Network Working Group
Internet Draft
Category
draft-meyer-gre-update-00.txt

David Meyer
Cisco Systems
Standards Track
November, 1999

Generic Routing Encapsulation (GRE)
<draft-meyer-gre-update-00.txt>

1. Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC 2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet- Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

2. Abstract

This document specifies a protocol for performing encapsulation of an arbitrary network layer protocol over another arbitrary network layer protocol.

3. Copyright Notice

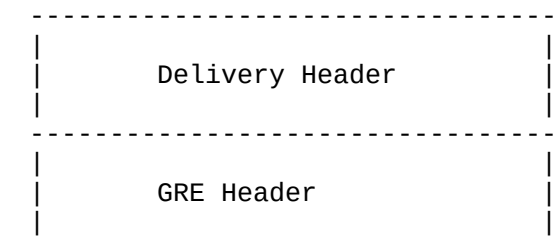
4. Introduction

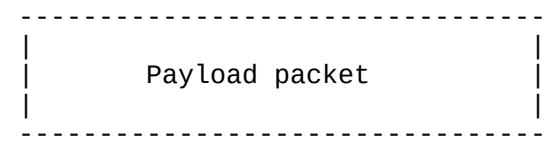
A number of different proposals [RFC1234, RFC1226] currently exist for the encapsulation of one protocol over another protocol. Other types of encapsulations [RFC1241, SDRP, RFC1479] have been proposed for transporting IP over IP for policy purposes. This memo describes a protocol which is very similar to, but is more general than, the above proposals. In attempting to be more general, many protocol specific nuances have been ignored. The result is that this proposal is may be less suitable for a situation where a specific "X over Y" encapsulation has been described. It is the attempt of this protocol to provide a simple, general purpose mechanism which is reduces the problem of encapsulation from its current O(n^2) problem to a more manageable state. This proposal also attempts to provide a lightweight encapsulation for use in policy based routing. This memo explicitly does not address the issue of when a packet should be encapsulated. This memo acknowledges, but does not address problems with other encapsuations such as mutual encapsulation [RFC1326] or MPLS [MPLS].

In the most general case, a system has a packet that needs to be encapsulated and delivered to some destination. We will call this the payload packet. The payload is first encapsulated in a GRE packet, which possibly also includes a route. The resulting GRE packet can then be encapsulated in some other protocol and then forwarded. We will call this outer protocol the delivery protocol. The algorithms or processing this packet are discussed later.

4.1. Overall packet

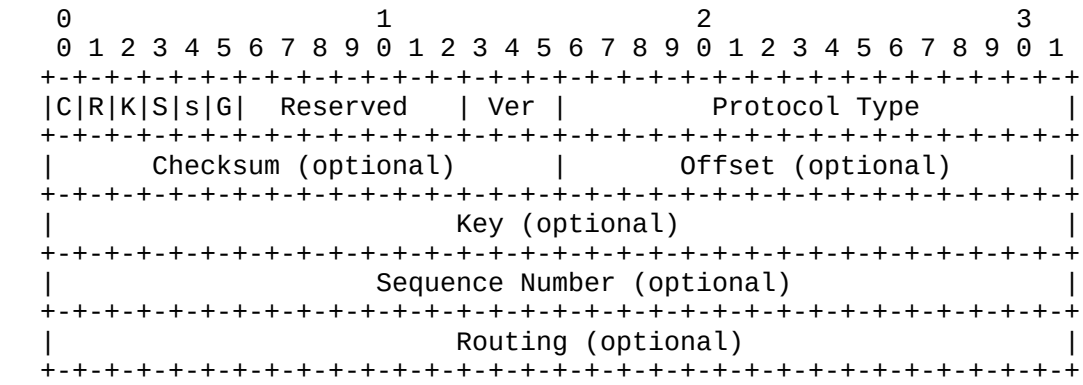
The entire encapsulated packet would then have the form:





4.2. Packet header

The GRE packet header has the form:



Note that a compliant implemenation MUST accept and process optional fields.

4.3. Flags and version (2 octets)

The GRE flags are encoded in the first two octets. Bit 0 is the most significant bit, bit 15 is the least significant bit. Bits 13 through 15 are reserved for the Version field. Bits 6 through 12 are reserved for future use and MUST be transmitted as zero.

4.4. Checksum Present (bit 0)

If the Checksum Present bit is set to 1, then the Checksum field is present and contains valid information.

If either the Checksum Present bit or the Routing Present bit are set, BOTH the Checksum and Offset fields are present in the GRE packet.

4.5. Routing Present (bit 1)

If the Routing Present bit is set to 1, then it indicates that the Offset and Routing fields are present and contain valid information.

If either the Checksum Present bit or the Routing Present bit are set, BOTH the Checksum and Offset fields are present in the GRE packet.

4.6. Key Present (bit 2)

If the Key Present bit is set to 1, then it indicates that the Key field is present in the GRE header. Otherwise, the Key field is not present in the GRE header. In general, the key is used to match packets that come over a point to multipoint tunnel.

4.7. Sequence Number Present (bit 3)

If the Sequence Number Present bit is set to one, then it indicates that the Sequence Number field is present. Otherwise, the Sequence Number field is not present in the GRE header. The Sequence Number is used to enforce packet ordering on the tunnel.

4.8. Strict Source Route (bit 4)

The meaning of the Strict Source route bit is defined in other documents. It is recommended that this bit only be set to one if all of the the Routing Information consists of Strict Source Routes.

4.9. Generic Routing Field (bit 5)

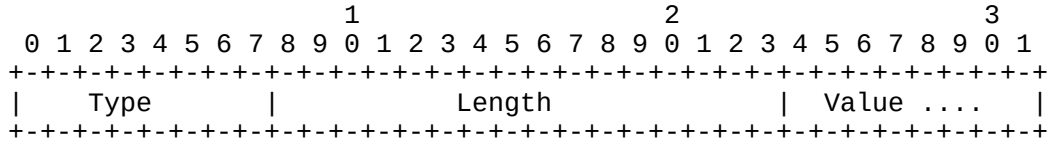
The Generic Routing Field is provided to generalize the Routing Field to provide additional flexibiity for future use. If the Generic Routing Field (G-bit) bit is set to one, then the Routing Field is encoded as a sequence of TLVs. The sequence of TLVs is terminated by a TLV with type 0x0000 and length 4. If an implemenation does not understand a TLV in the range 0-127, the TLV SHOULD be ignored. If an implemenation does not understand a TLV in the range 128-255, the packet MUST be dropped.

Since the Routing field is used when either the R-bit or the G-bit is

set, the R-bit takes precedence. That is if both bits are set, the Routing field is used in accordance to section 4.5.

The idea behind the G-bit is that when you have the G-bit set and the R-bit is not set, you escape from format specified in section 4.17. This provides some degree of backward compatability.

4.9.1. GRE TLV Format



Type (8 bits)
Describes the format of the Value field.

Length (16 bits)
Length of Type, Length, and Value fields in octets. Minimum length required is 3 octets, except in the case of the NULL TLV, which has length 4.

Value (variable length)
Format is based on the Type value. The length of the value field is Length field minus 3.

With the exception of the NULL TLV (Type 0x00 and and Length 4), this document does not define or document any TLVs for use with GRE.

4.10. Reserved (bits 6-12)

These bits are reserved for future use and MUST contain the value zero.

4.11. Version Number (bits 13-15)

The Version Number field MUST contain the value zero.

4.12. Protocol Type (2 octets)

The Protocol Type field contains the protocol type of the payload packet. In general, the value will be the Ethernet protocol type field for the packet. Currently defined protocol types are listed below [ETYPES].

4.13. Offset (2 octets)

The offset field indicates the octet offset from the start of the Routing field to the first octet of the active Source Route Entry to be examined. This field is present if the Routing Present or the Checksum Present bit is set to one, and contains valid information only if the Routing Present bit is set to one. If the R-bit is not set, this field should be set to zero.

4.14. Checksum (2 octets)

The Checksum field contains the IP (one's complement) checksum of the GRE header and the payload packet. This field is present if the Routing Present bit, the Checksum Present bit, or the Generic Routing Field bit are set to one, and contains valid information only if the Checksum Present bit is set to one.

4.15. Key (4 octets)

The Key field contains a four octet number which was inserted by the encapsulator. It is used to identify a security association and its associated keying information for the purposes of authenticating the source of the packet. The Key field is only present if the Key Present field is set to one.

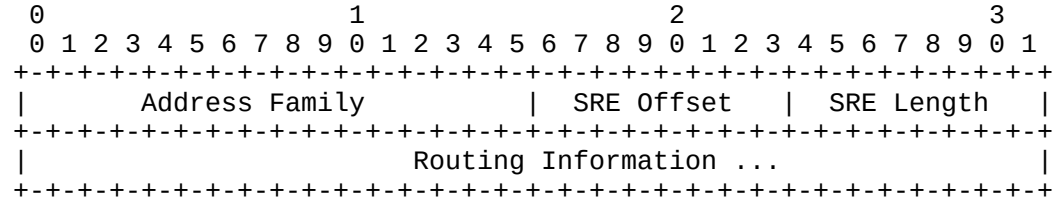
4.16. Sequence Number (4 octets)

The Sequence Number field contains an unsigned 32 bit integer which is inserted by the encapsulator. It may be used by the receiver to establish the order in which packets have been transmitted from the encapsulator to the receiver. It is not necessary to specify an exact algorithm other than to say that both sides should use montonically increasing sequence numbers.

4.17. Routing (variable)

The Routing field is optional and is present only if the Routing Present bit is set to one (note that the Generic Routing Field bit may also be set. However, the Routing field is interpreted in the same way if set, independent of value of the Generic Routing Field).

The Routing field is a list of Source Route Entries (SREs). Each SRE has the form:



The routing field is terminated with a "NULL" SRE containing an address family of type 0x0000 and a length of 0.

4.18. Address Family (2 octets)

Type is a two octet field that encodes an RFC1700 [RFC1700] address family.

4.19. SRE Offset (1 octet)

The SRE Offset field indicates the octet offset from the start of the Routing Information field to the first octet of the active entry in Source Route Entry to be examined.

4.20. SRE Length (1 octet)

The SRE Length field contains the number of octets in the SRE. If the SRE Length is zero, this indicates this is the last SRE in the Routing field.

4.21. Routing Information (variable)

The Routing Information field contains data which may be used in routing this packet. If the R-bit is set, the packet is processed as follows:

```
 if (RBIT(GREPAK) {                                  /* R-Bit present? */
   SRE = GETSRE(GREPAK);
   if (LENGTH(SRE) == 0)                             /* packet is for us */
     PROCESS_GREPAK(GREPAK);
   } else {
      switch (ADDRESS_FAMILY(SRE)) {
        case GRE_PROTO_TYPE_X:                       /* Processing for AF = <X> *
/
          DATA = GRESREDATA(SRE);
          AJUST_SRE_OFFSET(SRE);                     /* process next element */
          if (OFFSET(SRE) == LENGTH(SRE))            /* done with this SRE */
            AJUST_GRE_OFFSET(GREPAK);                /* get next SRE */
          SOURCE = IPADDRESS(GREPAK);
          DEST   = DATA;
          AF_SENDGREPACKET(GREPAK, SOURCE, DEST); /* Per AF forward the packet
 */
          RETURN;
      }
   }
```

Note that RFC1702 [RFC1702] describes GRE operation over IPv4 networks.

5. Forwarding of GRE packets

Normally, a system which is forwarding delivery layer packets will not differentiate GRE packets from other packets in any way. However, a GRE packet may be received by a system. In this case, the system should use some delivery-specific means to determine that this is a GRE packet. Once this is determined, the Key, Sequence Number and Checksum fields if they contain valid information as indicated by the corresponding flags may be checked. If the Routing Present bit is set to one, then the Address Family field should be checked to determine the semantics and use of the SRE Length, SRE Offset and Routing Information fields. The exact semantics for processing a SRE is dependent on the Address Family. However, for the IPv4 address family, see the psuedo-code above.

Once all SREs have been processed, then the source route is complete, the GRE header should be removed, the payload's TTL MUST be decremented (if one exists) and the payload packet should be

forwarded as a normal packet.

6. Current List of Protocol Types

The following are currently assigned protocol types for GRE. Future protocol types must be taken from DIX ethernet encoding. For historical reasons, a number of other values have been used for some protocols. The following table of values MUST be used to identify the following protocols:

Protocol Family	PTYPE
Reserved	0000
SNA	0004
OSI network layer	00FE
PUP	0200
XNS	0600
IP	0800
Chaos	0804
RFC 826 ARP	0806
Frame Relay ARP	0808
VINES	0BAD
VINES Echo	0BAE
VINES Loopback	0BAF
DECnet (Phase IV)	6003
Transparent Ethernet Bridging	6558
Raw Frame Relay	6559
Apollo Domain	8019
Ethertalk (Appletalk)	809B
Novell IPX	8137
RFC 1144 TCP/IP compression	876B
IP Autonomous Systems	876C
Secure Data	876D
Reserved	FFFF

See [ETYPES] for the complete list of these values.

7. Security Considerations

Security in a network using GRE should be relatively similar to security in a normal IP network, as routing using GRE follows the same routing that IP uses natively. Route filtering will remain unchanged. However packet filtering requires either that a firewall look inside the GRE packet or that the filtering is done on the GRE tunnel endpoints. In those environments in which this is considered to be a security issue it may be desirable to terminate the tunnel to the firewall.

8. Acknowledgements

This document is derrived from the original ideas of the authors of RFC1701 and RFC1702. Bill Fenner, Thomas Narten, and Dino Farinacci provided constructive and insightful comments.

9. References

[ETYPES] ftp://ftp.isi.edu/in-notes/iana/assignments/ethernet-numbers

[MPLS] Rosen, Eric, et. al, "Multiprotocol Label Switching Architecture", draft-ietf-mpls-arch-06.txt, August, 1999.

[RFC1479] Steenstrup, M. "Inter-Domain Policy Routing Protocol Specification: Version 1", RFC1479, BBN Systems and Technologies, July 1993.

[RFC1226] Kantor, B. "Internet Protocol Encapsulation of AX.25 Frames", RFC1226, University of California, San Diego, May 1991.

[RFC1234] Provan, D. "Tunneling IPX Traffic through IP Networks", RFC1234, Novell, Inc., June 1991.

[RFC1241] Woodburn, R., and D. Mills, "Scheme for an Internet Encapsulation Protocol: Version 1", RFC1241, SAIC, University of Delaware, July 1991.

[RFC1326] Tsuchiya, P., "Mutual Encapsulation Considered Dangerous", RFC1326, Bellcore, May 1992.

[RFC1700] J. Reynolds and J. Postel, "Assigned Numbers", RFC1700, October 1994.

[RFC1701] Hanks, S., Li, T, Farinacci, D., and P. Traina, "Generic Routing Encapsulation", RFC1701, NetSmiths, Ltd., and cisco Systems, October 1994.

[RFC1702] Hanks, S., Li, T., Farinacci, D., and P. Traina, "Generic Routing Encapsulation over IPv4 networks", RFC1702, NetSmiths, Ltd., cisco Systems, October 1994.

[SDRP] Estrin, D., Li, T., and Y. Rekhter, "Source Demand Routing Protocol Specification (Version 1)", Work in Progress.

10. Authors' Addresses

David Meyer
Cisco Systems, Inc.
170 W. Tasman Drive
San Jose, CA 95134-1706
United States
EMail: dmm@cisco.com