Tunneling the OSI Network Layer over IP (EON)

Status of this Memo

This document is an Internet Draft. 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. Internet Drafts may be updated, replaced, or obsoleted by other documents at any time. It is not appropriate to use Internet Drafts as reference material or to cite them other than as a "working draft" or "work in progress."

Please check the I-D abstract listing contained in each Internet Draft directory to learn the current status of this or any Internet Draft.

Abstract

This memo documents the subset of the Experimental OSI Net (EON) [1] that is in active use today. It serves to document current practice, which deviates somewhat from the usage described in the original RFC.

Potential implementors should note that the protocol described herein is archaic and is likely to be replaced in the near future.

1. Introduction

RFC 1070 [1] describes a scheme for experimenting with OSI Network Layer protocols over an IP backbone. The memo describes methods for mapping aspects of subnetwork operation (such as multicast and broadcast) and an NSAP address allocation and mapping scheme, as well as a packet encapsulation format.

In the time since the EON RFC was published, three independent implementations have been fielded and are currently deployed in production use. These implementations use a small subset of the functionality described in the original memo.

2. Functionality

The EON protocol as implemented and fielded is simply a virtual point-to-point encapsulation technology, using statically configured tunnel endpoints. There is no support for simulating a multipoint subnetwork, nor for dynamic mapping between NSAP addresses and IP addresses. Instead, IP addresses are simply viewed as Subnetwork Point of Attachment (SNPA) addresses that must be statically configured to create the tunnel.

Once a tunnel is established, data is transmitted using CLNP [2].
The ES-IS [3], IS-IS [4], and IDRP [5] protocols may be used to dynamically establish neighbor adjacencies and routing. Any NSAP addresses may be assigned to the systems at either end of the tunnel. There is no need to constrain the NSAP address format as documented in RFC 1070, since there is no need to perform dynamic address mapping.

3. Encapsulation

Only the direct IP encapsulation described in RFC 1070 is used. Within that encapsulation, only the unicast format is used. This results in a constant header value (after calculating the checksum). To summarize, the encapsulation is as follows:

- IP header (protocol = 80 decimal)
- EON header (value = hexadecimal 01 00 FC 02)
- OSI Network Layer packet

4. Errors on the IP subnetwork

No attempt has been made to implement feedback of error indications from ICMP in the IP subnetwork into CLNP error PDUs. The tunnel is ignorant of problems in the IP subnetwork, and depends upon mechanisms in the OSI routing protocols to detect connectivity failures.

References


Author’s Address

Dave Katz
cisco Systems, Inc.
1525 O’Brien Dr.
Menlo Park, CA 94025
+1 (415) 688-8284
EMail: dkatz@cisco.com