Network Working Group B. Liu
Internet Draft Huawei Technologies Co., Ltd
Intended status: Proposed Standard October 21, 2013
Expires: April 24, 2014

ISIS Auto-Configuration
draft-liu-isis-auto-conf-00.txt

Status of this Memo

Copyright Notice0

Abstract

This document describes mechanisms for IS-IS to be self-configuring. Such mechanisms could reduce the management burden to configure a network. One obvious environment that could benefit from these mechanisms is IPv6 home network where plug-and-play would be expected. Besides home network, some simple enterprise/ISP networks might also potentially benefit from the self-configuring mechanisms.

Table of Contents

1. Introduction

This memo describes mechanisms for IS-IS [RFC1195][RFC5308] to be auto-configuring. Such mechanisms could reduce the management burden to configure a network. One example is home network where plug-and-play would be expected. Besides home network, some simple enterprise/ISP networks might also potentially benefit from the auto-configuring mechanisms.

The auto-configuring mechanisms are designed based on IPv6-only environment. Some IPv4 environments might also applicable, but they are not specifically considered.

The following aspects of IS-IS auto-configuration are described:

1. IS-IS Default Configuration

2. IS-IS NET self-generation

3. IS-IS Adjacency Formation

However, this draft does not provide a completely configuration-free alternative to the IS-IS protocol, since some plan work by human so far is very difficult to be achieved through algorithm. The following features of IS-IS are not supported by this document:

o Auto-configuring multiple IS-IS processes. The auto-configuration mechanisms only support configuring a single process.

o Route between multiple IS-IS areas. The auto-configuration mechanisms only support routers that are within a single area.

o Auto-configuring multiple operation levels. The auto-configuration mechanisms only support level-1 operation mode.

o This document does not consider interoperability with other routing protocols.

2. IS-IS Default Configuration

o IS-IS SHOULD be enabled on all interfaces in a router as default. For some specific situations, interface MAY be excluded if it is a clear that running IS-IS on the interface is not required.

o IS-IS interfaces MUST be auto-configured to an interface type corresponding to their layer-2 capability. For example, Ethernet interfaces will be auto-configured as broadcast networks and Point-to-Point Protocol (PPP) interfaces will be auto-configured as Point-to-Point interfaces.

3. IS-IS NET Generation

In IS-IS, a router (known as an IS) is identified by an Network Entity Title (NET) which is the address of a Network Service Access Point (NSAP) and represented with an IS-IS specific address format. The NSAP is a logical entity which represents an instance of the IS-IS protocol running on an IS.

The NET consists of the following three parts:

Area address: This field is 1 to 13 octets in length. In IS-IS auto-configuring, this field MUST be 0 in 13 octets length.

System ID: This field follows the area address field, and is 6 octets in length. As specified in IS-IS protocol, this field must be unique among all level-1 routers in the same area when the IS operates at Level 1. In IS-IS auto-configuring, this field SHOULD be the MAC address of one IS-IS enabled interface.

NSEL: This field is the N-selector, and is 1 octet in length. In IS-IS auto-configuring, tt must be set to "00".

4. IS-IS NET Duplication Detection and Resolution

As described in Section 3, in IS-IS auto-configuring the NETs are distinguished by the System ID field in which it is a MAC address. So for IS-IS neighbors' NET duplication, it is equal to MAC address duplication in a LAN, which means a serious problem that devices would need to be changed. IS-IS auto-configuring does not consider this situation.

For the non-neighbor NET duplication detection within an area, this document utilizes a TLV as following to do it.

4.1. Router-Hardware-Fingerprint TLV

The Router-Hardware-Fingerprint TLV is defined in [OSPFv3AC]. This document re-uses it to achieve NET duplication detection.

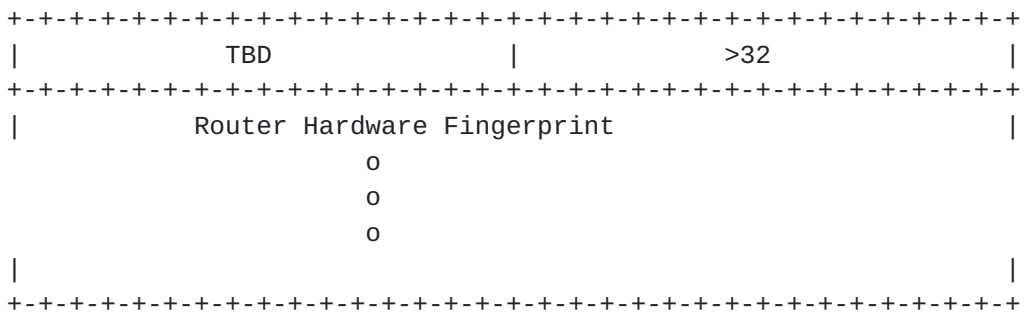

Figure 1 Router-Hardware-Fingerprint TLV Format

As defined in [OSPFv3AC], the contents of the hardware fingerprint should be some combination of CPU ID, or serial number(s) that provides an extremely high probability of uniqueness. It MUST be based on hardware attributes that will not change across hard and soft restarts. Note that, since the TLV is to detect MAC address based NET duplication, the TLV content MUST NOT use MAC address only again. Implementations SHOULD use other information exclude MAC address.

4.2. NET Duplication Detection and Resolution

The Router-Hardware-Fingerprint TLV MUST be included in the first originated level-1 LSP by every auto-configuring routers. An IS-IS auto-configuring router MUST compare a received self-originated LSP's Router-Hardware-Fingerprint TLV against its own one. If the they are not equal, there is a NET duplication and the Router with the numerically smaller router hardware fingerprint MUST generate a new NET.

After selecting a new NET, the LSP with the prior duplicate NET MUST be purged. And any IS-IS neighbor adjacencies MUST be reestablished.

5. Security Considerations

TBD.

6. IANA Considerations

The Router Hardware Fingerprint TLV type code needs an assignment.

7. Acknowledgments

Many useful comments and contributions were made by Sheng Jiang.

This document was inspired by [OSPFv3AC].

8. References

8.1. Normative References

[RFC1195] Callon, R., "Use of OSI IS-IS for routing in TCP/IP and dual environments", RFC 1195, December 1990.

[RFC5308] Hopps, C., "Routing IPv6 with IS-IS", RFC 5308, October 2008.

[OSPFv3AC] Lindem, A., and J. Arkko, "OSPFv3 Auto-Configuration", Work in Progress, October 2013

Authors' Addresses

Bing Liu
Huawei Technologies Co., Ltd
Q14, Huawei Campus
No.156 Beiqing Rd.
Hai-Dian District, Beijing 100095
P.R. China

Email: leo.liubing@huawei.com