

# ¿Por qué no puedo navegar por Internet cuando utilizo un túnel GRE?

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Fragmentación de paquetes y mensajes ICMP](#)

[Mensajes ICMP bloqueados](#)

[Soluciones](#)

[Soluciones adicionales](#)

[Información Relacionada](#)

## Introducción

A veces, cuando el tráfico atraviesa un encapsulado de ruteo genérico (GRE), puede utilizar con éxito el comando ping y realizar una conexión Telnet, pero no puede descargar páginas de Internet o transferir archivos utilizando el protocolo de transferencia de archivos (FTP). Este documento explica un motivo frecuente para este problema y ofrece varias soluciones alternativas.

## Prerequisites

### Requirements

Este documento requiere una comprensión básica de GRE. Consulte estos documentos para obtener más información sobre GRE:

- [Encapsulación de ruteo genérico](#)
- La sección [Configuración de un Túnel GRE](#) de [Escenarios Empresariales de VPN de Sitio a Sitio y Extranet](#)

### Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

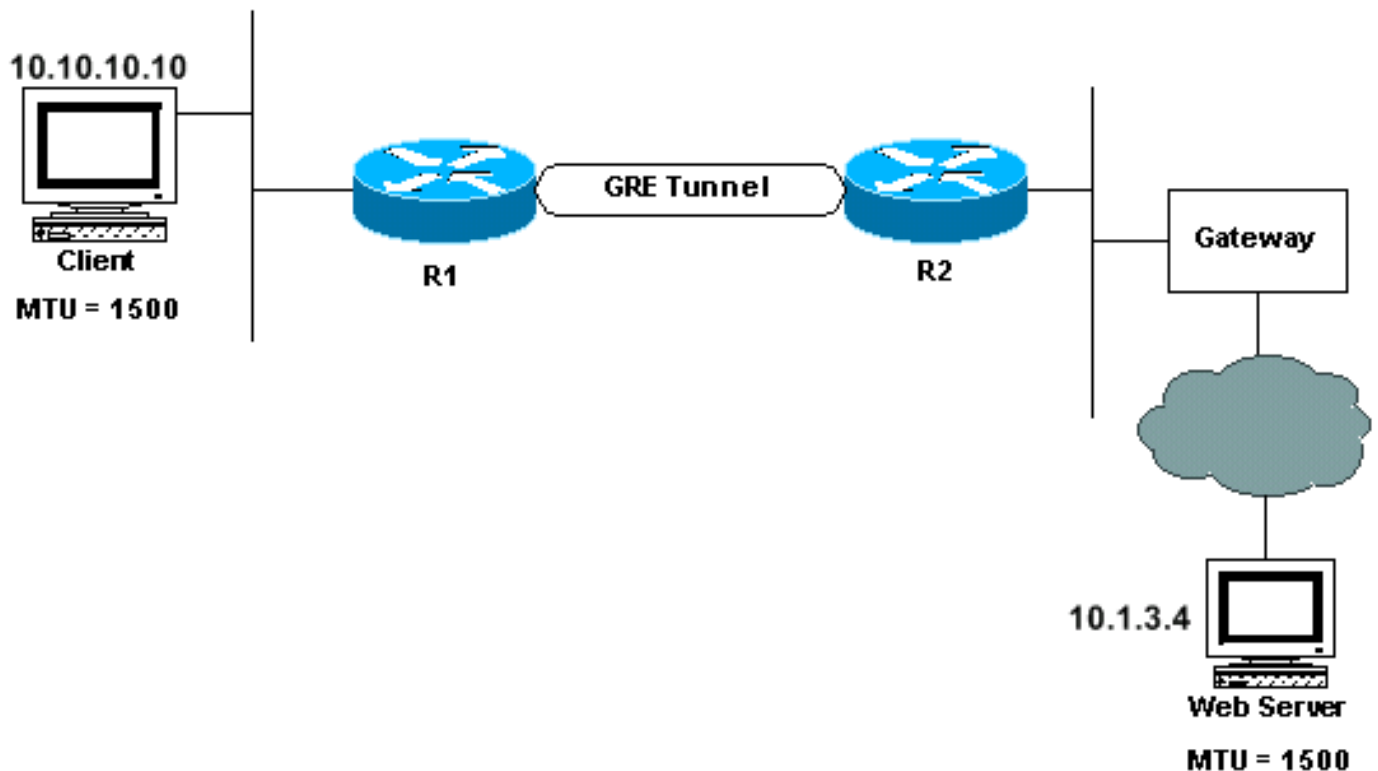
Use la herramienta [Command Lookup Tool \(clientes registrados solamente\)](#) para encontrar más información sobre los comandos usados en este documento.

## Convenciones

Consulte [Convenciones de Consejos Técnicos Cisco](#) para obtener más información sobre las convenciones del documento.

## Fragmentación de paquetes y mensajes ICMP

Este documento utiliza este diagrama de red como ejemplo:



En el diagrama precedente, cuando el cliente desea acceder a una página en Internet, establece una sesión TCP con el servidor Web. Durante este proceso, el cliente y el servidor Web anuncian el tamaño de segmento máximo (MSS), y así se indican el uno al otro que pueden aceptar segmentos TCP hasta este tamaño. Luego de recibir la opción MSS, cada dispositivo calcula el tamaño del segmento que se puede enviar. Esto se llama –Envío del tamaño máximo de segmento (SMSS) y es igual al más chico de los dos MSS. Si desea obtener más información sobre el tamaño máximo de segmento de TCP, consulte RFC 879.

En aras del argumento, digamos que el servidor Web en el ejemplo anterior determina que puede enviar paquetes de hasta 1500 bytes de longitud. Por lo tanto, envía un paquete de 1500 bytes al cliente y, en el encabezado IP, establece el bit "don't fragment" (DF). Cuando un paquete ingresa al router R2, el router intenta encapsularlo al paquete de túnel. En el caso de la interfaz de túnel GRE, la unidad de transmisión máxima (MTU) IP es 24 bytes menos que la MTU IP de la interfaz de salida real. Para una interfaz de salida Ethernet que significa que la MTU IP en la interfaz de túnel sería de 1500 menos 24 o 1476 bytes.

R2 intenta enviar un paquete IP de 1500 bytes dentro de una interfaz MTU IP de 1476 bytes. Dado que esto no es posible, R2 debe fragmentar el paquete, creando un paquete de 1476 bytes (datos y encabezado IP) y un paquete de 44 bytes (24 bytes de datos y un nuevo encabezado IP de 20 bytes). R2 luego GRE encapsula ambos paquetes para obtener paquetes de 1500 y 68

bytes, respectivamente. Estos paquetes ahora pueden enviarse a la interfaz de salida real, la cual tiene una MTU IP de 1500 bytes.

Sin embargo, recuerde que el paquete recibido por R2 tiene configurado el bit DF. Por lo tanto, R2 no puede fragmentar el paquete y, en su lugar, necesita instruir al servidor Web para que envíe paquetes más pequeños. Para ello, envía un paquete de código 4 (Destino inalcanzable; Fragmentación necesaria y DF configurado). Este mensaje ICMP contiene la MTU correcta que utilizará el servidor Web, que debe recibir este mensaje y ajustar el tamaño del paquete en consecuencia.

**Nota:** Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos debug.

Puede ver los mensajes ICMP enviados por R2 habilitando el comando **debug ip icmp**:

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

## Mensajes ICMP bloqueados

Un problema común ocurre cuando los mensajes ICMP se bloquean a lo largo de la trayectoria al servidor Web. Cuando esto sucede, el paquete ICMP nunca llega al servidor Web, evitando así que los datos pasen entre el cliente y el servidor.

## Soluciones

Una de estas cuatro soluciones debería resolver el problema:

- Averigüe adónde durante el camino, se bloquea el mensaje ICMP y vea si puede autorizarlo.
- Establezca la MTU en la interfaz de red del Cliente en 1476 bytes, lo que obliga al SMSS a ser más pequeño, de modo que los paquetes no tendrán que fragmentarse cuando alcancen R2. Sin embargo, si cambia la MTU para el Cliente, también debería cambiar la MTU para todos los dispositivos que comparten la red con este Cliente. En un segmento Ethernet, podría ser un gran número de dispositivos.
- Utilice un servidor proxy (o, mejor aún, un motor de caché Web) entre R2 y el router de la puerta de enlace, y deje que el servidor proxy solicite todas las páginas de Internet.
- Si el túnel GRE se ejecuta sobre links que pueden tener una MTU de más de 1500 bytes más el encabezado del túnel, entonces otra solución es aumentar la MTU a 1524 (1500 más 24 para el overhead de GRE) en todas las interfaces y links entre los routers de puntos extremos de GRE.

## Soluciones adicionales

Si las opciones anteriores no son factibles, estas opciones pueden ser útiles:

- Utilice el ruteo de políticas para borrar y establecer el bit DF en el paquete IP de datos (disponible en Cisco IOS® Software Release 12.1(6) y posteriores).

```
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
```

Esto permitirá que el paquete IP de datos se fragmente antes de que se encapsula GRE. Luego, el host final de recepción debe reensamblar los paquetes IP de datos. Esto no suele ser un problema.

- Cambie el valor de la opción TCP MSS en los paquetes SYN que atraviesan el router (disponible en IOS 12.2(4)T y superiores). Esto reduce el valor de la opción MSS en el paquete TCP SYN de modo que sea menor que el valor del comando **ip tcp adjust-mss value, en este caso 1436 (MTU menos el tamaño de los encabezados IP, TCP y GRE)**. Los hosts finales ahora envían paquetes TCP/IP no mayores 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.
```

- Una última opción es aumentar la MTU IP en la interfaz de túnel a 1500 (disponible en IOS 12.0 y posteriores). Sin embargo, al aumentar la MTU IP del túnel, los paquetes del túnel se fragmentan porque el bit DF del paquete original no se copia en el encabezado del paquete del túnel. En este escenario, el router en el otro extremo del túnel GRE debe volver a ensamblar el paquete del túnel GRE antes de que pueda quitar el encabezado GRE y reenviar el paquete interno. El reensamblado de paquetes de IP se realiza en modo de switch de proceso y utiliza memoria. Por lo tanto, esta opción puede reducir en gran medida la producción de paquetes a través del 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.
```

En resumen, la causa más frecuente por la que no se puede navegar por Internet sobre un túnel GRE se debe al problema de fragmentación ya mencionado. La solución es admitir los paquetes ICMP o resolver el problema ICMP con cualquiera de las soluciones alternativas previamente mencionadas.

## [Información Relacionada](#)

- [Resolver fragmentación IP y problemas de MTU, MSS y PMTUD con GRE e IPSEC](#)
- [¿Qué solución VPN es la adecuada para usted?](#)
- [Páginas de soporte de GRE](#)
- [Ejemplos de configuración de GRE](#)
- [Página de Soporte de IP Routing](#)
- [Soporte Técnico - Cisco Systems](#)