isis
Internet-Draft
Intended status: Standards Track
Expires: April 30, 2015

B. Liu
Huawei Technologies
B. Decraene
Orange
I. Farrer
Deutsche Telekom AG
M. Abrahamsson
T-Systems
October 27, 2014

ISIS Auto-Configuration
draft-liu-isis-auto-conf-03

Abstract

This document describes an IS-IS auto-configuration technology. The key mechanisms of this technology are IS-IS NET (Network Entity Title) self-generation, duplication detection and duplication resolution. This technology fits the environment where plug-and-play is expected, e.g., home networks and small or medium size enterprise networks.

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. Home networks and small or medium size enterprise networks where plug-n-play is expected can benefit from these mechanisms.

In addition, this memo defines how such un-configured routers should behave, in order to limit the risk on existing network using IS-IS (Section 3.4.1 & 3.5).

IS-IS auto-configuration mainly contains the following aspects:

1. IS-IS Default Configurations

2. IS-IS NET Self-Generation

3. NET Duplication Detection and Resolution

4. ISIS TLVs utilization such as Authentication TLV, Wide Metric TLV etc.

2. Scope

The auto-configuring mechanisms does not specifically destinguish IPv4 or IPv6.

The auto-configuring mechanisms enabled interfaces are assumed to have a 48-bit MAC address.

This auto-configuration mechanism aims at simple case. The following advanced features are out of scope:

- Multiple IS-IS instances.
- Multi-area and level-2 routers.
- Interworking with other routing protocols.

3. Protocol Specification

3.1. IS-IS Default Configuration

- IS-IS SHOULD be enabled as default on all interfaces in a router that requires the IS-IS auto-configuration. For some specific situations, interface MAY be excluded if it is a clear that running IS-IS on the interface is not required.
- 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.
- IS-IS auto-configuration interfaces MUST be configured with level-1.

3.2. 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 three parts. The auto-generation mechanisms of each part are described as the following:

- 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, it SHOULD be set to "00".

3.3. IS-IS NET Duplication Detection and Resolution

NET addresses need to be distinct within one IS-IS area. This document auto-configure the NET address based on the MAC address which are supposed to be globally unique, but in order to detect and correct the possible MAC duplication, this section defines how IS-IS may detect and correct NET duplication.

3.3.1. Router-Hardware-Fingerprint TLV

The Router-Hardware-Fingerprint TLV is defined in [I-D.ietf-ospf-ospfv3-autoconfig]. This document re-uses it to achieve NET duplication detection.

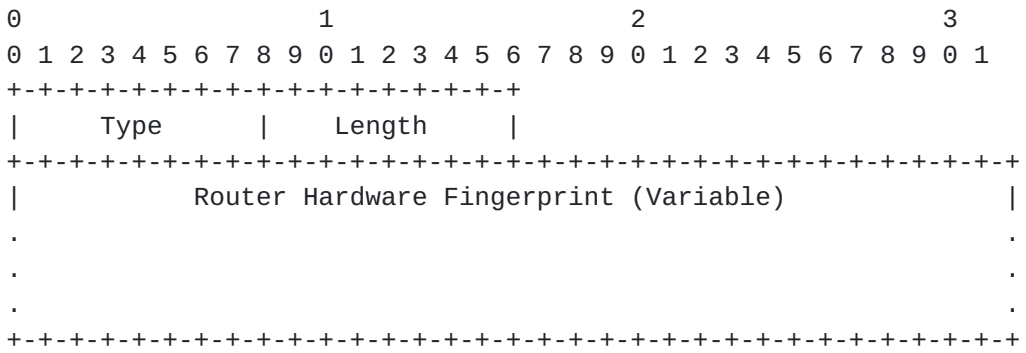

Figure 1 Router-Hardware-Fingerprint TLV Format

As defined in [I-D.ietf-ospf-ospfv3-autoconfig], 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. The length of the Router-Hardware-Fingerprint is variable but must be 32 octets or greater.

Note that, since the TLV is to detect MAC address based NET duplication, the TLV content SHOULD NOT use MAC address.

3.3.2. NET Duplication Detection and Resolution Procedures

1) Flood the Router-Hardware-Fingerprint TLVs

When an IS-IS auto-configuration router gets online, it MUST include the Router-Hardware-Fingerprint TLV in the first originated level-1 LSP. Then all the routers in the area could receive the information in the TLV.

2) Compare the received Router-Hardware-Fingerprint TLVs

An IS-IS auto-configuring router MUST compare a received self-originated LSP's Router-Hardware-Fingerprint TLV against its own one. If they are equal, it means the LSP was indeed originated by the router itself; if they are not equal, it means some other router has the same NET originated the LSP, thus there is a NET duplication.

3) Duplication resolution

When NET duplication occurs, the router with the numerically smaller router hardware fingerprint MUST generate a new NET. The newly generated NET SHOULD take a NET duplication detection as well.

4) Purge the LSPs containing duplicated NET

Before flooding the new NET, the LSP with the prior duplicate NET MUST be purged. And any IS-IS neighbor adjacencies MUST be reestablished.

5) Re-join the network with the new NET

After purging the LSPs with the duplicated NET, the router re-join the IS-IS auto-configuration network with the newly generated NET.

3.4. IS-IS TLVs Usage

3.4.1. Authentication TLV

Every IS-IS auto-configuration message MUST include an authentication TLV (TLV 10, [RFC5304]) with the Type 1 authentication mode ("Cleartext Password") in order to avoid the auto-conf router to accidentally join an existing IS-IS network which is not intended to be auto-configured.

This feature is necessary since it might seriously break an existing IS-IS network or cause unnecessary management confusion if a low end CPE (which might be the normal form of ISIS-autoconf routers) occasionally joins the network.

The cleartext password is specified as "isis-autoconf". Routers that implement IS-IS auto-configuration MUST use this password as default, so that different routers could authenticate each other with no human intervene as default. And routers MUST be able to set manual password by the users.

3.4.2. Wide Metric TLV

IS-IS auto-configuration routers SHOULD support wide metric (TLV 22, [RFC5305]). It is recommended that IS-IS auto-configuration routers use a high metric value (e.g. 1000000) as default in order to typically prefer the manually configured adjacencies rather than the auto-conf ones.

3.4.3. Dynamic Host Name TLV

IS-IS auto-configuration routers SHOULD advertise their Dynamic Host Names TVL (TLV 137, [RFC5301]). The host names could be provisioned by an IT system, or just use the name of vendor, device type or serial number etc.

3.4.4. Purge Originator Identification TLV

For troubleshooting purpose, the Purge Originator Identification TLV (TLV 13, [RFC6232]) MAY be used to determin the origin of the purge. Please refer to [RFC6232] for details.

3.5. Routing Behavior Considerations

3.5.1. Adjacency Formation

Since ISIS does not require strict hold timers matching to form adjacency, this document does not specify specific hold timers. However, the timers should be within a reasonable range based on current practisce in the industry. (For example, 30 seconds for holdtime and 20 minutes for LSP lifetime.)

3.5.2. Co-existing with Other IGP Auto-configuration

If a router supports multiple IGP auto-configuration mechanisms (e.g. both IS-IS auto-configuration and OSPF auto-configuration), then in practice it is a problem that there should be a mechanism to decide which IGP to be used, or even both.

However, the behavior of multiple IGP protocols interaction should be done in the router level rather than in any IGP protocols. Currently, there is some relevant work going on, for example, the [I-D.ietf-homenet-hncp] is to have the proposed HNCP (Home Network Control Protocol) choose what IGP should be used.

4. Security Considerations

In general, auto-configuration is mutually incompatible with authentication. So we can't have both. This is not really specific to IS-IS.

Unwanted routers could easily join in an existing IS-IS auto-configuration network by setting the authentication password as "isis-autoconf" default value or sniff the cleartext password online. However, this is a common security risk shared by other IS-IS networks that don't set proper authentication mechanisms. For wired deployment, the wired line itself could be considered as an implicit authentication that normally unwanted routers are not able to connect to the wire line; for wireless deployment, the authentication could be achieve at the lower wireless link layer.

Malicious router could modify the SystemID field to cause NET duplication detection and resolution vibrate thus cause the routing system vibrate.

5. IANA Considerations

The Router Hardware Fingerprint TLV type code needs an assignment by IANA.

6. Acknowledgements

Many useful comments and contributions were made by Sheng Jiang.

This document was inspired by [OSPFv3AC].

This document was produced using the xml2rfc tool [RFC2629].
(initiallly prepared using 2-Word-v2.0.template.dot.)

7. References

7.1. Normative References

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

[RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", RFC 2629, June 1999.

[RFC5301] McPherson, D. and N. Shen, "Dynamic Hostname Exchange Mechanism for IS-IS", RFC 5301, October 2008.

[RFC5304] Li, T. and R. Atkinson, "IS-IS Cryptographic Authentication", RFC 5304, October 2008.

[RFC5305] Li, T. and H. Smit, "IS-IS Extensions for Traffic Engineering", RFC 5305, October 2008.

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

[RFC6232] Wei, F., Qin, Y., Li, Z., Li, T., and J. Dong, "Purge Originator Identification TLV for IS-IS", RFC 6232, May 2011.

7.2. Informative References

[I-D.ietf-homenet-hncp]
Stenberg, M. and S. Barth, "Home Networking Control Protocol", draft-ietf-homenet-hncp-01 (work in progress), June 2014.

[I-D.ietf-ospf-ospfv3-autoconfig]
Lindem, A. and J. Arkko, "OSPFv3 Auto-Configuration", draft-ietf-ospf-ospfv3-autoconfig-09 (work in progress), September 2014.

Authors' Addresses

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

Email: leo.liubing@huawei.com

Bruno Decraene
Orange
Issy-les-Moulineaux FR
FR

Email: bruno.decraene@orange.com

Ian Farrer
Deutsche Telekom AG
Bonn
Germany

Email: ian.farrer@telekom.de

Mikael Abrahamsson
T-Systems
Stockholm
Sweden

Email: mikael.abrahamsson@t-systems.se