

# Por que não navegar na Internet usando um túnel GRE?

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Fragmentação de pacote e mensagens ICMP](#)

[Mensagens ICMP bloqueadas](#)

[Soluções](#)

[Outras soluções](#)

[Informações Relacionadas](#)

## [Introdução](#)

Às vezes, quando o tráfego passar por um túnel de Generic Routing Encapsulation (GRE), é possível usar com êxito o comando ping e o Telnet, porém será possível fazer o download de páginas de Internet ou transferir arquivos usando o File Transfer Protocol (FTP). Este documento explica um motivo comum para o problema e oferece várias soluções alternativas.

## [Pré-requisitos](#)

### [Requisitos](#)

Este documento exige noções básicas de GRE. Refira estes documentos para aprender mais sobre o GRE:

- [Encapsulamento de roteamento genérico](#)
- [Configurar uma seção do túnel GRE da site para site e dos cenários de negócios de VPN Extranet](#)

### [Componentes Utilizados](#)

Este documento não se restringe a versões de software e hardware específicas.

Use a ferramenta [Command Lookup Tool](#) ([apenas para clientes registrados](#)) para obter mais informações sobre os comandos usados neste documento.

### [Convenções](#)

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

## [Fragmentação de pacote e mensagens ICMP](#)

Este documento usa este diagrama da rede como um exemplo:

No diagrama acima, quando o cliente quiser acessar uma página da Internet, ele estabelece uma sessão de TCP com o Servidor de Web. Durante esse processo, os Servidores Cliente e Web anunciam o tamanho máximo de segmento (MSS), indicando um ao outro que podem aceitar segmentos de TCP até esse tamanho. Após o recebimento da opção MSS, cada dispositivo calcula o tamanho do segmento que pode ser enviado. Isso se chama Send Max Segment Size (SMSS) e equivale ao menor dos dois MSSs. [Para obter mais informações sobre o Tamanho máximo de segmento do TCP, consulte o RFC 879.](#)

Para o argumento, deixe-nos dizer o servidor de Web no exemplo acima determina que pode enviar a pacotes até 1500 bytes de comprimento. Envia conseqüentemente um pacote de bytes 1500 ao cliente, e, no cabeçalho IP, ajusta o bit do “Don't Fragment” (DF). Quando o pacote chega no R2, o roteador tenta encapsulá-lo no pacote de túnel. No caso da interface do túnel GRE, a unidade de transmissão máxima IP (MTU) é 24 bytes menos do que o IP MTU da interface enviada real. Para uma interface enviada dos Ethernet que significasse o IP MTU na interface de túnel seria 1500 menos 24, ou 1476 bytes.

O R2 está tentando enviar um pacote IP de 1500 byte em uma interface MTU IP de 1476 byte. Como isto não é possível, o R2 necessita fragmentar o pacote, criando um pacote de 1476 bytes (dados e cabeçalho de IP) e um pacote de 44 bytes (24 bytes de dados e um novo cabeçalho de IP de 20 bytes). O R2 então GRE encapsula both of these pacotes para obter 1500 e 68 pacotes de bytes, respectivamente. Esses pacotes podem ser enviados agora para a verdadeira interface externa, que tem uma MTU de IP de 1500 bytes.

No entanto, lembre-se de que o pacote recebido pelo R2 tem o conjunto de bits DF. Portanto, o R2 não pode fragmentar o pacote e, em vez disso, precisa instruir o servidor da Web a enviar pacotes menores. Faz este enviando um tipo 3 pacote do Internet Control Message Protocol (ICMP) do código 4 (destino inacessível; Fragmentação necessária e DF ajustar-se). Este mensagem ICMP contém o MTU correto a ser usado pelo servidor de Web, que deve receber esta mensagem e ajusta o tamanho do pacote em conformidade.

**Nota:** Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos **debug**.

Você pode ver os mensagens ICMP enviados pelo R2 permitindo o **comando debug ip icmp**:

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

## [Mensagens ICMP bloqueadas](#)

Um problema comum ocorre quando os mensagens ICMP são obstruídos ao longo do trajeto ao servidor de Web. Quando isto acontece, o pacote ICMP nunca alcança o servidor de Web, impedindo desse modo que os dados passem entre o cliente e servidor.

## [Soluções](#)

Uma destas quatro soluções deve resolver o problema:

- Descubra em que parte do caminho a mensagem de ICMP está bloqueada e veja se consegue obter permissão para ela.
- Ajuste o MTU na interface de rede do cliente a 1476 bytes, forçando o MSS para ser menor, assim que os pacotes não terão que ser fragmentados quando alcançam o R2. No entanto, se você alterar o MTU para o cliente, você também deve alterar o MTU para todos os dispositivos que compartilham a rede com este cliente. Em um segmento de Ethernet, este podia ser um grande número dispositivos.
- Use um proxy server (ou, mesmo melhor, um Engine de Cache da Web) entre o R2 e o gateway router, e deixe o pedido do proxy server todas as páginas de Internet.
- Se o túnel GRE for executado em links cujo MTU possa ser maior do que 1500 bytes, além do cabeçalho do túnel, então a outra solução é aumentar o MTU para 1524 (1500 mais 24 para a carga adicional do GRE) em todas as interfaces e links entre os roteadores de ponto final de GRE.

## Outras soluções

Se as opções acima não são praticáveis então estas opções podem ser úteis:

- Use o roteamento de política para cancelar e ajustar o DF mordido no pacote IP dos dados (disponível no Software Release 12.1(6) e Mais Recente de Cisco IOS®).

```
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
```

Isto permitirá que o pacote IP dos dados seja fragmentado antes que esteja GRE encapsulado. O host final receptor deve então remontar os pacotes de dados IP. Geralmente, isto não é um problema.
- Mude o valor de opção MSS TCP nos pacotes SYN que transversal através do roteador (disponível em IO 12.2(4)T e mais alto). Isto reduz o valor de opção MSS no pacote SYN de TCP de modo que seja menor do que o valor no comando **ip tcp adjust-mss value**, neste caso 1436 (MTU menos o tamanho do IP, do TCP, e dos cabeçalhos de GRE). Os host finais enviam agora os pacotes TCP/IP não maiores do que este valor.

```
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.
```
- Uma opção final é aumentar o IP MTU na interface de túnel a 1500 (disponível em IO 12.0 e mais atrasado). Contudo, aumentar o IP MTU do túnel faz com que os pacotes de túnel sejam fragmentados porque o bit DF do pacote original não é copiado ao encabeçamento de pacote de túnel. Neste cenário, o roteador na outra extremidade do túnel GRE deve remontar o pacote de túnel GRE antes de poder remover o cabeçalho GRE e encaminhar o pacote interno. A remontagem do pacote de IP é efetuada no modo de Process-Switch e usa memória. Portanto, essa opção pode reduzir significativamente o ritmo de transferência do pacote por meio do túnel GRE.

```
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.*

Concluindo, a causa mais comum da impossibilidade de navegar a internet por um túnel GRE é o problema de fragmentação mencionado acima. A solução é permitir pacotes ICMP ou resolver o problema ICMP com qualquer uma das soluções acima.

## Informações Relacionadas

- [Fragmentação de IP da resolução, edições MTU, MSS, e PMTUD com GRE e IPSEC](#)
- [Que solução de VPN é perfeita para você?](#)
- [Páginas de suporte de GRE](#)
- [Exemplos de Configuração GRE](#)
- [Página de Suporte do IP Routing](#)
- [Suporte Técnico - Cisco Systems](#)