Network Working Group
Request for Comments: 3147
Category: Informational

P. Christian
Nortel Networks

July 2001

Generic Routing Encapsulation over CLNS Networks

Status of this Memo

Copyright Notice

Abstract

This document proposes a method for transporting an arbitrary protocol over a CLNS (Connectionless Network Service) network using GRE (Generic Routing Encapsulation). This may then be used as a method to tunnel IPv4 or IPv6 over CLNS.

1. Introduction

RFC 2784 Generic Routing Encapsulation (GRE) [1] provides a standard method for transporting one arbitrary network layer protocol over another arbitrary network layer protocol.

RFC 1702 Generic Routing Encapsulation over IPv4 networks [2] provides a standard method for transporting an arbitrary network layer protocol over IPv4 using GRE.

However no standard method exists for transporting other network layer protocols over CLNS. This causes lack of interoperability between different vendors' products as they provide solutions to migrate from CLNS networks to IP networks. This is a problem specifically in, but not limited to, the context of management networks for SONET and SDH networks elements.

Large networks exist for the purpose of providing management communications for SONET and SDH network elements. Standards Bellcore GR-253-CORE [3] and ITU-T G.784 [4] mandate that these networks are based on CLNS.

Many vendors have already started to offer SONET and SDH products that are managed by IP instead of CLNS and a general migration from CLNS towards IP is anticipated within the industry.

Part of any migration strategy from CLNS to IP should provide for the co-existence of both CLNS managed and IP managed network elements in the same network.

Such a migration strategy should foresee the need to manage existing CLNS managed network elements that become isolated by a new IP network. Such a scenario may be tackled by tunnelling CLNP PDUs over IP using the existing GRE standard RFC 2784 [1] and informational RFC 1702 [2]. Networks have already been deployed that use this method.

Such a migration strategy should also foresee the need to manage new IP managed network elements that are installed on the far side of existing CLNS managed network. Such a scenario requires a method for tunnelling IP over CLNS.

2. GRE over CLNS advantages

Using GRE to tunnel IP over CLNS offers some advantages.

In the absence of a standard for tunnelling IP over CLNS, GRE as specified in RFC 2784 [1] is the most applicable standard that exists.

The move from CLNS to IP comes at a time when IP is itself migrating from IPv4 to IPv6. GRE defines a method to tunnel any protocol that has an Ethernet Protocol Type. Therefore by defining a method for CLNS to transport GRE, a method will then exist for CLNS to transport any other protocol that has an Ethernet Protocol Type defined in RFC 1700 [5]. Thus GRE over CLNS can be used to tunnel both IPv4 and IPv6.

GRE is already commonly used to tunnel CLNP PDUs over IP and so using GRE to tunnel IP over CLNS gives a common approach to tunnelling and may simplify software within network elements that initiate and terminate tunnels.

The only disadvantage of using GRE is the extra minimum of four bytes that will be used between CLNP header and IP payload packet. Given the large size of CLNP headers this will not make a significant difference to the performance of any network that has IP over CLNP PDUs present on it.

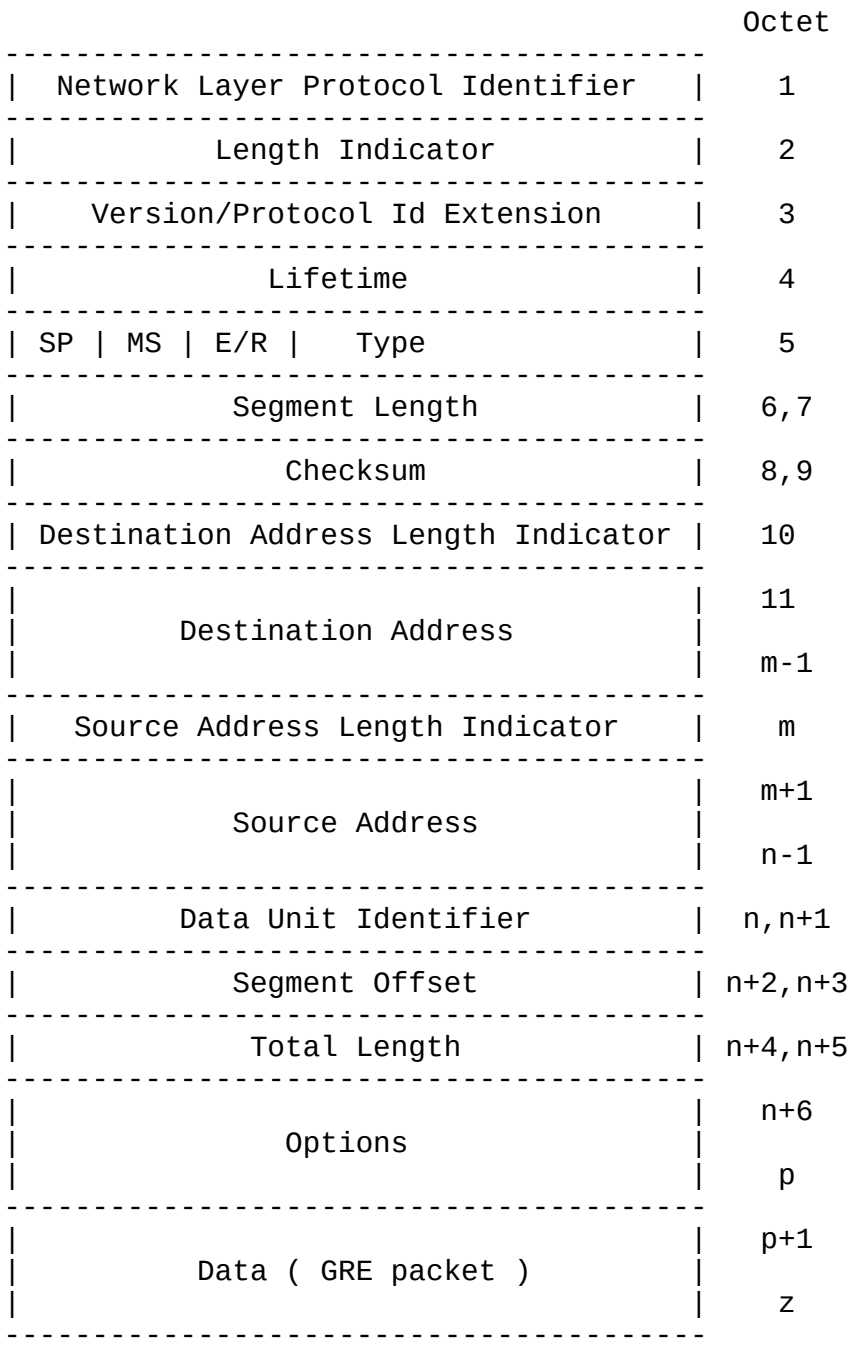
3. Transporting GRE packets over CLNS.

It is suggested that GRE should be transported over CLNS at the lowest layer possible, which is as a transport layer protocol over the network layer. This can be achieved by placing the entire GRE packet inside a CLNP Data Type PDU (DT PDU) as data payload.

The GRE packet is a GRE packet as defined in RFC 2784 [1], in other words GRE header plus payload packet.

Data payload is the part of a Data PDU that is described as "Data" in the structure of a Data PDU in ISO/IEC 8473-1 [6].

For convenience the structure of a Data PDU is reproduced from ISO/IEC 8473-1 [6] below:



4. NSAP selector (N-SEL) value.

   Transport of GRE packets is a new type of Network Service (NS) user. Different Network Service users are identified by using different NSAP selector bytes also known as N-SEL bytes.

   This is a similar concept to the use of the IP Protocol Type used in IP packets.

   Whilst it is not strictly necessary for all vendors to use the same N-SEL values, they must use the same N-SEL value for it to be possible for one vendor's CLNS device or network element to initiate a GRE tunnel which is then terminated on a different vendor's CLNS device.

   Although N-SEL values (other than zero) are not defined in CLNS/CLNP standards, some are defined when CLNS is used in SONET networks by Bellcore GR-253-CORE [3] whilst others are in common use.

   As the IP protocol number for GRE is 47, as defined in RFC 1702 [2], and as 47 is not commonly used as an N-SEL value, it is suggested that 47 (decimal) should be used as an N-SEL value to indicate to the CLNS stack that the Data portion of the Data Type PDU contains a GRE packet.

   The N-SEL byte should be set to 47 (decimal) in both the source address and the destination address of the CLNP PDU.

   The N-SEL value of 47 should indicate only that the payload is GRE, and the device or network element that transmits the PDU should use the GRE header to indicate what protocol (for example IPv4 or IPv6) is encapsulated within the GRE packet in conformance with RFC 2784 [1]. Similarly the device or network element that receives the PDU should then inspect the GRE header to ascertain what protocol is contained within the GRE packet in conformance with RFC 2784 [1].

5. Segmentation Permitted (SP) value.

   It is recommended that the SP flag in all CLNP PDUs containing GRE packets should be set.

   If the SP flag is not set, and a CLNP PDU is too large for a particular link, then a CLNS device or network element will drop the PDU. The originator of the packet that is inside the GRE packet will not have visibility of the packet loss or the reason for the packet loss, and a black hole may form.

6. Interaction with Path MTU Discovery (PMTU), RFC 1191 [7].

A tunnel entry point for a GRE tunnel should treat IP packets that are bigger than the MTU size of the GRE tunnel as per RFC 1191 [7]. If the oversize IP packet that is about to enter the GRE tunnel does not have its Don't Fragment (DF) bit set then it should be fragmented before entering the tunnel.

If the oversize IP packet that is about to enter the GRE tunnel has its DF bit set then the packet should be discarded, and an ICMP unreachable error message (in particular the "fragmentation needed and DF set" code) should be sent back to the originator of the packet as described in RFC 1191 [7].

7. Security Considerations

CLNS and GRE do not provide any security when employed in the way recommended in this document.

If security is required, then it must be provided by other methods and applied to the payload protocol before it is transported by GRE over CLNS.

8. References

[1] Farinacci, D., Li, T., Hanks, S., Meyer, D. and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 2784, March 2000.

[2] Hanks, S., Li, T., Farinacci, D. and P. Traina, "Generic Routing Encapsulation over IPv4", RFC 1702, October 1994.

[3] Bellcore Publication GR-253-Core "Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria", January 1999

[4] ITU-T Recommendation G.784 "Synchronous Digital Hierarchy (SDH) management", June 1999

[5] Reynolds, J. and J. Postel, "Assigned Numbers", STD 2, RFC 1700, October 1994.

[6] "Information technology - Protocol for providing the connectionless-mode network service", ISO/IEC 8473-1, 1994

[7] Mogul, J. and S. Deering, "Path MTU Discovery", RFC 1191, November 1990.

9. Acknowledgements

Chris Murton, Paul Fee, Mike Tate for their contribution in writing this document.

10. Author's Address

Philip Christian
Nortel Networks Harlow Laboratories
London Road, Harlow,
Essex, CM17 9NA UK

EMail: christi@nortelnetworks.com

11. Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.