Chapter 22

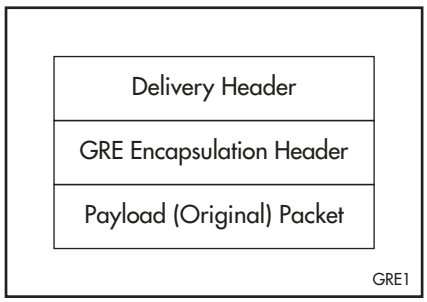
Generic Routing Encapsulation (GRE)

Introduction

Generic Routing Encapsulation (GRE) is a mechanism for encapsulating any network layer protocol over any other network layer protocol. The general specification is described in RFC 1701, and the encapsulation of IP packets over IP is defined in RFC 1702 as a specific implementation of GRE.

In the general case, a network layer packet, called the *payload packet*, is encapsulated in a GRE packet, which may also include source route information. The resulting GRE packet is then encapsulated in some other network layer protocol, called the *delivery protocol*, and then forwarded (Figure 22-1 on page 22-2).

Figure 22-1: Format of a packet with GRE encapsulation.



The only specific standard for GRE encapsulation is IP over IP (RFC 1702) and this is the standard supported by the router. The main use of the RFC 1702 standard is to route IP packets between private IP networks across an internet that uses globally assigned IP addresses. Private IP networks may either use IP addresses from the ranges of IP addresses reserved for private networks in RFC 1597 (Table 22-1 on page 22-2), or worse, any randomly selected range of IP addresses.

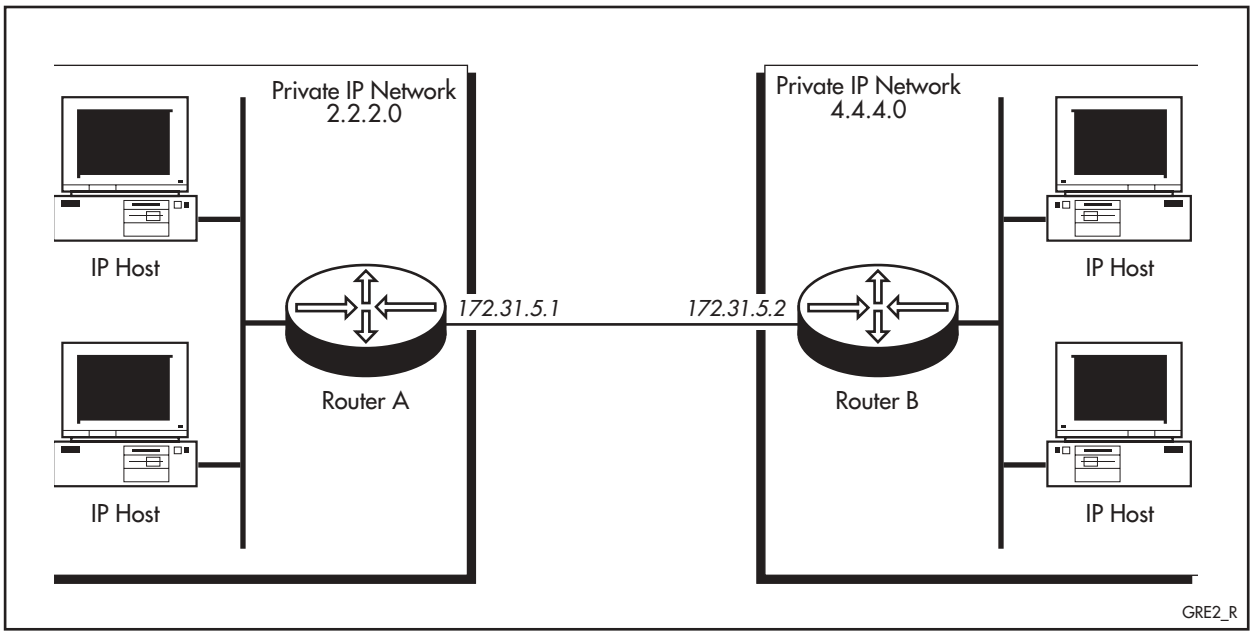
Table 22-1: IP address ranges reserved for private IP networks by RFC 1597.

Network Class	Reserved IP Address Range
A	10.0.0.0 – 10.255.255.255
B	172.16.0.0 – 172.31.255.255
C	192.168.0.0 – 192.168.255.255

In either case, the administration of a private IP network must ensure that packets using such IP addresses are not transmitted to external networks, to prevent routing conflicts. GRE allows hosts in one private IP network to communicate with hosts in another private IP network by effectively providing a tunnel between two routers across an internet (Figure 22-2 on page 22-3).

In the example shown in Figure 22-2 on page 22-3, IP packets from the private IP network 2.2.2.0 destined for a host in the private IP network 4.4.4.0 are encapsulated by Router A and forwarded to Router B. Intermediate routers route the packets using addresses in the delivery protocol header. Router B extracts the original payload packet and routes it to the appropriate destination within network 4.4.4.0.

Figure 22-2: A typical scenario for GRE encapsulation of IP over IP.



Support for GRE

The router supports RFC 1702, which defines the encapsulation of IP packets over IP.

Each router that provides GRE encapsulation defines one or more GRE entities. An entity contains a list of one or more patterns specifying a source interface or a source IP address/mask (and optionally a destination IP address/mask), and a target IP address. An entity is created using the command:

```
ADD GRE=gre-number {INTERFACE=interface|SOURCE=ipadd
    [SMASK=ipadd] [DESTINATION=ipadd [DMASK=ipadd]]}
    TARGET=ipadd [ENTRY=entry-number]
```

The router supports both point-to-point and multi-point configurations. In a point-to-point configuration, two private networks are connected across the Internet via a single link, and the GRE entity can be defined using only the INTERFACE or SOURCE and SMASK parameters. Any IP packet received from the source interface, or from the source IP address (and mask) will be encapsulated using GRE and forwarded to the target IP address.

In a multi-point configuration, multiple private networks are connected across the Internet. Each private network has multiple links to other private networks, and the GRE entity must be defined using the SOURCE, SMASK, DESTINATION and DMASK parameters. Any IP packet received from the source IP address and mask, and destined for the destination IP address and mask, will be encapsulated using GRE and forwarded to the target IP address.

The router specified by the target address decapsulates the GRE packet and forwards the IP packet to its destination. IP packets which do not match any patterns in the GRE entity are treated as normal IP packets and processed accordingly.

A GRE entity can be modified using the command:

```
SET GRE=gre-number ENTRY=entry-number [{INTERFACE=interface|
   SOURCE=ipadd [SMASK=ipadd] [DESTINATION=ipadd
   [DMASK=ipadd]]}] [TARGET=ipadd]
```

A GRE entity can be deleted using the command:

```
DELETE GRE=gre-number ENTRY={entry-number|ALL}
```

A GRE entity must be associated with an IP interface using one of the commands:

```
ADD IP INTERFACE=interface IPADDRESS={ipadd|DHCP}
   [BROADCAST={0|1}] [DIRECTEDBROADCAST={YES|NO|ON|OFF}]
   [FILTER={0..99|NONE}] [FRAGMENT={YES|NO}] [GRE={0..100|
   NONE}] [MASK=ipadd] [METRIC=1..16] [MULTICAST={OFF|SEND|
   RECEIVE|BOTH|ON}] [OSPFMETRIC=1..65534]
   [POLICYFILTER={100..199|NONE}] [PRIORITYFILTER={200..299|
   NONE}] [PROXYARP={ON|OFF}] [RIPMETRIC=1..16]
   [SAMODE={BLOCK|PASSTHROUGH}] [VJC={ON|OFF}]
SET IP INTERFACE=interface [BROADCAST={0|1}]
   [DIRECTEDBROADCAST={YES|NO|ON|OFF}] [FILTER={0..99|NONE}]
   [FRAGMENT={YES|NO}] [GRE={0..100|NONE}] [IPADDRESS=ipadd|
   DHCP] [MASK=ipadd] [METRIC=1..16] [MULTICAST={OFF|SEND|
   RECEIVE|BOTH|ON}] [OSPFMETRIC=1..65534]
   [POLICYFILTER={100..199|NONE}] [PRIORITYFILTER={200..299|
   NONE}] [PROXYARP={ON|OFF}] [RIPMETRIC=1..16]
   [SAMODE={BLOCK|PASSTHROUGH}] [VJC={ON|OFF}]
```

before the entity becomes active. A GRE entity may be associated with one or more IP interfaces. However, each IP interface may be associated with only one GRE entity.

Any IP packets received via the IP interface are checked against the patterns in the GRE entity and if a match is found the IP packet is encapsulated using GRE and forwarded to the specified target address. At the target address, the router's GRE module extracts the payload packet and forwards it to the IP module for normal processing. If the packet does not match any pattern in the entity, then the packet is treated as an ordinary IP packet and processed as usual. The order in which the patterns are listed in a GRE entity is an important factor in the efficiency of the encapsulation process.

GRE encapsulation on a specific IP interface can be enabled, disabled or modified by setting the GRE entity to NONE or another entity number, using:

```
SET IP INTERFACE=interface GRE={0..100|NONE}
```

GRE encapsulation may be enabled or disable for all IP interfaces on the router using the commands:

```
ENABLE GRE
DISABLE GRE
```

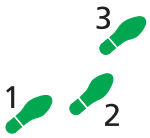
Configuration Examples

A Basic GRE Configuration

The following example illustrates the steps required to configure point-to-point GRE, based on the example configuration shown in Figure 22-2 on page 22-3. Table 22-2 on page 22-5 lists the parameter values that will be used in the example. This example assumes that IP has already been configured correctly and is operational on both routers.

Table 22-2: Example configuration parameters for point-to-point GRE.

Parameter	Router A	Router B
Private network IP address	2.2.2.0	4.4.4.0
Private network mask	255.255.255.0	255.255.255.0
Ethernet interface IP address	2.2.2.1	4.4.4.1
Local hosts gateway IP address	2.2.2.1	4.4.4.1
WAN interface IP address	172.31.5.1	172.31.5.2
Target IP address	172.31.5.2	172.31.5.1



To configure point-to-point GRE:

1. **Enable the GRE module.**

   The GRE module must be enabled on Router A and Router B, using the following command on each router:

   ```
   ENABLE GRE
   ```

2. **Create the GRE entity.**

   A GRE entity must be created on each router to specify which IP packets are to be encapsulated, and where to forward the encapsulated packets.

   On Router A, create a GRE entity to match all IP packets received from the private IP network 2.2.2.0 and forward them to Router B, using:

   ```
   ADD GRE=1 SOURCE=2.2.2.0 SMASK=255.255.255.0
       TARGET=172.31.5.2
   ```

   On Router B, create a GRE entity to match all IP packets received from the private IP network 4.4.4.0 and forward them to Router A, using:

   ```
   ADD GRE=1 SOURCE=4.4.4.0 SMASK=255.255.255.0
       TARGET=172.31.5.1
   ```

The IP addresses specified for the TARGET parameter must be valid, globally assigned public IP addresses.

3. Associate the GRE entity with an IP interface.

A GRE entity must be associated with an IP interface before it becomes active. In this example the GRE entity is associated with the router's Ethernet interface which is attached to the private IP network.

On Router A, associate the GRE entity with IP interface eth0, using:

```
ADD IP INTERFACE=ETH0 IP=2.2.2.1 GRE=1
```

On Router B, associate the GRE entity with IP interface eth0, using:

```
ADD IP INTERFACE=ETH0 IP=4.4.4.1 GRE=1
```

4. Assign the gateway for local hosts.

Local hosts in each private IP network must be configured to use the appropriate router as their gateway to the internet and the other private IP network. Hosts in private network 2.2.2.0 need to be configured to use Router A as their gateway, and specifically the router's eth0 interface which has the IP address 2.2.2.1. Hosts in private network 4.4.4.0 need to be configured to use Router B as their gateway, and specifically the router's eth0 interface which has the IP address 4.4.4.1.

The exact method depends on the particular TCP/IP software used on the hosts, but typically for TCP/IP software running on PCs, there will be a configuration file on the PC containing a line like:

```
gateway=2.2.2.1; for hosts in private network 2.2.2.0
gateway=4.4.4.1; for hosts in private network 4.4.4.0
```

Consult the documentation for the TCP/IP software used on the local hosts.

A Multi-point GRE Configuration

The following example illustrates the steps required to configure multi-point GRE, based on the example configuration shown in Figure 22-3 on page 22-7. Table 22-3 on page 22-7 lists the parameter values that will be used in the example. This example assumes that IP has not already been configured. IP will be enabled on each router and IP interfaces will be added for the local private IP network and the WAN link to the Internet.

Figure 22-3: Example configuration for multi-point GRE encapsulation of IP over IP.

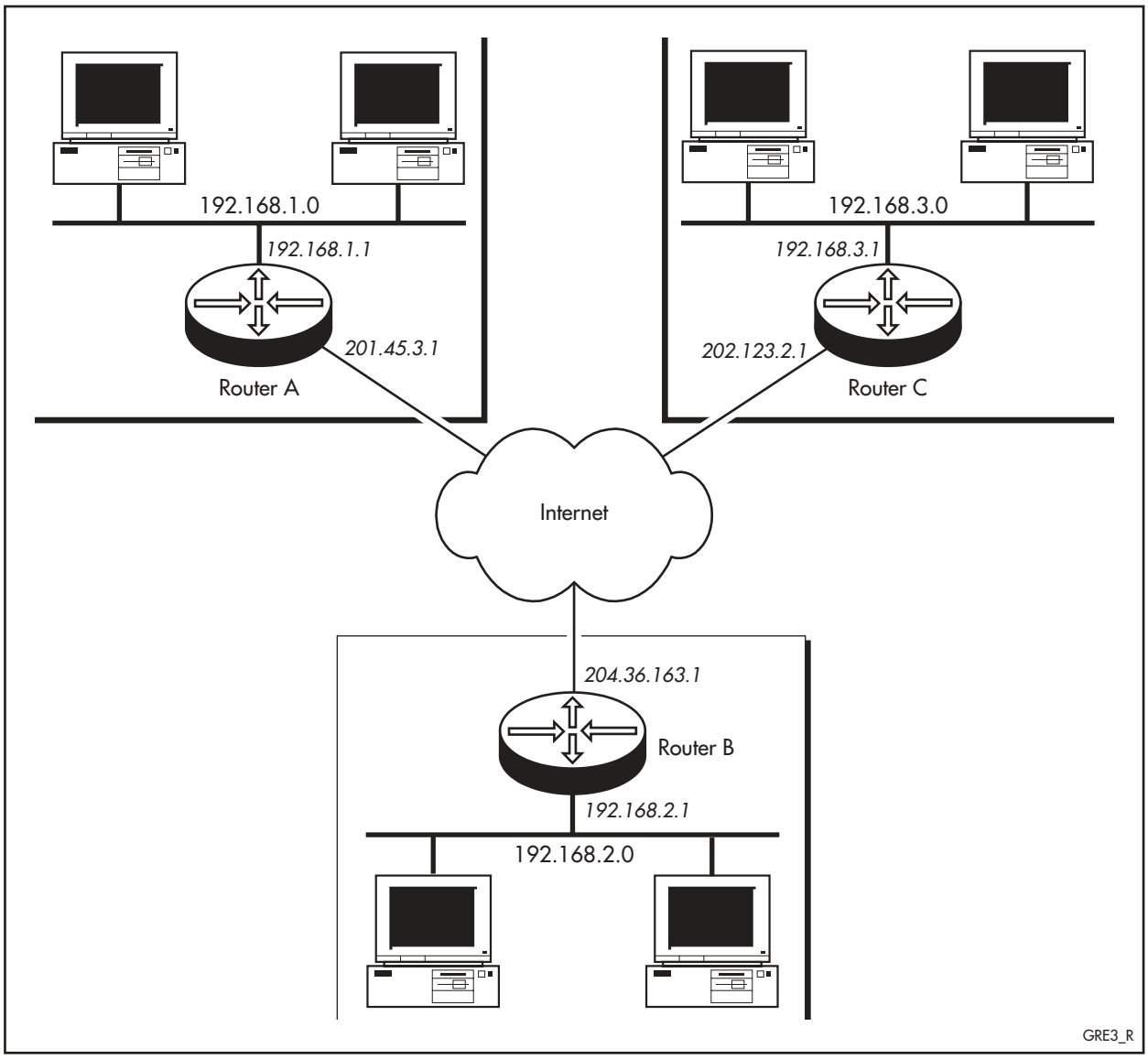
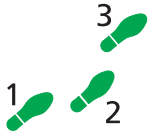


Table 22-3: Example configuration parameters for multi-point GRE.

Parameter	Router A	Router B	Router C
Private network IP address	192.168.1.0	192.168.2.0	192.168.3.0
Private network mask	255.255.255.0	255.255.255.0	255.255.255.0
Ethernet interface	eth0	eth0	eth0
Ethernet interface IP address	192.168.1.1	192.168.2.1	192.168.3.1
Local hosts gateway IP address	192.168.1.1	192.168.2.1	192.168.3.1
PPP interface	ppp0	ppp0	ppp0
PPP interface IP address	201.45.3.1	204.36.163.1	202.123.2.1
Target IP addresses	204.36.163.1, 202.123.2.1	201.45.3.1, 202.123.2.1	201.45.3.1, 204.36.163.1



To configure multi-point GRE:

1. Enable the GRE module.

The GRE module must be enabled on routers A, B and C, using the following command on each router:

```
ENABLE GRE
```

2. Create the GRE entity.

A GRE entity must be created on each router to specify which IP packets are to be encapsulated, and where to forward the encapsulated packets.

On Router A, create a GRE entity to match all IP packets from the local private IP network 192.168.1.0 and destined for the remote private IP network 192.168.2.0, and forward them to Router B. Add a second entry to the GRE entity to match all IP packets from the local private IP network 192.168.1.0 and destined for the remote private IP network 192.168.3.0, and forward them to Router C, using:

```
ADD GRE=1 SOU=192.168.1.0 SMASK=255.255.255.0
    DEST=192.168.2.0 DMASK=255.255.255.0
    TARGET=204.36.163.1
ADD GRE=1 SOU=192.168.1.0 SMASK=255.255.255.0
    DEST=192.168.3.0 DMASK=255.255.255.0
    TARGET=202.123.2.1
```

On Router B, create a GRE entity to match all IP packets from the local private IP network 192.168.2.0 and destined for the remote private IP network 192.168.1.0, and forward them to Router A. Add a second entry to the GRE entity to match all IP packets from the local private IP network 192.168.2.0 and destined for the remote private IP network 192.168.3.0, and forward them to Router C, using:

```
ADD GRE=1 SOU=192.168.2.0 SMASK=255.255.255.0
    DEST=192.168.1.0 DMASK=255.255.255.0 TARGET=201.45.3.1
ADD GRE=1 SOU=192.168.2.0 SMASK=255.255.255.0
    DEST=192.168.3.0 DMASK=255.255.255.0
    TARGET=202.123.2.1
```

On Router C, create a GRE entity to match all IP packets from the local private IP network 192.168.3.0 and destined for the remote private IP network 192.168.1.0, and forward them to Router A. Add a second entry to the GRE entity to match all IP packets from the local private IP network 192.168.3.0 and destined for the remote private IP network 192.168.2.0, and forward them to Router B, using:

```
ADD GRE=1 SOU=192.168.3.0 SMASK=255.255.255.0
    DEST=192.168.1.0 DMASK=255.255.255.0 TARGET=201.45.3.1
ADD GRE=1 SOU=192.168.3.0 SMASK=255.255.255.0
    DEST=192.168.2.0 DMASK=255.255.255.0
    TARGET=204.36.163.1
```

The IP addresses specified for the TARGET parameter must be valid, globally assigned public IP addresses.

3. Associate the GRE entity with an IP interface.

A GRE entity must be associated with an IP interface before it becomes active. Enable IP routing and add two IP interfaces, one for the Ethernet interface to which the local private IP network is attached, and one for the PPP connection to the Internet. Associate the GRE entity with the Ethernet interface.

On Router A, use the commands:

```
ENA IP
ADD IP INT=ETH0 IP=192.168.1.1 MASK=255.255.255.0 GRE=1
CREATE PPP=0 OVER=syn0
ADD IP INT=PPP0 IP=201.45.3.1
```

On Router B, use the commands:

```
ENA IP
ADD IP INT=ETH0 IP=192.168.2.1 MASK=255.255.255.0 GRE=1
CREATE PPP=0 OVER=syn0
ADD IP INT=PPP0 IP=204.36.163.1
```

On Router C, use the commands:

```
ENA IP
ADD IP INT=ETH0 IP=192.168.3.1 MASK=255.255.255.0 GRE=1
CREATE PPP=0 OVER=syn0
ADD IP INT=PPP0 IP=202.123.2.1
```

4. Assign the gateway for local hosts.

Local hosts in each private IP network must be configured to use the appropriate router as their gateway to the internet and the other private IP network. Hosts in private network 192.168.1.0 need to be configured to use Router A as their gateway, and specifically the router's eth0 interface which has the IP address 192.168.1.1. Hosts in private network 192.168.2.0 need to be configured to use Router B as their gateway, and specifically the router's eth0 interface which has the IP address 192.168.2.1.

The exact method depends on the particular TCP/IP software used on the hosts, but typically for TCP/IP software running on PCs, there will be a configuration file on the PC containing a line like:

```
gateway=192.168.1.1; for hosts in network 192.168.1.0
gateway=192.168.2.1; for hosts in network 192.168.2.0
gateway=192.168.3.1; for hosts in network 192.168.3.0
```

Consult the documentation for the TCP/IP software used on the local hosts.

Command Reference

This section describes the commands available on the router to configure and manage Generic Routing Encapsulation (GRE).

GRE requires the IP module to be enabled and configured correctly. See *Chapter 8, Internet Protocol (IP)* for detailed descriptions of the commands required to enable and configure IP.

See "*Conventions*" on page lxxx of *Preface* in the front of this manual for details of the conventions used to describe command syntax. See *Appendix A, Messages* for a complete list of error messages and their meanings.

ADD GRE

Syntax

```
ADD GRE=gre-number {INTERFACE=interface|SOURCE=ipadd
   [SMASK=ipadd] [DESTINATION=ipadd [DMASK=ipadd]]}
   TARGET=ipadd [ENTRY=entry-number]
```

where:

- *gre-number* is a decimal number in the range 0 to 99.
- *interface* is an interface name formed by concatenating an interface type and an interface instance (e.g. eth0).
- *ipadd* is an IP address in dotted decimal notation.
- *entry-number* is a non-zero decimal number.

Description

This command is used to add a pattern to a GRE entity in the encapsulation table. The exact pattern should not already exist in the GRE entity. The pattern comprises either an interface name or an IP source address and mask to match IP packets against, and a destination IP address for matching packets.

The GRE parameter specifies the number of the GRE entity to which the pattern is to be added.

The INTERFACE parameter specifies the name of an interface used by the IP module. All IP packets received via the interface will be encapsulated and forwarded using GRE. If INTERFACE is specified, SOURCE, SMASK, DESTINATION and DMASK may not be specified.

The SOURCE parameter specifies a source IP address in dotted decimal notation. IP packets originating from this IP address will be treated as IP packets from a private IP address and will be encapsulated. The SOURCE parameter can be used with the SMASK parameter to specify a range of IP addresses. The SOURCE and MASK parameters must be compatible. For each bit in SOURCE that is zero (0), the equivalent bit in MASK must also be zero (0). If INTERFACE is specified, SOURCE, SMASK, DESTINATION and DMASK may not be specified.

The SMASK parameter specifies the network mask, in dotted decimal notation, to be used with the source IP address specified by the SOURCE parameter. The SOURCE parameter can be used with the SMASK parameter to specify a range of IP addresses. The SOURCE and SMASK parameters must be compatible. For each bit in SOURCE that is zero (0), the equivalent bit in MASK must also be zero (0). If INTERFACE is specified, SOURCE, SMASK, DESTINATION and DMASK may not be specified.

The DESTINATION parameter specifies the destination IP address of the packet to be encapsulated, in dotted decimal notation. IP packets originating from the IP address specified by the SOURCE parameter *and* destined for this IP address will be treated as IP packets from a private IP address and will be encapsulated. The DESTINATION parameter can be used with the DMASK parameter to specify a range of IP addresses. The DESTINATION and DMASK parameters must be compatible. For each bit in DESTINATION that is zero (0), the equivalent bit in DMASK must also be zero (0). If INTERFACE is specified, SOURCE, SMASK, DESTINATION and DMASK may not be specified.

The DMASK parameter specifies the network mask, in dotted decimal notation, to be used with the destination IP address specified by the DESTINATION parameter to define a range of IP addresses. The DESTINATION and DMASK

parameters must be compatible. For each bit in DESTINATION that is zero (0), the equivalent bit in DMASK must also be zero (0). If INTERFACE is specified, SOURCE, SMASK, DESTINATION and DMASK may not be specified.

The TARGET parameter specifies the IP address dotted decimal notation of an interface on a destination router. The IP address must be a valid global (non-private) IP address. The encapsulated IP packets will be sent to this address.

The ENTRY parameter specifies the entry number in the GRE entity that this pattern will occupy. Existing patterns with the same or higher entry numbers will be pushed down the list. If the number is greater than the total number of patterns in the list, then this pattern will be added to the end of the list. The default is to add the pattern to the end of the list.

Examples To add a pattern to GRE entity 1 to encapsulate IP packets from hosts with IP addresses in the range 192.168.23.0 to 192.168.23.255 and forward them to the router with IP address 202.50.100.23, use:

```
ADD GRE=1 SOURCE=192.168.23.0 SMASK=255.255.255.0
   TARGET=202.50.100.23
```

See Also DELETE GRE
SET GRE
SHOW GRE

DELETE GRE

Syntax `DELETE GRE=`*`gre-number`* `ENTRY={`*`entry-number`*`|ALL}`

where:

- *gre-number* is a decimal number in the range 0 to 99.
- *entry-number* is a non-zero decimal number.

Description This command is used to delete a pattern or patterns from a GRE entity in the encapsulation table. The pattern must exist in the GRE entity.

The GRE parameter specifies the number of the GRE entity from which the pattern is to be deleted.

The ENTRY parameter specifies the entry number in the GRE entity to be deleted. If ALL is specified all patterns in the GRE entity are deleted. Existing patterns with the same or higher entry numbers will be pushed up the list to fill the vacant entry.

Examples To delete GRE entry number 3 from the GRE entity 1 pattern list, use:

```
DELETE GRE=1 ENTRY=3
```

See Also ADD GRE
SET GRE
SHOW GRE

DISABLE GRE

Syntax `DISABLE GRE`

Description This command disables GRE encapsulation on the router. GRE encapsulation must currently be enabled.

Examples To disable GRE module, use:

```
DISABLE GRE
```

See Also ENABLE GRE

ENABLE GRE

Syntax `ENABLE GRE`

Description This command enables GRE encapsulation on the router. GRE encapsulation must currently be disabled.

Examples To enable GRE module, use:

```
ENABLE GRE
```

See Also DISABLE GRE

PURGE GRE

Syntax `PURGE GRE`

Description This command resets GRE encapsulation on the router, and purges all GRE configurations and patterns in nonvolatile storage.

Examples To purge GRE module, use:

```
PURGE GRE
```

See Also RESET GRE

RESET GRE

Syntax `RESET GRE`

Description This command resets GRE encapsulation on the router. GRE encapsulation must currently be enabled. This has the same effect as entering the command sequence:

```
DISABLE GRE
ENABLE GRE
```

Examples To reset GRE module, use:

```
RESET GRE
```

See Also DISABLE GRE
ENABLE GRE

SET GRE

Syntax

```
SET GRE=gre-number ENTRY=entry-number
   [{INTERFACE=interface|SOURCE=ipadd [SMASK=ipadd]
   [DESTINATION=ipadd [DMASK=ipadd]]}] [TARGET=ipadd]
```

where:

- *gre-number* is a decimal number in the range 0 to 99.
- *interface* is an interface name formed by concatenating an interface type and an interface instance (e.g. eth0).
- *ipadd* is an IP address in dotted decimal notation.
- *entry-number* is a non-zero decimal number.

Description This command is used to modify a pattern in a GRE entity in the encapsulation table. The pattern must exist in the GRE entity. The pattern comprises either an interface name or an IP source address and mask to match IP packets against, and a destination IP address for matching packets.

The GRE parameter specifies the number of the GRE entity in which the pattern is to be changed.

The ENTRY parameter specifies the entry number in the GRE entity to be changed.

The INTERFACE parameter specifies the name of an interface used by the IP module. All IP packets received via the interface will be encapsulated and forwarded using GRE. If INTERFACE is specified, SOURCE, SMASK, DESTINATION and DMASK may not be specified.

The SOURCE parameter specifies a source IP address in dotted decimal notation. IP packets originating from this IP address will be treated as IP packets from a private IP address and will be encapsulated. The SOURCE parameter can be used with the SMASK parameter to specify a range of IP addresses. The SOURCE and MASK parameters must be compatible. For each

bit in SOURCE that is zero (0), the equivalent bit in MASK must also be zero (0). If INTERFACE is specified, SOURCE, SMASK, DESTINATION and DMASK may not be specified.

The SMASK parameter specifies the network mask, in dotted decimal notation, to be used with the source IP address specified by the SOURCE parameter to define a range of IP addresses. The SOURCE and SMASK parameters must be compatible. For each bit in SOURCE that is zero (0), the equivalent bit in MASK must also be zero (0). If INTERFACE is specified, SOURCE, SMASK, DESTINATION and DMASK may not be specified.

The DESTINATION parameter specifies the destination IP address of the packet to be encapsulated, in dotted decimal notation. IP packets originating from the IP address specified by the SOURCE parameter *and* destined for this IP address will be treated as IP packets from a private IP address and will be encapsulated. The DESTINATION parameter can be used with the DMASK parameter to specify a range of IP addresses. The DESTINATION and DMASK parameters must be compatible. For each bit in DESTINATION that is zero (0), the equivalent bit in DMASK must also be zero (0). If INTERFACE is specified, SOURCE, SMASK, DESTINATION and DMASK may not be specified.

The DMASK parameter specifies the network mask, in dotted decimal notation, to be used with the destination IP address specified by the DESTINATION parameter to define a range of IP addresses. The DESTINATION and DMASK parameters must be compatible. For each bit in DESTINATION that is zero (0), the equivalent bit in DMASK must also be zero (0). If INTERFACE is specified, SOURCE, SMASK, DESTINATION and DMASK may not be specified.

The TARGET parameter specifies the IP address dotted decimal notation of an interface on a destination router. The IP address must be a valid global (non-private) IP address. The encapsulated IP packets will be sent to this address.

Examples To modify entry 3 in GRE entity 1 to use a target of 192.168.163.45, use:

```
SET GRE=1 ENTRY=3 TARGET=192.168.163.45
```

See Also DELETE GRE
SET GRE
SHOW GRE

SHOW GRE

Syntax `SHOW GRE[=`*`gre-number`*`] [GENERAL]`

where:

- *gre-number* is a decimal number in the range 0 to 99.

Description This command displays the pattern list of a GRE entity, or general configuration information for GRE.

The GRE parameter specifies the number of the GRE entity to be displayed. If a GRE entity is not specified, all GRE entities are displayed (Figure 22-4 on page 22-15, Table 22-4 on page 22-15).

If GENERAL is specified, general configuration information is displayed. The GRE entity number may not be specified (Figure 22-5 on page 22-15, Table 22-5 on page 22-15).

Figure 22-4: Example output from the SHOW GRE command.

```
-------------------------------------------------------------------------
GRE   Entry   Interface   Source           Destination      Target
                          Source Mask      Dest. Mask       Match
-------------------------------------------------------------------------
  1     1     -           192.168.1.0      192.168.10.0     202.36.163.5
                          255.255.255.0    255.255.255.0            0
        2     -           192.168.2.0      192.168.8.0      202.36.137.21
                          255.255.255.0    255.255.255.0            0

          Requests:          0           Translations:          0
-------------------------------------------------------------------------
```

Table 22-4: Parameters displayed in the output of the SHOW GRE command.

Parameter	Meaning
GRE	The GRE entity number.
Entry	The entry number for this pattern in the GRE entity.
Interface	The interface name for this pattern, or "-".
Source	The source IP address of the packet for this pattern, or "-".
Source Mask	The source network mask for this pattern, or "-".
Destination	The destination IP address of the packet for this pattern, or "-".
Dest. Mask	The destination network mask for this pattern, or "-".
Target	The target (router interface) IP address for this pattern.
Match	The number of IP packets processed that matched this pattern.
Requests	The number of IP packets checked against this GRE entity.
Translations	The number of IP packets processed that matched a pattern in this entity and were encapsulated by GRE.

Figure 22-5: Example output from the SHOW GRE GENERAL command.

```
GRE General Information
-----------------------
Status ..................... Enabled
greInPkts ..................          0
```

Table 22-5: Parameters displayed in the output of the SHOW GRE GENERAL command.

Parameter	Meaning
Status	The status of GRE; one of "Enabled" or "Disabled".
greInPkts	The number of GRE-encapsulated packets received by this router and forwarded to a private network.

Examples To show the pattern list for GRE entity 1, use:

```
SHOW GRE=1
```

See Also ADD GRE
DELETE GRE