туннеля r-pGRE IP-адреса **источника туннеля ...** и **назначения туннеля ...** могут использоваться для сравнения. В этом примере туннели r-pGRE будут использоваться с двумя концентраторами и с двойной DMVPN; классификатор **shared** не используется.

### Системы с двумя концентраторами – топология двойной динамической многоточечной виртуальной частной сети (DMVPN)



Следующие выделенные изменения связаны с настройками динамического многоточечного концентратора и лучевого устройства, ранее показанными в этом документе.

#### Маршрутизатор концентратора 1

```

version 12.3
!
hostname Hub1
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp holdtime 600

```

```

no ip split-horizon eigrp 1
delay 1000
tunnel source Ethernet0
tunnel mode gre multipoint
tunnel key 100000
tunnel protection ipsec profile vpnprof
!
interface Ethernet0
ip address 172.17.0.1 255.255.255.252
!
interface Ethernet1
ip address 192.168.0.1 255.255.255.0
!
router eigrp 1
network 10.0.0.0 0.0.0.255
network 192.168.0.0 0.0.0.255
no auto-summary
!

```

## ● Маршрутизатор концентратора 2 ●

```

version 12.3
!
hostname Hub2
!
crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
mode transport
!
crypto ipsec profile vpnprof
set transform-set trans2
!
interface Tunnel0
bandwidth 1000
ip address 10.0.1.1 255.255.255.0
ip mtu 1400
ip nhrp authentication test
ip nhrp map multicast dynamic
ip nhrp network-id 100001
ip nhrp holdtime 600
no ip split-horizon eigrp 1
delay 1000
tunnel source Ethernet0
tunnel mode gre multipoint
tunnel key 100001
tunnel protection ipsec profile vpnprof
!
interface Ethernet0
ip address 172.17.0.5 255.255.255.252
!
interface Ethernet1
ip address 192.168.0.2 255.255.255.0
!
router eigrp 1
network 10.0.1.0 0.0.0.255
network 192.168.0.0 0.0.0.255
no auto-summary
!

```

В этом случае настройки концентраторов 1 и 2 похожи. Главное отличие состоит в том, что они являются концентраторами разных DMVPN. Каждая DMVPN использует различные:

- подсеть IP(10.0.0.0/24, 10.0.0.1/24)
- id сети NHRP (100000, 100001)
- ключ туннеля (100000, 100001)

Протокол динамической маршрутизации был переключен с OSPF на EIGRP, поскольку настройка и управление сети NBMA с помощью EIGRP упрощаются, как описано в этом документе в дальнейшем.

### Маршрутизатор луча 1

```
version 12.3
!
hostname Spoke1
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.11 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.1
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Tunnel1
 bandwidth 1000
 ip address 10.0.1.11 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.1.1 172.17.0.5
 ip nhrp network-id 100001
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.1.1
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.5
 tunnel key 100001
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke1
!
interface Ethernet1
 ip address 192.168.1.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 10.0.1.0 0.0.0.255
 network 192.168.1.0 0.0.0.255
 no auto-summary
!
```

Каждый из лучевых маршрутизаторов настроен с двумя туннельными интерфейсами p-pGRE, по одному в каждой из двух DMVPN. Значения **ip адрес ...**, **ip nhrp network-id ...**, **tunnel key ...** и **tunnel destination ...** используются для обозначения различий между двумя туннелями. Протокол динамической маршрутизации, EIGRP, выполняется на обоих подсетях туннеля p-pGRE и используется для выбора одного интерфейса p-pGRE (DMVPN) посредством другого.

### Маршрутизатор луча 2



```

version 12.3
!
hostname Spoke2
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.12 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.1
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Tunnell
 bandwidth 1000
 ip address 10.0.1.12 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.1.1 172.17.0.5
 ip nhrp network-id 100001
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.1.1
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.5
 tunnel key 100001
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke2
!
interface Ethernet1
 ip address 192.168.2.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 10.0.1.0 0.0.0.255
 network 192.168.2.0 0.0.0.255
 no auto-summary
!

```

## ● Маршрутизатор луча<n> ●

```

version 12.3
!
hostname Spoke<n>
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.<n+10> 255.255.255.0
 ip mtu 1400

```

```

ip nhrp authentication test
ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp network-id 100000
ip nhrp holdtime 300
ip nhrp nhs 10.0.0.1
delay 1000
tunnel source Ethernet0
tunnel destination 172.17.0.1
tunnel key 100000
tunnel protection ipsec profile vpnprof
!
interface Tunnell
bandwidth 1000
ip address 10.0.1.<n+10> 255.255.255.0
ip mtu 1400
ip nhrp authentication test
ip nhrp map 10.0.1.1 172.17.0.5
ip nhrp network-id 100001
ip nhrp holdtime 300
ip nhrp nhs 10.0.1.1
delay 1000
tunnel source Ethernet0
tunnel destination 172.17.0.5
tunnel key 100001
tunnel protection ipsec profile vpnprof
!
interface Ethernet0
ip address dhcp hostname Spoke<x>
!
interface Ethernet1
ip address 192.168.<n>.1 255.255.255.0
!
router eigrp 1
network 10.0.0.0 0.0.0.255
network 10.0.1.0 0.0.0.255
network 192.168.<n>.0 0.0.0.255
no auto-summary
!

```

На этом этапе обратите внимание на таблицы маршрутизации, таблицы соответствий NHRP и соединения IPsec на маршрутизаторах концентратора 1 и 2, луча1 и 2 для получения начальных условий (сразу после включения луча 1 и 2).

## Начальные условия и изменения

### ● Информация о маршрутизаторе концентратора 1 ●

```

Hub1#show ip route
172.17.0.0/30 is subnetted, 1 subnets
C    172.17.0.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 2 subnets
C    10.0.0.0 is directly connected, Tunnel0
D    10.0.1.0 [90/2611200] via 192.168.0.2, 00:00:46, Ethernet1
C    192.168.0.0/24 is directly connected, Ethernet1
D    192.168.1.0/24 [90/2841600] via 10.0.0.11, 00:00:59, Tunnel0
D    192.168.2.0/24 [90/2841600] via 10.0.0.12, 00:00:34, Tunnel0
Hub1#show ip nhrp
10.0.0.12/32 via 10.0.0.12, Tunnel0 created 23:48:32, expire 00:03:50
Type: dynamic, Flags: authoritative unique registered
NBMA address: 172.16.2.75
10.0.0.11/32 via 10.0.0.11, Tunnel0 created 23:16:46, expire 00:04:45
Type: dynamic, Flags: authoritative unique registered
NBMA address: 172.16.1.24
Hub1#show crypto engine connection active
ID Interface IP-Address State Algorithm Encrypt Decrypt
15 Ethernet0 172.17.63.18 set HMAC_SHA+DES_56_CB 0 0
16 Ethernet0 10.0.0.1 set HMAC_SHA+DES_56_CB 0 0
2038 Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB 0 759
2039 Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB 726 0
2040 Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB 0 37
2041 Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB 36 0

```

## Информация о маршрутизаторе концентратора 2

```
Hub2#show ip route
172.17.0.0/30 is subnetted, 1 subnets
C    172.17.0.4 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 2 subnets
D    10.0.0.0 [90/2611200] via 192.168.0.1, 00:12:22, Ethernet1
C    10.0.1.0 is directly connected, Tunnel0
C    192.168.0.0/24 is directly connected, Ethernet1
D    192.168.1.0/24 [90/2841600] via 10.0.1.11, 00:13:24, Tunnel0
D    192.168.2.0/24 [90/2841600] via 10.0.1.12, 00:12:11, Tunnel0
Hub2#show ip nhrp
10.0.1.12/32 via 10.0.1.12, Tunnel3 created 06:03:24, expire 00:04:39
Type: dynamic, Flags: authoritative unique registered
NBMA address: 172.16.2.75
10.0.1.11/32 via 10.0.1.11, Tunnel3 created 23:06:47, expire 00:04:54
Type: dynamic, Flags: authoritative unique registered
NBMA address: 172.16.1.24
Hub2#show crypto engine connection active
ID Interface IP-Address State Algorithm Encrypt Decrypt
  4 Ethernet0 171.17.0.5 set HMAC_SHA+DES_56_CB 0 0
  6 Ethernet0 171.17.0.5 set HMAC_SHA+DES_56_CB 0 0
2098 Tunnel0 10.0.1.1 set HMAC_MD5+DES_56_CB 0 722
2099 Tunnel0 10.0.1.1 set HMAC_MD5+DES_56_CB 690 0
2100 Tunnel0 10.0.1.1 set HMAC_MD5+DES_56_CB 0 268
2101 Tunnel0 10.0.1.1 set HMAC_MD5+DES_56_CB 254 0
```

## Информация о маршрутизаторе луча 1

```
Spoke1#show ip route
172.16.0.0/24 is subnetted, 1 subnets
C    172.16.1.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 1 subnets
C    10.0.0.0 is directly connected, Tunnel0
C    10.0.1.0 is directly connected, Tunnel1
D    192.168.0.0/24 [90/2841600] via 10.0.1.1, 00:26:30, Tunnel1
[90/2841600] via 10.0.0.1, 00:26:30, Tunnel0
C    192.168.1.0/24 is directly connected, Ethernet1
D    192.168.2.0/24 [90/3097600] via 10.0.1.1, 00:26:29, Tunnel1
[90/3097600] via 10.0.0.1, 00:26:29, Tunnel0
Spoke1#show ip nhrp
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 23:25:46, never expire
Type: static, Flags: authoritative
NBMA address: 172.17.0.1
10.0.1.1/32 via 10.0.1.1, Tunnel1 created 23:24:40, never expire
Type: static, Flags: authoritative
NBMA address: 172.17.0.5
Spoke1#show crypto engine connection active
ID Interface IP-Address State Algorithm Encrypt Decrypt
 16 Ethernet0 172.16.1.24 set HMAC_SHA+DES_56_CB 0 0
 18 Ethernet0 172.16.1.24 set HMAC_SHA+DES_56_CB 0 0
2118 Tunnel0 10.0.0.11 set HMAC_MD5+DES_56_CB 0 181
2119 Tunnel0 10.0.0.11 set HMAC_MD5+DES_56_CB 186 0
2120 Tunnel1 10.0.1.11 set HMAC_MD5+DES_56_CB 0 105
2121 Tunnel1 10.0.1.11 set HMAC_MD5+DES_56_CB 110 0
```

## Информация о маршрутизаторе луча 2

```
Spoke2#show ip route
172.16.0.0/24 is subnetted, 1 subnets
C    172.16.2.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 2 subnets
C    10.0.0.0 is directly connected, Tunnel0
C    10.0.1.0 is directly connected, Tunnel1
D    192.168.0.0/24 [90/2841600] via 10.0.1.1, 00:38:04, Tunnel1
[90/2841600] via 10.0.0.1, 00:38:04, Tunnel0
D    192.168.1.0/24 [90/3097600] via 10.0.1.1, 00:38:02, Tunnel1
[90/3097600] via 10.0.0.1, 00:38:02, Tunnel0
```

```

C 192.168.2.0/24 is directly connected, Ethernet1
Spoke2#show ip nhrp
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 1d02h, never expire
  Type: static, Flags: authoritative used
  NBMA address: 172.17.0.1
10.0.1.1/32 via 10.0.1.1, Tunnel1 created 1d02h, never expire
  Type: static, Flags: authoritative used
  NBMA address: 172.17.0.5
Spoke2#show crypto engine connection active
  ID Interface  IP-Address  State  Algorithm  Encrypt  Decrypt
   8 Ethernet0  172.16.2.75  set    HMAC_SHA+DES_56_CB  0         0
   9 Ethernet0  172.16.2.75  set    HMAC_SHA+DES_56_CB  0         0
2036 Tunnel0    10.0.0.12    set    HMAC_MD5+DES_56_CB  0         585
2037 Tunnel0    10.0.0.12    set    HMAC_MD5+DES_56_CB  614       0
2038 Tunnel1    10.0.1.12    set    HMAC_MD5+DES_56_CB  0         408
2039 Tunnel1    10.0.1.12    set    HMAC_MD5+DES_56_CB  424       0

```

Следует отметить несколько особенностей, касающихся таблиц маршрутизации на концентраторах 1 и 2 и лучах 1и 2:

- У обоих маршрутизаторов концентраторов стоимости маршрутов к сетям после лучевых маршрутизаторов равны.

Концентратор1:

```

D 192.168.1.0/24 [90/2841600] via 10.0.0.11, 00:00:59, Tunnel0
D 192.168.2.0/24 [90/2841600] via 10.0.0.12, 00:00:34, Tunnel0

```

Концентратор2:

```

D 192.168.1.0/24 [90/2841600] via 10.0.1.11, 00:13:24, Tunnel0
D 192.168.2.0/24 [90/2841600] via 10.0.1.12, 00:12:11, Tunnel0

```

Это означает, что концентраторы 1 и 2 будут объявлять одну и ту же стоимость для сетей с лучевыми маршрутизаторами тем маршрутизаторам, которые входят в сеть с концентраторами. Например, таблица маршрутизации на маршрутизаторе R2, который связан непосредственно с локальной сетью 192.168.0.0/24, выглядит следующим образом:

R2:

```

D 192.168.1.0/24 [90/2867200] via 192.168.0.1, 00:51:51, Ethernet1/0/3
                        [90/2867200] via 192.168.0.2, 00:51:51, Ethernet1/0/3
D 192.168.2.0/24 [90/2867200] via 192.168.0.2, 00:52:43, Ethernet1/0/3
                        [90/2867200] via 192.168.0.1, 00:52:43, Ethernet1/0/3

```

- Лучевые маршрутизаторы имеют равные стоимости маршрутов через оба маршрутизатора концентратора к сетям после маршрутизаторов концентраторов.

Луч 1:

```

D 192.168.0.0/24 [90/3097600] via 10.0.1.1, 00:26:30, Tunnel1
                        [90/3097600] via 10.0.0.1, 00:26:30, Tunnel0

```

Луч 2:

```

D 192.168.0.0/24 [90/3097600] via 10.0.1.1, 00:38:04, Tunnel1
                        [90/3097600] via 10.0.0.1, 00:38:04, Tunnel0

```

Выполнение оконечными маршрутизаторами по пакетной балансировки нагрузки может привести к появлению поврежденных пакетов.

Чтобы избежать асимметричной маршрутизации или по пакетной балансировки нагрузки через связи к двум концентраторам, нужно так настроить протокол маршрутизации, чтобы был предпочтительным один путь к от луча к концентратору в обоих направлениях. Если необходимо настроить концентратор 1 в качестве основного и концентратор 2 в качестве резервного, необходимо установить различные значения задержки для туннельных интерфейсов концентраторов.

Концентратор1:

```
interface tunnel0
...
delay 1000
...
```

Концентратор2:

```
interface tunnel0
...
delay 1050
...
```

**Примечание.** В этом примере к задержке на интерфейсе туннеля на Hub2 было добавлено 50, потому что она меньше задержки на интерфейсе Ethernet1 (100) между этими двумя концентраторами. Сделав это, концентратор 2 еще будет напрямую пересылать пакеты лучевым маршрутизаторам, но он будет менее желательным, нежели маршрут от концентратора 1 к маршрутизаторам за концентраторами 1 и 2. Если задержка увеличится более, чем на 100, то концентратор 2 будет передавать пакеты для лучевых маршрутизаторов с помощью концентратора 1 через интерфейс Ethernet1, хотя маршрутизаторы за концентраторами 1 и 2 будут по-прежнему предпочитать концентратор 1 для передачи пакетов.

Теперь маршруты выглядят следующим образом:

Концентратор1:

```
D    192.168.1.0/24 [90/2841600] via 10.0.0.11, 00:01:11, Tunnel0
D    192.168.2.0/24 [90/2841600] via 10.0.0.12, 00:01:11, Tunnel0
```

Концентратор2:

```
D    192.168.1.0/24 [90/2854400] via 10.0.1.11, 00:00:04, Tunnel0
D    192.168.2.0/24 [90/2854400] via 10.0.1.12, 00:00:04, Tunnel0
```

R2:

```
D    192.168.1.0/24 [90/2867200] via 192.168.0.1, 00:02:18, Ethernet1/0/3
D    192.168.2.0/24 [90/2867200] via 192.168.0.1, 00:02:18, Ethernet1/0/3
```

Два маршрутизатора концентратора имеют разный приоритет при сетевой маршрутизации к лучевым маршрутизаторам, в этом случае, концентратор 1 будет более предпочтителен для пересылки трафика лучевым маршрутизаторам, как можно увидеть на R2. Это решает проблему, описанную выше в первом пункте.

Проблема, описанная выше во втором пункте, все еще сохраняется, но так как у вас два туннельных интерфейса p-rGRE, вы можете настроить для них различные значения **задержки...**, чтобы изменить метрику EIGRP для маршрутов, сведения о которых поступают от концентратора 1 и 2.

Луч 1:

```
interface tunnel0
  delay 1000
interface tunnel1
  delay 1050
```

Луч 2:

```
interface tunnel0
  delay 1000
interface tunnel1
  delay 1050
```

Теперь маршруты выглядят следующим образом:

Луч 1:

```
D 192.168.0.0/24 [90/2841600] via 10.0.0.1, 00:15:44, Tunnel0
D 192.168.2.0/24 [90/3097600] via 10.0.0.1, 00:15:44, Tunnel0
```

Луч 2:

```
D 192.168.0.0/24 [90/2841600] via 10.0.0.1, 00:13:54, Tunnel0
D 192.168.1.0/24 [90/3097600] via 10.0.0.1, 00:13:54, Tunnel0
```

Вышеописанная настройка маршрутизатора обеспечивает защиту от асимметричной маршрутизации, при этом разрешая переключение на концентратор 2 при отказе концентратора 1. Это означает, что при двух работающих концентраторах используется только концентратор 1.

Если вы хотите использовать оба концентратора путем балансировки лучевых устройств по концентраторам, с функцией обхода отказа и без асимметричной маршрутизации, то настройка маршрутизации может усложниться; но вы можете это сделать при использовании EIGRP. Для этого установите равное значение **задержки...** на туннельных интерфейсах маршрутизаторов концентраторов, а затем выполните команду **offset-list <acl> out <offset> <interface>** на лучевых маршрутизаторах для увеличения метрики EIGRP маршрутов, объявленных туннельными интерфейсами GRE для дополнительного концентратора. Неравная **задержка...** для интерфейсов Tunnel0 и Tunnel1 луча сохраняется, поэтому маршрутизатор луча выберет основной концентратор. На лучевых маршрутизаторах требуются следующие изменения.

### Маршрутизатор луча 1

```
version 12.3
!
hostname Spoke1
!
...
!
interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.11 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
```

```
delay 1000
tunnel source Ethernet0
tunnel destination 172.17.0.1
tunnel key 100000
tunnel protection ipsec profile vpnprof
!
interface Tunnell
bandwidth 1000
ip address 10.0.1.11 255.255.255.0
ip mtu 1400
ip nhrp authentication test
ip nhrp map 10.0.1.1 172.17.0.5
ip nhrp network-id 100001
ip nhrp holdtime 300
ip nhrp nhs 10.0.1.1
delay 1500
tunnel source Ethernet0
tunnel destination 172.17.0.5
tunnel key 100001
tunnel protection ipsec profile vpnprof
!
...
!
router eigrp 1
offset-list 1 out 12800 Tunnell
network 10.0.0.0 0.0.0.255
network 10.0.1.0 0.0.0.255
network 192.168.1.0
distribute-list 1 out
no auto-summary
!
access-list 1 permit 192.168.1.0
!
```

## ● Маршрутизатор луча 2 ●

```
version 12.3
!
hostname Spoke2
!
...
!
interface Tunnel0
bandwidth 1000
ip address 10.0.0.12 255.255.255.0
ip mtu 1400
ip nhrp authentication test
ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp network-id 100000
ip nhrp holdtime 300
ip nhrp nhs 10.0.0.1
delay 1500
tunnel source Ethernet0
tunnel destination 172.17.0.1
tunnel key 100000
tunnel protection ipsec profile vpnprof
!
interface Tunnell
bandwidth 1000
ip address 10.0.1.12 255.255.255.0
ip mtu 1400
ip nhrp authentication test
ip nhrp map 10.0.1.1 172.17.0.5
ip nhrp network-id 100001
ip nhrp holdtime 300
ip nhrp nhs 10.0.1.1
delay 1000
tunnel source Ethernet0
tunnel destination 172.17.0.5
tunnel key 100001
tunnel protection ipsec profile vpnprof
!
...
!
router eigrp 1
offset-list 1 out 12800 Tunnell
network 10.0.0.0 0.0.0.255
```

```
network 10.0.1.0 0.0.0.255
network 192.168.2.0
distribute-list 1 out
no auto-summary
!
access-list 1 permit 192.168.2.0
!
```

**Примечание.** Величина смещения 12800 (50\*256) была добавлена к метрике EIGRP, т.к. она меньше 25600 (100\*256). Это значение (25600) – то, что добавляется к метрике EIGRP для маршрутов, полученных между маршрутизаторами концентратора. Используя значение 12800 в команде **offset-list**, дополнительный маршрутизатор концентратора будет напрямую направлять пакеты лучевым маршрутизаторам посредством Ethernet через главный для этих лучей маршрутизатор концентратора. Метрика на маршрутах, объявляемых маршрутизаторами концентраторов, такова, что предпочтение отдается основному маршрутизатору. Помните, что у половины периферийных устройств основным маршрутизатором является концентратор 1, а у другой половины основным маршрутизатором является концентратор 2.

**Примечание.** Если значение смещения превысило 25600 (100\*256), концентраторы направят пакеты половине маршрутизаторов на конце луча через другой концентратор через интерфейс Ethernet1, даже если маршрутизаторы после концентраторов по-прежнему предпочитают, чтобы пакеты отправлял правильный концентратор.

**Примечание.** Команда **distribute-list 1 out** также была добавлена, так как существует вероятность того, что маршруты, полученные от одного центрального концентратора через туннельный интерфейс на луче, могли быть объявлены в обратную сторону для другого концентратора через другой туннель. Команда **distribute-list ...** гарантирует, что лучевой маршрутизатор может объявлять лишь собственные маршруты.

**Примечание.** Если вы предпочитаете управлять объявлением маршрутов на концентраторах, а не на лучах, тогда команды **offset-list <acl1> in <value> <interface>** и **distribute-list <acl2> in** можно настроить не на лучевых, а на центральных маршрутизаторах. Список доступа <acl2> предоставит список маршрутов за всеми лучами, а список доступа <acl1> предоставит только те маршруты за лучами, у которых главным является другой маршрутизатор концентратора.

Теперь маршруты выглядят следующим образом:

Концентратор1:

```
D    192.168.1.0/24 [90/2841600] via 10.0.0.11, 00:12:11, Tunnel2
D    192.168.2.0/24 [90/2854400] via 10.0.0.12, 00:13:24, Tunnel2
```

Концентратор2:

```
D    192.168.1.0/24 [90/2854400] via 10.0.1.11, 00:09:58, Tunnel0
D    192.168.2.0/24 [90/2841600] via 10.10.1.12, 00:11:11, Tunnel0
```

R2:

```
D    192.168.1.0/24 [90/2867200] via 192.168.0.1, 00:13:13, Ethernet1/0/3
D    192.168.2.0/24 [90/2867200] via 192.168.0.2, 00:14:25, Ethernet1/0/3
```

Луч 1:

```
D    192.168.0.0/24 [90/2841600] via 10.0.0.1, 00:16:12, Tunnel0
```



## Заключение

Решение DMVPN обеспечивает следующую функциональность для лучшего масштабирования больших и малых сетей IPsec VPN.

- DMVPN обеспечивает лучшее масштабирование в полно-связанных и частично-связанных сетях IPsec VPNs.

Оно особенно полезно при наличии нерегулярного трафика между лучами (например, каждый луч отправляет данные на другие лучи не постоянно). Оно позволяет каждому лучу напрямую посылать данные на любой другой луч при наличии прямого IP-соединения между лучами.

- DMVPN поддерживает узлы IPsec с динамически присвоенными номерами (такие как Cable, ISDN и DSL).

Это применимо к сетям как с топологией звезды, так и с ячеистой топологией. Для DMVPN может понадобиться постоянно установленная связь между лучами.

- DMVPN упрощает добавление узлов VPN.

Чтобы добавить новый лучевой маршрутизатор, необходимо настроить его и подключить к сети (хотя, может потребоваться добавить информацию авторизации ISAKMP для нового лучевого маршрутизатора на концентраторе). Концентратор динамически запомнит новый луч, протокол динамической маршрутизации распространит информацию о маршрутизации на концентратор и остальные лучи.

- DMVPN уменьшает размер настройки, необходимой для всех маршрутизаторов сети VPN.

Это также относится к сетям VPN GRE+IPsec с топологией "только звезда".

- DMVPN использует GRE и, таким образом, поддерживает IP-широковещание и динамическую маршрутизацию трафика через VPN.

Это означает, что протокол динамической маршрутизации можно использовать, а избыточные концентраторы могут поддерживаться протоколом. Многоадресные приложения также поддерживаются.

- DMVPN поддерживает раздельное туннелирование на лучах.

---

## Дополнительные сведения

- **Динамическая многоточечная сеть VPN (DMVPN)**
- **Страница поддержки IPSec**
- **Техническая поддержка – Cisco Systems**