

使用 GRE 隧道时为什么不能访问互联网？

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[数据包分段与 ICMP 消息](#)

[被阻挡的 ICMP 消息](#)

[解决方案](#)

[进一步的解决方法](#)

[相关信息](#)

简介

有时当时数据流经过通用路由封装 (GRE) 隧道时，您可以成功地使用ping命令和Telnet，但您不能使用文件传输协议(FTP) 下载互联网页或传输文件。本文档将说明此问题的常见原因，并提供几种解决方法。

先决条件

要求

本文档需要对 GRE 拥有基本的了解。要了解有关 GRE 的详细信息，请参阅以下文档：

- [通用路由封装](#)
- [站点到站点和外联网 VPN 业务方案](#)中的[配置 GRE 隧道](#)部分

使用的组件

本文档不限于特定的软件和硬件版本。

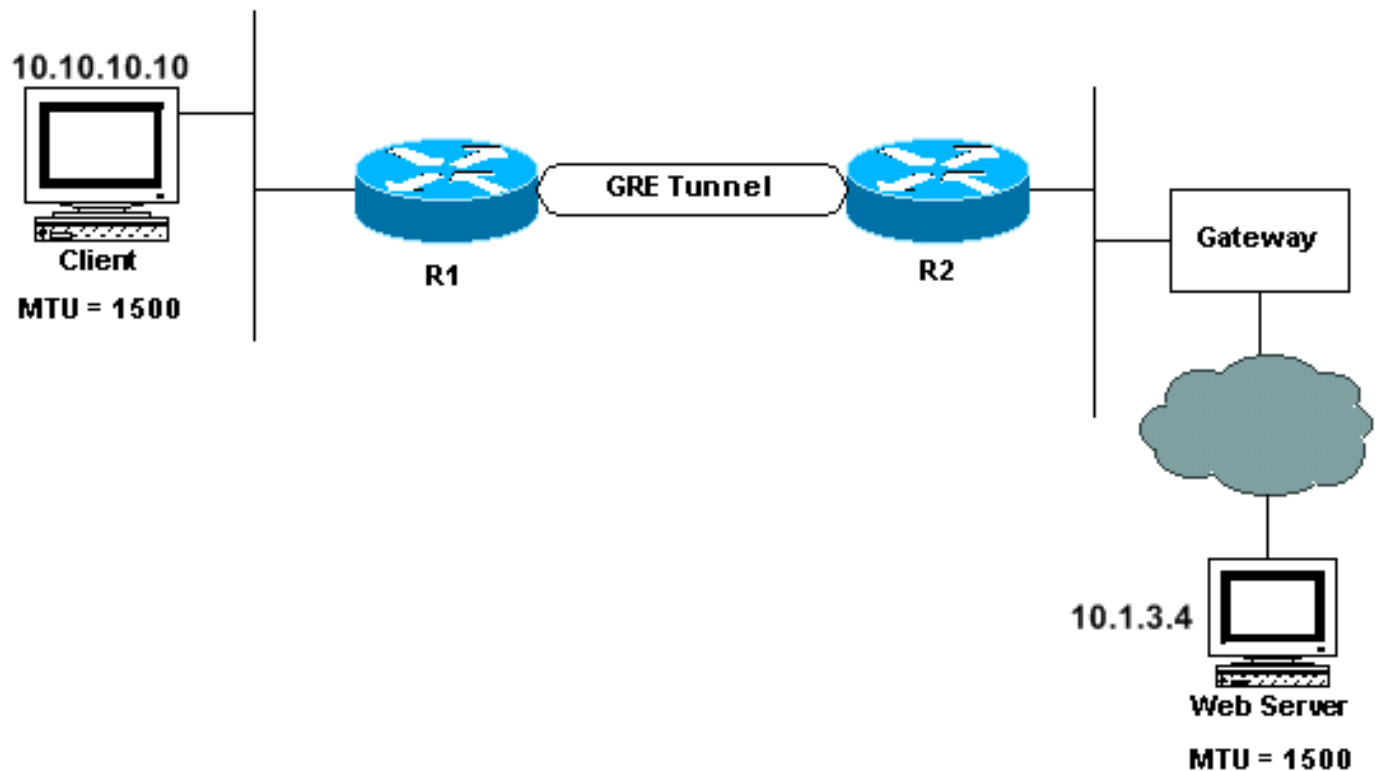
有关本文档所用命令的详细信息，请使用[命令查找工具](#) ([仅限注册用户](#))。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

[数据包分段与 ICMP 消息](#)

本文档使用以下网络图作为示例：



在以上图表中，当客户端想要访问互联网上的页面时，它将使用网络服务器建立 TCP 会话。在此进程期间，客户端和网络服务器宣布它们的最大分段尺寸(MSS)，彼此指示各自能接受最大这个尺寸的TCP分段。在接收 MSS 选项时，每个设备计算可以发送的分段大小。这呼叫发送最大分段大小(SMSS)，并且等于小两个MSSs。有关 TCP 最大数据段大小的详细信息，请参阅 [RFC 879](#)。

为了函数，假设网络服务器在上面的例子中确定它能发送 1500 个字节长的数据包。因此它向客户端发送 1500 字节数据包，并且，在 IP 头，设置“don't fragment”(DF)位。当数据包到达 R2 时，路由器会尝试将其封装成隧道数据包。在 GRE 隧道接口中，IP 最大传输单位(MTU)是 24 个字节，低于实际流出接口的 IP 最大传输单位。对于以太网流出接口，这意味着隧道接口上的 IP MTU 可能是 1500 减 24 或者 1476 个字节。

R2 在尝试将 1500 字节的 IP 数据包发送到 IP MTU 为 1476 字节的接口。由于这不可能实现，因此 R2 需要分段数据包，创建一个 1476 个字节的数据包(数据和 IP 头)和一个 44 个字节的数据包 (24 个字节的数据和一个 20 个字节的新 IP 头)。然后，R2 将这两个数据包以 GRE 方式封装，分别获得大小为 1500 字节和 68 字节的数据包。这些数据包现在可能被发送到实际出局接口外，共有 1500 字节 IP MTU。

但是，请记住，R2 接收的数据包设置了 DF 位。所以，R2 不能对数据包分段，相反地，它需要指示网络服务器发送更小的数据包。它通过发送互联网控制消息协议(ICMP) type 3 代码 4 数据包执行此(目的地不可达;需要分段但设置了 DF)。此 ICMP 数据包包含网络服务器将要使用的正确 MTU，网络服务器应该收到此消息，并相应调整数据包大小。

注意： 使用 `debug` 命令之前，请参阅 [有关 Debug 命令的重要信息](#)。

可以通过启用 `debug ip icmp` 命令查看 R2 发送的 ICMP 消息：

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

[被阻挡的 ICMP 消息](#)

在指向 Web 服务器的路径上阻止了 ICMP 消息时，就会发生常见问题。发生这一问题后，ICMP 数据包将始终无法到达 Web 服务器，从而使数据无法在客户端和服务器之间传输。

解决方案

这四个解决方案之一应能解决此问题：

- 找到 ICMP 消息被阻拦的路径，并查看您是否能够得到它的允许。
- 设置在客户端的网络接口的 MTU 为 1476 个字节，强制 MSS 更加小，因此数据包不会必须被分段，当他们到达 R2。然而，如果更改客户端的 MTU，您应该也更改与该客户端共享这个网络的所有设备的 MTU。在以太网段上，这可能会涉及大量的设备。
- 在 R2 和网关路由器之间使用一个代理服务器（或更好，使用 Web 缓存引擎），并且让代理服务器请求所有互联网页。
- 如果 GRE 隧道运行在链路上，可以有大于 1500 字节加隧道报头的 MTU，则另一个解决方案是将 GRE 终端路由器上的所有接口和链路上的 MTU 增加到 1524（1500 加上作为 GRE 开销的 24）。

进一步的解决方法

如果上述方案不可行，那么以下方案可能会有用：

- 使用策略路由清除并设置数据 IP 数据包中的 DF 位（在 Cisco IOS® 软件 12.1(6) 版和更高版本中可实现）。

```
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
```

这将允许数据 IP 数据包在 GRE 封装之前进行分段。接收端主机随后必须重组数据 IP 数据包。这通常不是问题。
- 更改穿过路由器（使用 IOS 12.2(4)T 和更高版本）的 SYN 数据包上的 TCP MSS 选项值。这降低了 TCP Syn 数据包中的 MSS 选项值，因此它比 `ip tcp adjust-mss value` 命令中的值小，在这种情况下为 1436（MTU 减 IP、TCP 和 GRE 头的大小）。终端主机现在发送的 TCP/IP 数据包将不会大于该值。

```
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.
```
- 最后一种方案是将隧道接口上的 IP MTU 增加到 1500（在 IOS 12.0 和更高版本中可实现）。然而，增加隧道 IP MTU 会导致隧道数据包分段，因为初始数据包的 DF 位没有被复制到隧道数据包包头。在此方案中，在能去除 GRE 头并转发内部数据包之前，在 GRE 封装隧道另一端的路由器必须重新组装 GRE 隧道数据包。IP 数据包重组在进程交换模式下完成，并且会占用内存。所以，此方案会显著降低通过 GRE 隧道的数据包吞吐量。

```
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.
```

总之，不能通过 GRE 隧道浏览互联网的最常见原因是上述分段问题。解决方案将允许 ICMP 数据包通过，或者使用任何上述解决方案作为解决 ICMP 相关故障的 workaround。

相关信息

- [解决 GRE 和 IPSEC 中的 IP 分段、MTU、MSS 和 PMTUD 问题](#)
- [哪种 VPN 解决方案适合您？](#)
- [GRE 支持页面](#)
- [GRE 配置示例](#)
- [IP 路由支持页](#)
- [技术支持 - Cisco Systems](#)