INTERNET-DRAFT
Intended status: Experimental

W A Simpson
DayDreamer

8 August 2011

Generation of Unique IS-IS System Identifiers
draft-simpson-isis-ppp-unique-02

Abstract

The IS-IS routing protocol (Intermediate System to Intermediate System, ISO 10589) requires unique System Identifiers at the link layer. A common practice has been to use an existing IEEE 802 MAC link-layer interface identifier. When no unique MAC is available, this document specifies automatic generation of identifiers. It is fully interoperable with systems that do not support this extension.

Additionally, the extension automatically resolves conflicts between System Identifiers.

Status of this Memo

Table of Contents

1. Introduction

The System Identifier is 6 octets for OSI end systems, and 7 octets for IS-IS routers or pseudonodes. This identifier is not required to be the Destination or Source of any packet. (See [ISO10589], [RFC1195], and [RFC5342] for further details.)

Typically, IS-IS implementations base the identifier on an existing Media Access Control (MAC) link-layer interface identifier. The 48-bit MAC is usually composed of a 24-bit Organizationally Unique Identifier (OUI) followed by a 24-bit Network Interface Controller (NIC) specific number.

Other systems have a configured identifier that is independent of the interfaces.

When no unique MAC is available, this document specifies automatic generation of identifiers. In the presence of PPP [RFC1661] links, the PPP Magic Number is unique with respect to its neighbors and further reduces the potential for conflict.

This mechanism is also necessary to resolve conflicts between multiple systems with the same System Identifier due to manufacturing or misconfiguration.

1.1. Terminology

The key words "MAY", "MUST, "MUST NOT", "OPTIONAL", "RECOMMENDED", "REQUIRED", "SHOULD", and "SHOULD NOT" in this document are to be interpreted as described in [RFC2119].

2. Random Generation

Some systems have only point-to-point or other links without any conveniently available MAC, and do not have a configured identifier. This status might change dynamically, as hot swap interfaces are added or removed.

In this case, a 48-bit System Identifier MUST be randomly generated. (See [RFC4086] for requirements.)

To mitigate against potential assignment conflicts, this System Identifier (considered as a pseudo-MAC) MUST have both the "locally-assigned" and "broadcast/multicast" (group) bits set; that is, the least significant two bits of the most significant octet are equal to 0x3.

The probability of conflict between these identifiers is of the order (N**2)/(2**47); where N is the number of systems in the same IS-IS area. This is considerably less likely than a duplicate MAC (see below).

2.1. PPP Links

PPP [RFC1661] links (such as [RFC1377]) already specify negotiation of a randomly generated unique 32-bit Magic Number "to detect looped-back links and other Data Link Layer anomalies." Although only a single interface negotiation is described in the main document, it has long been understood [RFC1220] [Simpson1992] [Baker1992] that the term "unique" applies across all local system interfaces. This protects against patch-panel errors in addition to looped-back modems, to detect unexpected loopbacks of a link from an endpoint to itself. [Simpson1993] [RFC1663] [RFC1717]

An implementation conforming with this specification MUST have different Magic Numbers for every link in a single system, and each end of every link between two peers MUST have Magic Numbers which are unique to those peers. That is, the Magic Number MUST be unique for all visible interfaces.

Whenever such a Magic Number has been successfully negotiated, only the most significant 2 octets of a pseudo-OUI are randomly generated, followed by (concatenated to) the selected Magic Number.

To mitigate against potential assignment conflicts, this System Identifier (considered as a pseudo-OUI) MUST have both the "locally-assigned" and "broadcast/multicast" (group) bits set; that is, the least significant two bits of the most significant octet are equal to

0x3.

The probability of conflict is considerably less than the wholly generated pseudo-MAC (above), as the Magic Number has already been determined to be locally unique. The pseudo-OUI differentiates among PPP systems in the same IS-IS area.

3. Resolving Conflicts

As multiple systems generate System Identifiers, they might not have sufficiently divergent random bits available (especially on startup). Resolving conflicts is REQUIRED.

Field experience has shown that IEEE 802 MAC identifiers are frequently not unique. Reuse is more likely to recycle a block varying only the least significant bits, increasing the probability considerably over a normal distribution.

A MAC is most often reused by companies that have defective manufacturing processes, or manufacture more than 2**24 (16,777,214) devices. Many companies reuse the same MAC for different product lines, or different speeds or types of media. Some implementations failed to correctly convert the MAC to canonical form [RFC2469], causing unintentional conflicts through multi-media bridges.

If a duplicated MAC is used as a System Identifier within an IS-IS area, this leads to the condition colloquially called "LSP War" or "LSR War". The Update Process will increment its LSP sequence number repeatedly. Currently, IS-IS has no method to autonomously resolve conflicts.

An implementation conforming with this specification MUST generate a replacement System Identifier using one of the techniques specified above, upon:

(a) detecting a conflicting System Identifier in

(a)(1) 1 IS-IS Hello from any neighbor, or

(a)(2) 2 consecutive LSPs and/or SNPs from the same source;

(b) failing to resolve participation in an area after

(b)(1) incrementing its Sequence Number 3 or more times, and

(b)(2) 10 seconds.

This will not usually detect conflicts between different areas that do not affect routing within those areas. Each system participating in two or more areas MUST maintain a distinction between System Identifiers found in each area. Never-the-less, any replacement System Identifier SHOULD propagate in every such area.

The system SHOULD delay generation and transmission of this replacement System Identifier for a random amount of time between 0 and MAX_GENERATION_DELAY. Although the randomization range is specified in units of seconds, the actual randomly-chosen value SHOULD NOT be in units of whole seconds, but rather in units of the highest available timer resolution.

This reduces the probability of synchronization with advertisements from other systems in the same IS-IS area. If a message is received during the delay indicating the conflict was resolved by another system, the existing local System Identifier remains unchanged.

Acknowledgments

This document parallels text originally in [RFC2153] and various other drafts.

James Carlson, Donald Eastlake, Dave Katz, and Radia Perlman provided background information and helpful comments.

Members of the IESG, ISIS WG, PPPext WG, and TRILL WG contributed additional comments.

IANA Considerations

This document has no IANA actions.

[RFC Editor: please remove this section prior to publication.]

Operational Considerations

MAX_GENERATION_DELAY
: Default: 1 second. This is based on an anticipated IS-IS Hello interval of no more than 4 seconds.

  When Hellos are sent at a greater time interval, this MUST NOT be greater than interval/2, and SHOULD NOT be greater than interval/4.

Configurable System Identifier
: Default 0 (off). Although the probability of conflict with another System Identifier is minuscule, some implementations might not have a sufficient source of randomness, and could repeatedly select conflicting values. An implementation conforming with this specification SHOULD have the capability of manually configuring the System Identifier, preventing random generation of a replacement System Identifier.

  To mitigate against potential assignment conflicts, this System Identifier (considered as a pseudo-MAC) MUST have the "locally-assigned" bit set and "broadcast/multicast" (group) bit clear; that is, the least significant two bits of the most significant octet are equal to 0x2.

Remote Management
: Additional options have been suggested to configure other actions taken upon detecting a conflicting System Identifier. For example, the system might send an alert to a remote management facility and disable IS-IS until remote management updates the configuration. Such remote management configuration options are beyond the scope of this specification.

Security Considerations

These mechanisms provide protection against compromised, malfunctioning, or misconfigured systems [RFC4593]; spoofing attacks are thwarted by quickly renegotiating a replacement System Identifier.

Never-the-less, [RFC5304] increases protection against maliciously configured conflicting System Identifiers.

Normative References

[ISO10589] ISO/IEC 10589:2002, "Intermediate system to Intermediate system routeing information exchange protocol for use in conjunction with the Protocol for providing the Connectionless-mode Network Service (ISO 8473)"

[RFC1195] Callon, R., "Use of OSI IS-IS for routing in TCP/IP and dual environments", December 1990.

[RFC1377] Katz, D., "The PPP OSI Network Layer Control Protocol (OSINLCP)", November 1992.

[RFC1661] Simpson, W., Ed., "The Point-to-Point Protocol (PPP)", STD 51, July 1994.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, March 1997.

[RFC4086] Eastlake, D. (3rd), Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, June 2005.

Informative References

[Baker1992] Baker, F., "PPP Reliable and Multi-Link Transmission", Message to PPP Compression List, June 29, 1992. Message-Id: <9206292135.AA00620@saffron.acc.com>

[RFC1220] Baker, F., "Point-to-Point Protocol extensions for bridging", April 1991.

[RFC1663] Rand, D., "PPP Reliable Transmission", July 1994.

[RFC1717] Sklower, K., Lloyd, B., McGregor, G., and D. Carr, "The PPP Multilink Protocol (MP)", November 1994.

[RFC2153] Simpson, W., "PPP Vendor Extensions", May 1997.

[RFC2469] Narten, T., and C. Burton, "A Caution On The Canonical Ordering Of Link-Layer Addresses", December 1998.

[RFC4593] Barbir, A., Murphy, S., and Y. Yang, "Generic Threats to Routing Protocols", October 2006.

[RFC5304] Li, T., and R. Atkinson, "IS-IS Cryptographic Authentication", October 2008.

[RFC5342] Eastlake 3rd, D., "IANA Considerations and IETF Protocol Usage for IEEE 802 Parameters", BCP 141, September 2008.

[Simpson1992] Simpson, W., "where are we?", Message to IESG and others, April 17, 1992. Message-Id: <269.bsimpson@vela.acs.oakland.edu>

[Simpson1993] Simpson, W., "Re: Simple Multilink Proceedure for PPP - the document", Message to ietf-ppp and iplpdn mailing lists, February 21, 1993. Message-Id: <988.bill.simpson@um.cc.umich.edu>

Author's Address

Questions about this document can be directed to:

William Allen Simpson
DayDreamer
Computer Systems Consulting Services
1384 Fontaine
Madison Heights, Michigan 48071

William.Allen.Simpson@Gmail.com