

Построение туннелей на маршрутизаторах Cisco с использованием интерфейсов Loopback

Общее описание

Моделируется ситуация, когда провайдер маршрутизирует ограниченные диапазоны IP-адресов, например, организывает связь между двумя сетями /24. На основании этого для связи офисов строится туннель на loopback-интерфейсах двух граничных маршрутизаторов клиента, IP-адреса для интерфейсов Loopback выбираются из сетей, выделенных (маршрутизируемых) провайдером.

Для лучшего понимания задачи, поставленной в лабораторной работе, предлагается выполнить предварительную подготовку. А, именно, рассмотреть стандартную ситуацию маршрутизации офисов клиента через сеть провайдера (без конфигурирования туннеля). Пусть провайдер выделяет клиенту офисные сети /24. Необходимо настроить IP-адреса интерфейсов и прописать статическую маршрутизацию для роутеров Provider, Router1, Router2, согласно схеме сети, приведенной в работе, не принимая во внимание туннель и loopback-интерфейсы. Подчеркнем, что для адресации офисных сетей клиента используем маску /24.

Подготовительная настройка

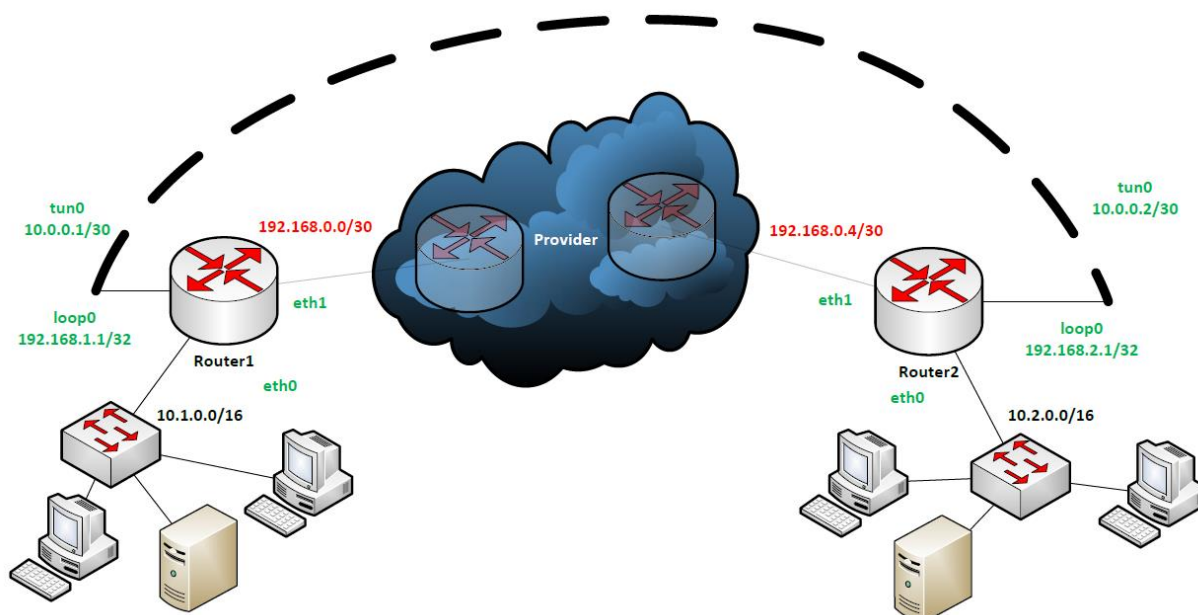
В роли сети провайдера используем маршрутизатор Cisco серии 3600, офисные сети подключены к маршрутизаторам Cisco серии 1600.

1. Подключите два маршрутизатора Cisco серии 1600 к маршрутизатору Cisco серии 3600. К каждому маршрутизатору Cisco серии 1600 также подключите компьютер.
2. Подключитесь к консольному порту каждого из маршрутизаторов и из конфигурационного режима задайте имя с помощью команды **hostname name**. Например, Provider, Router1, Router2.
3. Для каждого маршрутизатора в режиме конфигурации интерфейса настройте IP-адреса интерфейсов Ethernet0, Ethernet1 с помощью команды **ip address address mask**. Для адресов интерфейсов Ethernet0 маршрутизаторов Cisco 1600 (к которым подключены офисные сетки) используем маску /24 (mask 255.255.255.0).
4. Для каждого компьютера офисных клиентских сетей настройте IP-адрес, используя маску /24, в качестве default gateway укажите IP-адрес интерфейса Ethernet0 соответствующего маршрутизатора Cisco серии 1600.
5. На маршрутизаторе Cisco серии 3600 (Provider) настройте статическую маршрутизацию на выделенные сети, используя конфигурационную команду **ip route ip-address mask next_hop**.
6. На каждом маршрутизаторе Cisco 1600 также пропишите статическую маршрутизацию на удаленную офисную сеть через маршрутизатор провайдера.
7. Для отслеживания состояния таблицы маршрутизации используйте команду **show ip route**.

8. С помощью ICMP эхо-запросов (**ping**) убедитесь в доступности каждого из маршрутизаторов с компьютера(-ов) и в том, что между офисами клиента установлена связь через маршрутизатор провайдера.

Основная настройка

Теперь предположим, что ситуация изменилась. Клиенту необходимо использовать большее количество адресов, чем предоставляется выделенными провайдером сетями /24. Для этого при адресации офисных сетей используется маска /16. Но провайдер по-прежнему маршрутизирует и предоставляет клиенту сети /24. Решением проблемы связи офисов клиента может служить построение туннеля на loopback-интерфейсах двух граничных маршрутизаторов клиента.



9. С помощью команды **ip address address mask** для каждого маршрутизатора Cisco серии 1600 в режиме конфигурации интерфейса настройте новые IP-адреса интерфейсов Ethernet0, к которым подключены офисные сети клиента, необходимо использовать маску /16 (mask 255.255.0.0).
10. Для каждого компьютера офисных клиентских сетей настройте новый IP-адрес, используя маску /16.
11. Для каждого из маршрутизаторов Cisco 1600 в режиме конфигурирования виртуального интерфейса loopback0 настройте IP-адрес с помощью команды **ip address address mask**, в качестве mask следует использовать /32 (mask 255.255.255.255), IP-адрес выбирается из сети, выделенной провайдером.
12. Для каждого маршрутизатора Cisco 1600 сконфигурируйте туннельный интерфейс, с помощью конфигурационной команды **interface tunnel 0**.
13. В режиме конфигурирования интерфейса-туннеля настройте IP-адрес, используя команду **ip address address mask**, в качестве маски следует указать значение /30 (mask 255.255.255.252).
14. Используя интерфейсные команды **tunnel source ip-address** и **tunnel destination ip-address** настройте IP-адреса конечных точек туннеля. В качестве *ip-address* следует использовать настроенные ранее адреса loopback-интерфейсов.

15. Настройте режим туннелирования с помощью интерфейсной команды **tunnel mode mode**, где в качестве mode укажите, например, ipip.
16. Принимая во внимание сконфигурированный выше туннель, создайте на каждом маршрутизаторе Cisco серии 1600 статический маршрут на вторую офисную сеть, используя конфигурационную команду **ip route network ip-address mask next-hop**.
17. Убедитесь в доступности каждого из маршрутизаторов с компьютера(-ов) с помощью ICMP эхо-запросов (**ping**).
18. Посмотрите, как маршрутизируются офисные сети, используя команду **tracert ip-address (tracert для Windows)**.
19. Посмотрите IP-адреса отправителя и получателя пакетов, маршрутизируемых между офисными сетями клиента. Для этого подключите маршрутизатор Cisco серии 1600 и маршрутизатор Cisco серии 3600 (Provider) к коммутатору Cisco серии Catalyst 2960, к которому также подключите ещё один компьютер.
20. Настройте на коммутаторе SPAN-сессию для копирования данных, проходящих через коммутатор на порт, к которому подключен дополнительный компьютер. Для этого используйте конфигурационные команды **monitor session 1 source interface interface both, monitor session 1 destination interface interface**, где в качестве source interface и destination interface укажите порты, к которым подключены офисный маршрутизатор и дополнительный компьютер, соответственно.
21. Для просмотра настроенной SPAN-сессии воспользуйтесь командой **show monitor session 1**.
22. Запустите на дополнительном компьютере, подключенном к коммутатору, программу Wireshark, «перехватите» пакет, отправленный из одной офисной сети в другую. Посмотрите MAC и IP-адреса отправителя и получателя.
23. Осуществите такой «перехват» пакета в разных частях построенной сети (между офисным ПК первого офиса и Router1, между Router1 и Provider, между Provider и Router2, между Router2 и офисным ПК во втором офисе), используя коммутатор Cisco серии 2960. Установленные MAC и IP-адреса отправителя и получателя занесите в таблицу. Проанализируйте полученные данные.

Точка перехвата	IP и MAC отправителя	IP и MAC получателя	IP и MAC отправителя в перехваченных данных	IP и MAC получателя в перехваченных данных
ПК1-Router1				
Router1-Provider				
Provider-Router2				
Router2-ПК2				

Далее перейдем ко второй части лабораторной работы.

Запустите протокол динамической маршрутизации EIGRP, с помощью которого установите соседство между двумя офисными маршрутизаторами через туннельные интерфейсы. Передайте с помощью этого протокола маршрутную информацию обо всех подключенных сетях.

1. На каждом маршрутизаторе Cisco серии 1600 удалите прописанный ранее статический маршрут на соответствующую офисную сеть с маской /16. Это

- требуется сделать, так как далее предполагается передавать информацию об этой сети по EIGRP. Обратите внимание на состояние туннеля.
2. На каждом клиентском маршрутизаторе запустите протокол EIGRP. Для этого следует использовать конфигурационную команду **router eigrp process_number**, где в качестве номера процесса укажите, например, 1.
 3. С помощью команды **network network_ip-address** в режиме конфигурации роутера пропишите сетку, в которой будет работать EIGRP (протокол включится на всех интерфейсах данного маршрутизатора, адреса которых попадают в указанный диапазон).
 4. Отключите автоматическое суммирование маршрутов с помощью команды **no auto-summary** в режиме конфигурации маршрутизатора.
 5. Командой **redistribute connected** укажите маршрутизатору, что следует отправлять маршрутную информацию обо всех подключенных сетях.
 6. Для отслеживания изменений используйте команды **show ip route eigrp**, **show ip eigrp neighbors**, **show ip eigrp interfaces**, **show ip eigrp topology**.
 7. Обратите внимание на периодическое изменение состояния туннеля. Такой эффект - следствие рекурсивной маршрутизации. Изучите и объясните явление.

По согласованию с преподавателем исправьте возникшую проблему. Для ее решения следует изменить конфигурацию на клиентских маршрутизаторах так, чтобы по EIGRP отправлялась информация обо всех подключенных сетях, но не пересылалась информация о loopback-интерфейсе. Для этого будем использовать механизм route-map.

8. Создайте route-map на каждом маршрутизаторе Cisco серии 1600, используя конфигурационную команду **route-map rm-name deny seq1**, в качестве *seq1* укажите, например, 10. Постфикс deny указывает на создание запрещающего правила.
9. Пропишите само запрещение с помощью команды **match interface interface**, в качестве *interface* укажите loopback-интерфейс данного маршрутизатора. Вернитесь в режим глобальной конфигурации.
10. Для созданного route-map создайте разрешающее правило, используя команду **route-map rm-name permit seq2**, где, согласно логике работы route-map, в качестве *seq2* следует указать значение, большее *seq1*, например, 20. По умолчанию разрешающее правило разрешает всё, не указанное в предварительном запрещающем правиле.
11. Укажите, что по EIGRP следует отправлять маршрутную информацию обо всех подключенных сетях, с применением правил, указанных в созданном route-map. Для этого отмените команду **redistribute connected** в режиме конфигурации роутера для eigrp 1, и примените **redistribute connected route-map rm-name**.
12. Обратите внимание на состояние туннеля. Проанализируйте изменения.
13. Предложите и реализуйте другие способы решения проблемы.

Примечание. Познакомьтесь с *distribute-lists* и *prefix-lists* применительно к данной лабораторной работе.