

Why Can't I Browse the Internet when Using a GRE Tunnel?

Document ID: 13725

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Packet Fragmentation and ICMP Messages

Blocked ICMP Messages

- Solutions
- Further Solutions

Related Information

Introduction

Sometimes when traffic goes through a generic routing encapsulation (GRE) tunnel, you can successfully use the **ping** command and Telnet, but you cannot download Internet pages or transfer files using File Transfer Protocol (FTP). This document explains a common reason for this problem, and offers several workarounds.

Prerequisites

Requirements

This document requires a basic understanding of GRE. Refer to these documents to learn more about GRE:

- [Generic Routing Encapsulation](#) 
- The Configuring a GRE Tunnel section of Site-to-Site and Extranet VPN Business Scenarios

Components Used

This document is not restricted to specific software and hardware versions.

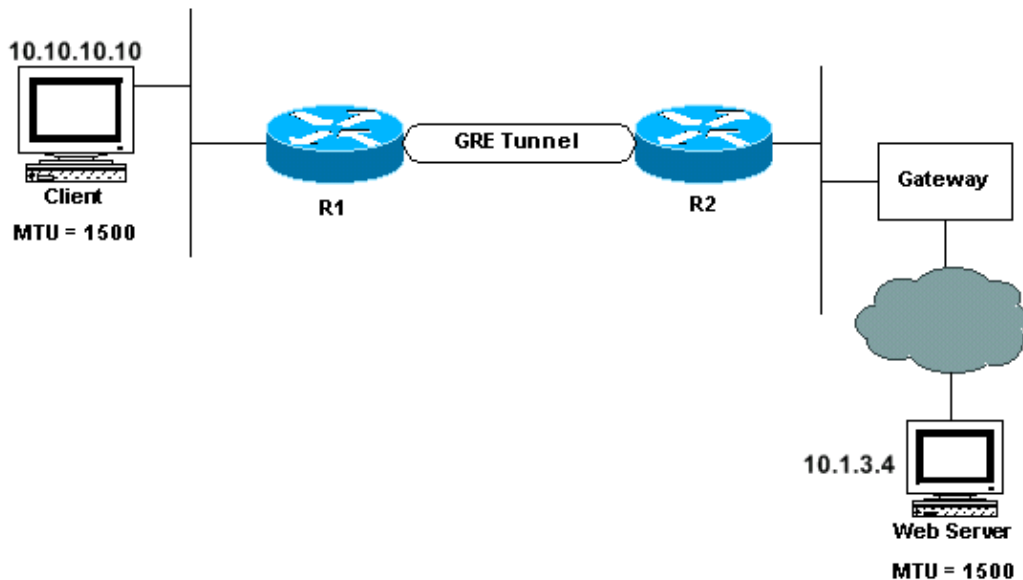
Use the Command Lookup Tool (registered customers only) to find more information on the commands used in this document.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Packet Fragmentation and ICMP Messages

This document uses this network diagram as an example:



In the diagram above, when the Client wants to access a page on the Internet, it establishes a TCP session with the Web Server. During this process, the Client and Web Server announce their maximum segment size (MSS), indicating to each other that they can accept TCP segments up to this size. Upon receiving the MSS option, each device calculates the size of the segment that can be sent. This is called the Send Max Segment Size (SMSS), and it equals the smaller of the two MSSs. For more information about TCP Maximum Segment Size, see RFC 879 [↗](#).

For the sake of argument, let's say the Web Server in the example above determines that it can send packets up to 1500 bytes in length. It therefore sends a 1500 byte packet to the Client, and, in the IP header, it sets the "don't fragment" (DF) bit. When the packet arrives at R2, the router tries encapsulating it into the tunnel packet. In the case of the GRE tunnel interface, the IP maximum transmission unit (MTU) is 24 bytes less than the IP MTU of the real outgoing interface. For an Ethernet outgoing interface that means the IP MTU on the tunnel interface would be 1500 minus 24, or 1476 bytes.

R2 is trying to send a 1500 byte IP packet into a 1476 byte IP MTU interface. Since this is not possible, R2 needs to fragment the packet, creating one packet of 1476 bytes (data and IP header) and one packet of 44 bytes (24 bytes of data and a new IP header of 20 bytes). R2 then GRE encapsulates both of these packets to get 1500 and 68 byte packets, respectively. These packets can now be sent out the real outbound interface, which has a 1500 byte IP MTU.

However, remember that the packet received by R2 has the DF bit set. Therefore, R2 can't fragment the packet, and instead, it needs to instruct the Web Server to send smaller packets. It does this by sending an Internet Control Message Protocol (ICMP) type 3 code 4 packet (Destination Unreachable; Fragmentation Needed and DF set). This ICMP message contains the correct MTU to be used by the Web Server, which should receive this message and adjust the packet size accordingly.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

You can view the ICMP messages sent by R2 by enabling the **debug ip icmp** command:

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

Blocked ICMP Messages

A common problem occurs when ICMP messages are blocked along the path to the Web server. When this

happens, the ICMP packet never reaches the Web server, thereby preventing data from passing between client and server.

Solutions

One of these four solutions should solve the problem:

- Find out where along the path the ICMP message is blocked, and see if you can get it allowed.
- Set the MTU on the Client's network interface to 1476 bytes, forcing the MSS to be smaller, so packets will not have to be fragmented when they reach R2. However, if you change the MTU for the Client, you should also change the MTU for all devices that share the network with this Client. On an Ethernet segment, this could be a large number of devices.
- Use a proxy-server (or, even better, a Web cache engine) between R2 and the Gateway router, and let the proxy-server request all the Internet pages.
- If the GRE tunnel runs over links that can have an MTU greater than 1500 bytes plus the tunnel header, then another solution is to increase the MTU to 1524 (1500 plus 24 for the GRE overhead) on all interfaces and links between the GRE endpoint routers.

Further Solutions

If the above options are not feasible then these options can be useful:

- Use policy routing to clear and set the DF bit in the data IP packet (available in Cisco IOS® Software Release 12.1(6) and later).

```
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
```

This will allow the data IP packet to be fragmented before it is GRE encapsulated. The receiving end host must then reassemble the data IP packets. This is usually not a problem.

- Change the TCP MSS option value on SYN packets that traverse through the router (available in IOS 12.2(4)T and higher). This reduces the MSS option value in the TCP SYN packet so that it's smaller than the value in the `ip tcp adjust-mss value` command, in this case 1436 (MTU minus the size of the IP, TCP, and GRE headers). The end hosts now send TCP/IP packets no larger than this value.

```
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.
```

- A final option is to increase the IP MTU on the tunnel interface to 1500 (available in IOS 12.0 and later). However, increasing the tunnel IP MTU causes the tunnel packets to be fragmented because the DF bit of the original packet is not copied to the tunnel packet header. In this scenario, the router on the other end of the GRE tunnel must reassemble the GRE tunnel packet before it can remove the GRE header and forward the inner packet. IP packet reassembly is done in process-switch mode and uses memory. Therefore, this option can significantly reduce the packet throughput through the GRE tunnel.

```
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 conclusion, the most common cause of not being able to browse the Internet over a GRE tunnel is due to the above mentioned fragmentation issue. The solution is to allow the ICMP packets or work around the ICMP problem with any of the above solutions.

Related Information

- [Resolve IP Fragmentation, MTU, MSS, and PMTUD Issues with GRE and IPSEC](#)
- [Which VPN Solution is Right for You?](#)
- [GRE Support Pages](#)
- [GRE Configuration Examples](#)
- [IP Routing Support Page](#)
- [Technical Support – Cisco Systems](#)