

Perché non è possibile esplorare Internet quando si utilizza un tunnel GRE?

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Frammentazione dei pacchetti e messaggi ICMP](#)

[Messaggi ICMP bloccati](#)

[Soluzioni](#)

[Ulteriori soluzioni](#)

[Informazioni correlate](#)

[Introduzione](#)

A volte, quando il traffico attraversa un tunnel GRE (Generic Routing Encapsulation), è possibile usare il comando **ping** e Telnet, ma non è possibile scaricare pagine Internet o trasferire file con il protocollo FTP (File Transfer Protocol). Questo documento spiega una causa comune del problema e offre diverse soluzioni.

[Prerequisiti](#)

[Requisiti](#)

Questo documento richiede una comprensione di base del GRE. Per ulteriori informazioni sul GRE, consultare i seguenti documenti:

- [Generic Routing Encapsulation](#)
- Sezione [Configurazione di un tunnel GRE in scenari aziendali VPN da sito a sito ed Extranet](#)

[Componenti usati](#)

Il documento può essere consultato per tutte le versioni software o hardware.

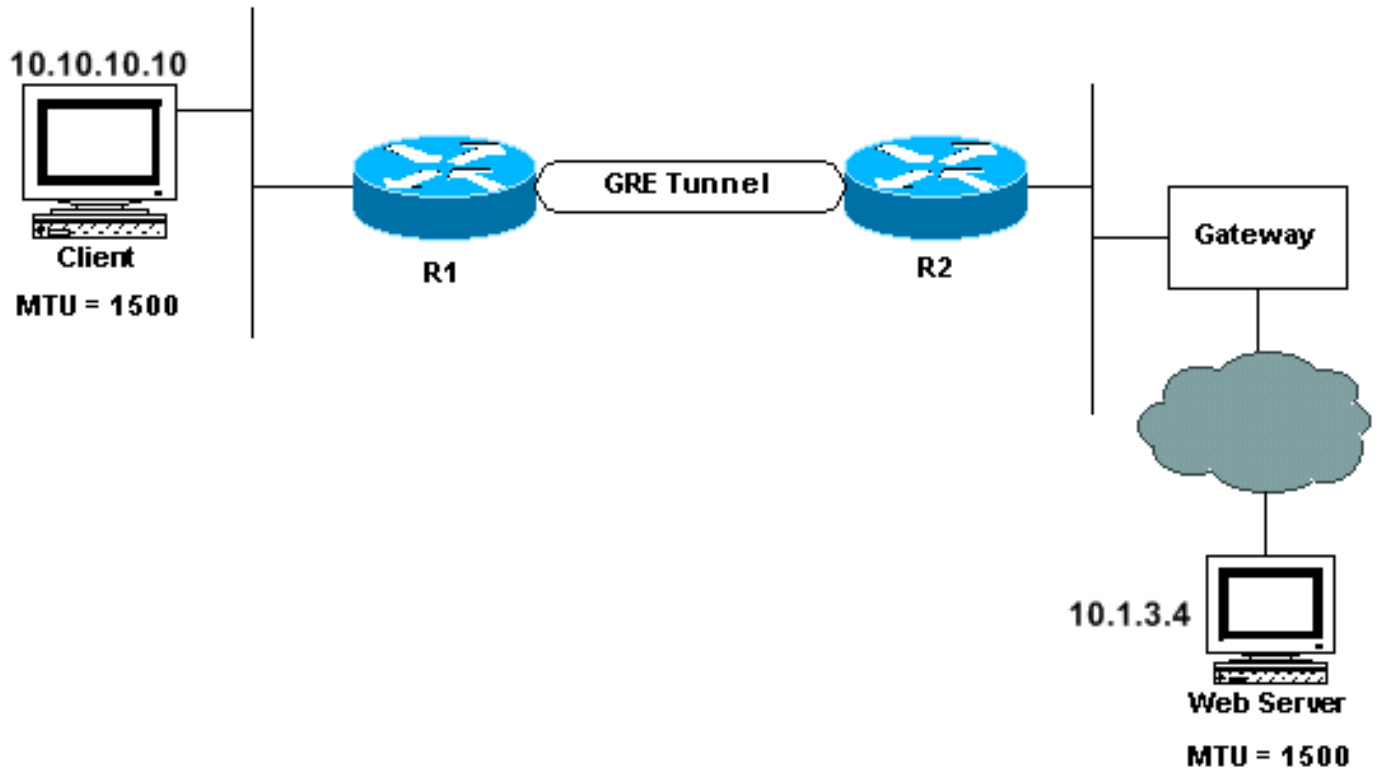
per ulteriori informazioni sui comandi menzionati in questo documento, usare lo [strumento di ricerca dei comandi](#) (solo utenti [registrati](#)).

[Convenzioni](#)

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

Frammentazione dei pacchetti e messaggi ICMP

In questo documento viene usato questo diagramma di rete come esempio:



Nel diagramma precedente, quando il client desidera accedere a una pagina su Internet, stabilisce una sessione TCP con il server Web. Durante questo processo, il client e il server Web annunciano le dimensioni massime del segmento (MSS), indicando a vicenda che possono accettare segmenti TCP fino a queste dimensioni. Dopo aver ricevuto l'opzione MSS, ciascun dispositivo calcola le dimensioni del segmento che può essere inviato. Questo valore è denominato SMSS (Send Max Segment Size) e corrisponde al valore più piccolo dei due valori MSS. Per ulteriori informazioni sulle dimensioni massime del segmento TCP, vedere la [RFC 879](#).

Per motivi di praticità, supponiamo che il server Web nell'esempio precedente determini che può inviare pacchetti fino a 1500 byte. Pertanto, invia un pacchetto da 1500 byte al client e, nell'intestazione IP, imposta il bit "non frammentare" (DF, Don't Fragment). Quando il pacchetto arriva alla R2, il router tenta di incapsularlo nel pacchetto del tunnel. Nel caso dell'interfaccia del tunnel GRE, l'MTU (Maximum Transmission Unit) dell'IP è 24 byte inferiore all'MTU dell'IP dell'interfaccia in uscita reale. Per un'interfaccia Ethernet in uscita, cioè, l'MTU IP sull'interfaccia del tunnel sarebbe 1500 meno 24, o 1476 byte.

R2 sta tentando di inviare un pacchetto IP da 1500 byte a un'interfaccia MTU IP da 1476 byte. Poiché questo non è possibile, R2 deve frammentare il pacchetto, creando un pacchetto di 1476 byte (dati e intestazione IP) e un pacchetto di 44 byte (24 byte di dati e una nuova intestazione IP di 20 byte). R2 quindi GRE incapsula entrambi i pacchetti per ottenere rispettivamente i pacchetti da 1500 e 68 byte. Questi pacchetti possono ora essere inviati all'interfaccia in uscita reale, che ha una MTU IP di 1500 byte.

Tuttavia, tenere presente che per il pacchetto ricevuto da R2 il bit DF è impostato. Pertanto, R2 non può frammentare il pacchetto e deve indicare al server Web di inviare pacchetti più piccoli. A tale scopo, invia un pacchetto di codice 4 per il protocollo ICMP (Internet Control Message Protocol) 3 (destinazione irraggiungibile; frammentazione richiesta e DF impostato). Questo messaggio ICMP contiene l'MTU corretta che deve essere usata dal server Web, che deve ricevere il messaggio e modificare le dimensioni del pacchetto di conseguenza.

Nota: consultare le [informazioni importanti sui comandi di debug prima di usare i comandi di debug](#).

È possibile visualizzare i messaggi ICMP inviati da R2 abilitando il comando **debug ip icmp**:

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

Messaggi ICMP bloccati

Un problema comune si verifica quando i messaggi ICMP vengono bloccati lungo il percorso al server Web. In questo caso, il pacchetto ICMP non raggiunge mai il server Web, impedendo il passaggio dei dati tra il client e il server.

Soluzioni

Una di queste quattro soluzioni dovrebbe risolvere il problema:

- Verificare in quale punto del percorso il messaggio ICMP è bloccato e verificare che sia possibile visualizzarlo.
- Impostare l'MTU dell'interfaccia di rete del client a 1476 byte, forzando la riduzione del valore SMSS in modo che i pacchetti non debbano essere frammentati quando raggiungono la R2. Tuttavia, se si modifica l'MTU del client, è necessario modificare anche l'MTU di tutti i dispositivi che condividono la rete con questo client. Su un segmento Ethernet, potrebbe trattarsi di un numero elevato di dispositivi.
- Utilizzare un server proxy (o, meglio, un motore di cache Web) tra R2 e il router gateway e lasciare che il server proxy richieda tutte le pagine Internet.
- Se il tunnel GRE viene eseguito su collegamenti che possono avere una MTU superiore a 1500 byte più l'intestazione del tunnel, un'altra soluzione è aumentare la MTU a 1524 (1500 più 24 per il sovraccarico GRE) su tutte le interfacce e i collegamenti tra i router dell'endpoint GRE.

Ulteriori soluzioni

Se le opzioni di cui sopra non sono possibili, queste opzioni possono essere utili:

- Usare il routing di policy per cancellare e impostare il bit DF nel pacchetto IP dei dati (disponibile a partire da Cisco IOS® versione 12.1(6)).

```
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
```

In questo modo, il pacchetto IP dei dati verrà frammentato prima di essere incapsulato dal GRE. L'host ricevente deve quindi ricomporre i pacchetti IP di dati. Questo solitamente non è un problema.

- Modificare il valore dell'opzione TCP MSS sui pacchetti SYN che attraversano il router (disponibile su IOS versione 12.2(4)T e successive). In questo modo il valore MSS nel pacchetto TCP SYN viene abbassato in modo che sia inferiore al valore specificato nel comando **ip tcp adjust-mss value** (MTU meno le dimensioni delle intestazioni IP, TCP e GRE). Gli host terminali non inviano ora pacchetti TCP/IP più grandi di questo valore.

```
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.
```

- In alternativa, è possibile aumentare l'MTU IP sull'interfaccia del tunnel a 1500 (disponibile su IOS versione 12.0 e successive). Tuttavia, se si aumenta l'MTU IP del tunnel, i pacchetti del tunnel vengono frammentati perché il bit DF del pacchetto originale non viene copiato nell'intestazione del pacchetto del tunnel. In questo scenario, il router sull'altra estremità del tunnel GRE deve ricomporre il pacchetto del tunnel GRE prima di poter rimuovere l'intestazione GRE e inoltrare il pacchetto interno. Il riassettaggio del pacchetto IP viene eseguito in modalità process-switch e usa la memoria. Pertanto, questa opzione può ridurre in modo significativo il throughput del pacchetto attraverso il tunnel 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.
```

In conclusione, la causa più comune dell'impossibilità di navigare in Internet su un tunnel GRE è la suddetta frammentazione. La soluzione è consentire i pacchetti ICMP o risolvere il problema ICMP con una delle soluzioni sopra indicate.

[Informazioni correlate](#)

- [Risoluzione dei problemi di IP Fragmentation, MTU, MSS e PMTUD con GRE e IPSEC](#)
- [Quale soluzione VPN è giusta per te?](#)
- [Pagine di supporto GRE](#)
- [Esempi di configurazione GRE](#)
- [Pagina di supporto per il routing IP](#)
- [Supporto tecnico – Cisco Systems](#)