isis
Internet-Draft
Intended status: Standards Track
Expires: December 21, 2015

B. Liu
Huawei Technologies
B. Decraene
Orange
I. Farrer
Deutsche Telekom AG
M. Abrahamsson
T-Systems
June 19, 2015

ISIS Auto-Configuration
draft-liu-isis-auto-conf-05

Abstract

This document specifies 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.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 21, 2015.

Copyright Notice

Table of Contents

1. Introduction

This document 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-and-play is expected can benefit from these mechanisms.

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

IS-IS auto-configuration contains the following aspects:

1. IS-IS default configurations

2. IS-IS NET (Network Entity Title) 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 distinguish IPv4 or IPv6.

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 auto-configuration 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.

- o 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 Intermediate System) is identified by an 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:

- o Area address

  This field is 1 to 13 octets in length. In IS-IS auto-configuration, this field MUST be 0 in 13 octets length.

- o System ID

  This field follows the area address field, and is 6 octets in length. There are two basic requirements for the System ID generation:

  - As specified in IS-IS protocol, this field must be unique among all routers in the same area.

  - In order to make the routing system stable, the System ID SHOULD remain the same after it is firstly generated. It SHOULD not be changed due to device status change (such as interface enable/disable, interface plug in/off, device reboot, firmware update etc.) or configuration change (such as changing system configurations or IS-IS configurations etc.); but it MUST allow be changed by collision resolution and SHOULD allow be cleared by user enforced system reset.

  More specific considerations for SysID generation are described in Section 3.3.3 .

o NSEL

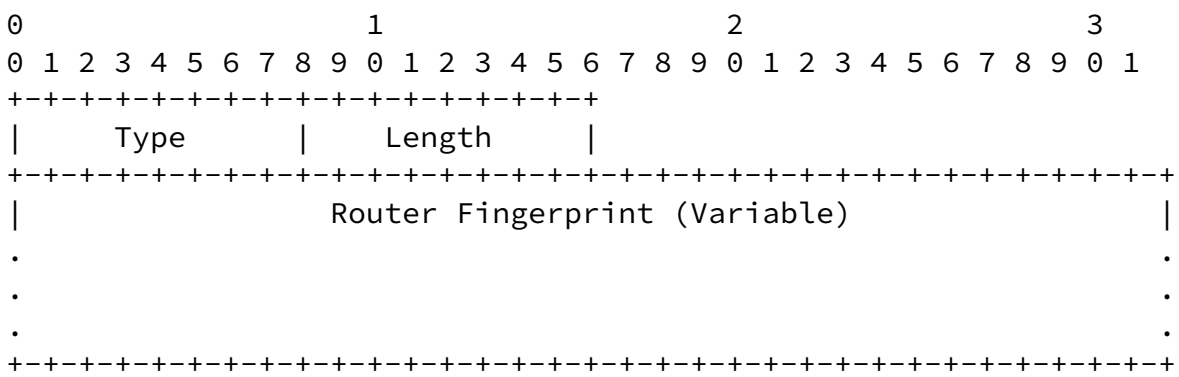
This field is the N-selector, and is 1 octet in length. In IS-IS auto-configuration, it SHOULD be set to "00".

3.3. IS-IS NET Duplication Detection and Resolution

NET addresses need to be distinct within one IS-IS area. As described in Section 3.3.3, the NET address is generated based on entropies such as MAC address which are supposed to be unique, but in theory there is still possibility of duplication. This section defines how IS-IS detects and corrects NET duplication.

3.3.1. Router-Fingerprint TLV

The Router-Fingerprint TLV re-uses the design of Router-Hardware-Fingerprint TLV defined in [RFC7503].



The length of the Router-Fingerprint is variable but must be 32 octets or greater; and the content is also supposed to be unique among all the routers.

More specific considerations for Router-Fingerprint is described in Section 3.3.3 .

3.3.2. NET Duplication Detection and Resolution Procedures

1) Flood the Router-Fingerprint TLVs

When an IS-IS auto-configuration router gets online, it MUST include the Router-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-Fingerprint TLVs

When receiving a LSP having its own NET address, an IS-IS router MUST check the Router-Fingerprint TLV. If the Router-Fingerprint TLV is different from its own, there is a NET duplication and the following procedure SHOULD be performed.

3) Duplication resolution

When NET duplication occurs, the router with the numerically smaller Router-Fingerprint MUST generate a new NET. Note that, the router MUST compare the two Router-Fingerprint in terms of two numeric numbers (e.g. unsigned integer).

4) Re-join the network with the new NET

The router with the smaller Router-Fingerprint advertise new LSPs based on the newly generated NET to re-join the IS-IS auto-configuration network.

Note that, since the other router still uses the old NET, the smaller Router-Distinguisher router MUST NOT purge it's LSPs; the router with the highest Router-Distinguisher MUST re-advertise its own LSP (after increasing the sequence number).

The newly generated NET SHOULD take a NET duplication detection as well.

Note that, there might be an exceptional case that one auto-configuring router detects the NET duplication by LSP war (as described in Section 3.3.4), but there is no Router-Fingerprint TLV from the duplicated router for comparing. This might be caused by a non-autoconfiguration router by accident connected to the auto-configuration domain (with the Authentication TLV correctly set by accident) or other unexpected bad behaviors. In this case, the auto-

configuration router MUST generate a new NET and re-joint the network.

3.3.3. SysID and Router-Fingerprint Generation Considerations

As specified in this document, there are two distinguisher need to be self-generated, which is SysID and Router-Fingerprint. In a network device, normally there are resources which provide an extremely high probability of uniqueness thus could be used as seeds to derive distinguisher (e.g. hashing or generating pseudo-random numbers), such as:

- MAC address(es)
- Configured IP address(es)
- Hardware IDs (e.g. CPU ID)
- Device serial number(s)
- System clock at a certain specific time
- Arbitrary received packet

This document does not specify a certain method to generate the SysID and Router-Fingerprint. However, the generation of SysID and Router-Fingerprint MUST be based on different seeds so that the two distinguisher would not collide.

There is an important concern that the seeds listed above (except MAC address) might not be available in some small devices such as home routers. This is because of the hardware/software limitation and the lack of sufficient communication packets at the initial stage in the

home routers when doing ISIS-autoconfiguration. In this case, this document suggests to use MAC address as SysID and generate a pseudo-random number based on another seed (such as the memory address of a certain variable in the program) as Router-Fingerprint. The pseudo-random number might not have a very high quality in this solution, but should be sufficient in home networks scenarios.

Note that, the Router-Fingerprint SHOULD also remain the same after

it is firstly generated. It SHOULD not be changed due to device status change (such as interface enable/disable, interface plug in/off, device reboot, firmware update etc.) or configuration change (such as changing system configurations or IS-IS configurations etc.); but it MUST allow be changed by double-duplication resolution Section 3.3.4 and SHOULD allow be cleared by user enforced system reset.

3.3.4. Double-Duplication of both NET and Router-Fingerprint

As described above, the resources for generating the distinguisher might be very constrained at the initial stage. Hence, the double-duplication of both NET and Router-Fingerprint needs to be considered.

ISIS-autoconfiguring routers SHOULD support detecting NET duplication by LSP war. LSP war is a phenomenon that if a router receives a LSP originated with it's NET, but it doesn't find it in the database, or it does not match the one the router has (e.g. It advertises IP prefixes that the router doesn't own, or IS neighbors that the router doesn't see), then per ISIS specification, the router must re-originate its LSP with an increased sequence number. If double-duplication happens, the duplicated two routers will both continuously have the above behavior. After multiples iterations, the program should be able to deduce that double-duplication happens.

At the point when double-duplication happens, routers should have much more entropies available. Thus, the router is to extend or re-generate its Router-Fingerprint (one simple way is just adding the LSP sequence number of the next LSP it will send to the Router-Fingerprint).

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-autoconfiguration 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 TLV (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 determine 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 practise 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. For example, with the Home Network Control Protocol ([I-D.ietf-homenet-hncp]), the routers could achieve a consensus on what IGP to use.

4. Security Considerations

In general, auto-configuration is mutually incompatible with authentication. This is a common problem that IS-IS auto-configuration can not avoid.

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 SysID field to keep causing NET duplication detection and resolution thus cause the routing system vibrate.

5. IANA Considerations

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

6. Acknowledgements

This document was heavily inspired by [RFC7503].

Martin Winter, Christian Franke and David Lamparter gave essential feedback to improve the technical design based on their implementation experience. Many useful comments and contributions were made by Sheng Jiang, Qin Wu, Hannes Gredler, Peter Lothberg, Uma Chundury, Nan Wu, Acee Lindem, Karsten Thomann, Les Ginsberg and some

other people in ISIS working group.

This document was produced using the xml2rfc tool [RFC2629]. (initially 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., Barth, S., and P. Pfister, "Home Networking Control Protocol", draft-ietf-homenet-hncp-06 (work in progress), June 2015.

[RFC7503] Lindem, A. and J. Arkko, "OSPFv3 Autoconfiguration", RFC 7503, April 2015.

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