

Почему нельзя просматривать интернет при использовании туннеля GRE?

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Фрагментация пакетов и сообщений ICMP](#)

[Заблокированные сообщения ICMP](#)

[Решения](#)

[Дальнейшие решения](#)

[Дополнительные сведения](#)

[Введение](#)

Иногда при прохождении трафика через туннель настраиваемой инкапсуляции маршрутизации (GRE), можно успешно использовать команду ping и Telnet, но нельзя скачивать Internet страницы или пересылать файлы при помощи протокола передачи файлов (FTP). Данный документ содержит описание стандартной причины этой проблемы, а также методов ее обхода.

[Предварительные условия](#)

[Требования](#)

Для понимания данного документа требуется общее знание протокола GRE. См. эти документы для узнавания больше о GRE:

- [Общая маршрутная инкапсуляция](#)
- [Настройка](#) раздел [Туннеля GRE От узла к узлу и рабочих сценариев экстрасети VPN](#)

[Используемые компоненты](#)

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

[Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд \(только для зарегистрированных клиентов\).](#)

Условные обозначения

[Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.](#)

Фрагментация пакетов и сообщений ICMP

Этот документ использует эту схему сети в качестве примера:

На диаграмме, представленной выше, показано, как устанавливается сеанс TCP с веб-сервером, когда клиент хочет получить доступ к странице в Интернет. Во время этого процесса клиент и веб-сервер объявляют размеры своих MSS, сообщая друг другу о возможности принимать сегменты TCP, не превышающие эти значения. Получив значение MSS, каждое устройство вычисляет размер сегмента, который сможет отправлять. Такой размер называется максимальным размером сегмента для отправки (SMSS); он равен меньшему из двух MSS. [Дополнительные сведения о максимальном размере сегмента TCP см. в документе RFC 879.](#)

Предположим, что веб-сервер в предыдущем примере определяет размер отправляемых пакетов в 1500 байт. Следовательно, сервер отправляет клиенту пакет длиной 1500 байт и в IP-заголовке задает необходимость включения бита "не фрагментировать" (DF). Когда пакет поступает на R2, маршрутизатор пытается инкапсулировать его в туннельный пакет. При использовании туннельного интерфейса GRE максимальный размер передаваемого блока данных (MTU) на 24 байта меньше, чем IP MTU реального исходящего интерфейса. Для исходящего интерфейса Ethernet максимальный размер передаваемого блока данных IP на туннельном интерфейсе будет составлять 1500 минус 24, что составляет 1476 байт.

R2 осуществляет попытку отправки IP-пакета в 1500 байт на 1476-байтный IP MTU интерфейс. Поскольку это невозможно, R2 необходимо фрагментировать пакет, создав один пакет размером 1476 байт (IP-заголовок и данные) и один пакет размером 44 байта (24 байта данных и новый IP-заголовок размером 20 байт). R2 затем осуществляет инкапсуляцию GRE двух пакетов для получения пакетов 1500 и 68 байт, соответственно. Эти пакеты теперь можно отправить через реальный исходящий интерфейс, MTU IP которого составляет 1500 байт.

Однако помните, что пакет, полученный R2, имеет набор битов DF. Следовательно, R2 не может фрагментировать пакеты; вместо этого он должен подать команду веб-серверу для сокращения размеров пакетов. Для этого он отправляет пакет протокола управляющих сообщений Интернета (ICMP) тип 3 код 4 (Назначение недоступно; необходима фрагментация и набор DF). В этом сообщении ICMP содержатся правильный MTU для использования веб-сервером, который должен получить это сообщение и соответствующим образом изменить размер пакета.

Примечание: [Прежде чем выполнять какие-либо команды отладки, ознакомьтесь с документом "Важные сведения о командах отладки".](#)

Можно просмотреть сообщения ICMP, передаваемые R2 путем включения команды `debug ip icmp`:

```
ICMP: dst (10.10.10.10) frag. needed and DF set unreachable sent to 10.1.3.4
```

Заблокированные сообщения ICMP

Блокировка сообщений ICMP на пути к веб-серверу - это типичная проблема. Когда это происходит, пакет ICMP не достигает веб-сервера, что препятствует передаче данных между клиентом и сервером.

Решения

Одно из этих четырех решений позволит решить проблему:

- Определите, в каком месте пути заблокировано сообщение ICMP и можно ли его разблокировать.
- Установите MTU на сетевом интерфейсе Клиента к 1476 байтам, вынудив S S быть меньшими, таким образом, пакеты не должны будут быть фрагментированы, когда они достигают R2. Однако, если вы изменяете MTU для клиента, следует также изменить MTU для всех устройств, работающих в сети вместе с клиентом. В сегменте Ethernet может присутствовать большое количество этих устройств.
- Используйте прокси-сервер (или еще лучше Web cache engine) между R2 и маршрутизатором шлюза и позвольте прокси-серверу посылать запрос ко всем Интернет-страницам.
- Если туннель GRE проходит по соединениям, для которых значение MTU может превышать 1500 байт плюс заголовок туннеля, решением является увеличение значения MTU до 1524 байт (1500 плюс 24 байта для служебных данных GRE) для всех интерфейсов и соединений между конечными маршрутизаторами GRE.

Дальнейшие решения

Если вышеупомянутые опции не выполнимы тогда, эти опции могут быть полезными:

- Используйте маршрутизацию в соответствии с политикой, чтобы очистить и установить бит DF в пакете IP данных (доступный в релизе 12.1 программного обеспечения Cisco IOS (6) и позже).

```
interface ethernet0
...
ip policy route-map clear-df !--- This command is used to identify a route map !--- to use
for policy routing on an interface, !--- use the ip policy route-map command in !---
interface configuration mode. route-map clear-df permit 10 match ip address 101 set ip df 0
!--- This command is used to change the Don't Fragment (DF) !--- bit value in the IP header,
use this command !--- in route-map configuration mode. access-list 101 permit tcp 10.1.3.0
0.0.0.255 any
```

Это позволит пакетам данных IP фрагментироваться перед инкапсуляцией GRE. Принимающий конечный хост должен затем повторно собрать IP-пакеты данных. Это не представляет трудности.
- Измените значение параметра TCP MSS для пакетов SYN, которые проходят сквозь маршрутизатор (доступен в IOS версии 12.2(4)T и выше). *Это позволит сделать значение параметра MSS в пакете TCP SYN меньше, чем значение в команде ip tcp adjust-mss value, что в данном случае составляет 1436 (MTU минус размер заголовков IP, TCP и GRE).* После этого конечные хосты отправляют пакеты TCP/IP размером менее указанного значения.

```
interface tunnel0
...
ip tcp adjust-mss 1436 !--- This command is used to adjust the maximum segment size (MSS)
!--- value of TCP SYN packets going through the router. !--- The maximum segment size is in
the range from 500 to 1460.
```
- Последний вариант должен увеличить IP MTU на туннельном интерфейсе к 1500 (доступный в IOS 12.0 и позже). Однако увеличение туннеля IP MTU приводит к

фрагментации туннельных пакетов, поскольку DF-бит исходного пакета не копируется в заголовок туннельного пакета. В этом сценарии перед тем, как удалить заголовок GRE и переслать внутренний пакет, маршрутизатор на другом конце туннеля GRE должен повторно собрать туннельный пакет GRE. Повторная сборка IP-пакета выполняется в режиме обычной коммутации и использует память. Следовательно, этот параметр может значительно уменьшить проброс пакетов через GRE-туннель.

```
interface tunnel0
...
ip mtu 1500 !--- This command is used to set the maximum transmission unit (MTU) !--- size
of IP packets sent on an interface. The minimum size !--- you can configure is 128 bytes;
the maximum depends on the interface medium.
```

В заключение, наиболее часто причиной невозможности просмотра Интернет-страниц через туннель GRE, становится упомянутая выше проблема фрагментации. Решение заключается в разрешении пакетов ICMP или исследовании проблемы ICMP с помощью любого из приведенных выше решений.

[Дополнительные сведения](#)

- ["Устранение проблем с фрагментацией IP, значениями MTU, MSS, и PMTUD для GRE и IPSEC"](#)
- [Выбор подходящего VPN-решения?](#)
- [Страницы поддержки GRE](#)
- [Примеры конфигурации GRE](#)
- [Страница поддержки IP-маршрутизации](#)
- [Техническая поддержка - Cisco Systems](#)