isis
Internet-Draft
Intended status: Standards Track
Expires: April 21, 2016

B. Liu, Ed.
Huawei Technologies
B. Decraene
Orange
I. Farrer
Deutsche Telekom AG
M. Abrahamsson
T-Systems
L. Ginsberg
Cisco Systems

October 19, 2015

ISIS Auto-Configuration
draft-liu-isis-auto-conf-06

Abstract

This document specifies an IS-IS auto-configuration technology. The key mechanisms of this technology are IS-IS System ID self-generation, duplication detection and duplication resolution. This technology fits the environment where plug-and-play is expected.

Table of Contents

1. Introduction

This document describes mechanisms for IS-IS [RFC1195] [ISO_IEC10589][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.

This document also defines mechanisms which prevent unintentional interoperation of autoconfigured routers with non-autoconfigured routers. See Section 3.3.1 .

IS-IS auto-configuration contains the following aspects:

1. IS-IS default configurations

2. IS-IS System ID self-generation

3. System ID duplication detection and resolution

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

2. Scope

The auto-configuring mechanisms support both IPv4 and IPv6 deployments.

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 routing
- Interworking with other routing protocols

3. Protocol Specification

3.1. IS-IS Default Configuration

- 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 instance MUST be configured with level-1, so that the interfaces operate at level-1 only.
- IS-IS auto-configuration SHOULD allow P2P mode on Ethernet interfaces.

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 Intermediate System.

The autoconfiguration mechanism generates the IS-IS NET as the following:

o Area address

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

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.

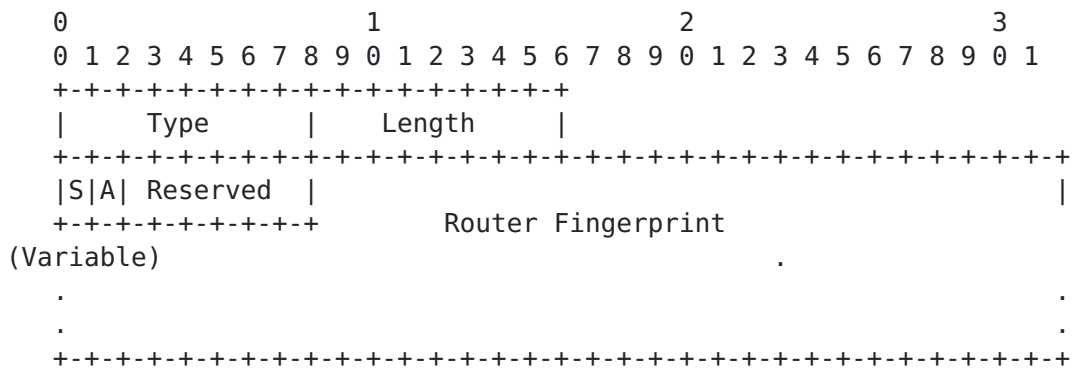
More specific considerations for System ID generation are described in Section 3.3.3 .

3.3. IS-IS System ID Duplication Detection and Resolution

The System ID of each node MUST be unique. As described in Section 3.3.3, the System ID 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 resolves System ID duplication.

3.3.1. Router-Fingerprint TLV

The Router-Fingerprint TLV basically re-uses the design of Router-Hardware-Fingerprint TLV defined in [RFC7503]. However, there is one difference that one flag is added to indicate the node is in "start-up mode" which is defined in Section 3.3.2 .



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.

- Type: to be assigned by IANA.
- Length: the length of the value field.
- S flag: indicates the router is in "start-up" mode as described below.
- A flag: indicates the router is operating in autoconfiguration mode. This flag is in case the TLV gets used outside of autoconfiguration. If A flag setting does not match in hellos then no adjacency should be formed.
- Reserved: these bits MUST be set to zero and MUST be ignored when received.
- Router Fingerprint: uniquely identifies a router, variable length.

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

3.3.2. System ID Duplication Detection and Resolution Procedures

This section describes the System ID duplication detection and resolution between two neighbors and two non-neighbors respectively. This is because the routing messages between neighbors and non-neighbors are a bit different.

3.3.2.1. Start-up Mode

While in startup-mode, an auto-configuration router forms adjacencies but generates only LSP #0 which contains only the Router-Fingerprint TLV. A router remains in startup-mode until it has successfully completed LSPDB synchronization with all neighbors or until 1 minute

has elapsed - whichever is longer. If duplicate system-ID is detected while in startup-mode the router MUST clear all adjacencies, select a new system-id (subject to rules defined in Section 3.3.2.2), and reenter Startup-mode.

The start-up mode is to minimize the occurrence of System ID changes for a router once it has become fully operational. It has minimal impact on a running network because the startup node is not yet being used for forwarding traffic. Once duplicate System ID has been resolved the router begins normal operation. If two routers are both in startup mode (or both NOT in startup mode) and duplicate system-id is detected then they determine which one changes its system-id based on fingerprint.

When an IS-IS auto-configuration router boots up, it MUST operate in start-up mode until duplicate system-id detection has successfully completed.

3.3.2.2. Duplication Between Neighbors

In case of System ID duplication occurs between neighbors, an IS-IS auto-configuration router MUST include the Router-Fingerprint TLV in the Hello messages, so that the duplication could be detected before adjacency forming.

Procedures of the nodes in Start-up Mode:

1. Boot up, advertise the Router-Fingerprint TLV in Hello message

   The router sends Hellos which include the Router-Fingerprint TLV. Adjacencies are formed as normal but MUST NOT be advertised in LSPs until the router exits startup-mode.

2. Receive Hello message(s), and verifies System ID duplication

   Received hellos are inspected for possible duplicate System ID. If duplication is detected, the router MUST check the S flag of the Router-Fingerprint TLV.

   + If the S flag is NOT set (which means the Hello was NOT generated by a neighbor also in Start-up mode), then the router MUST re-generate the System ID and reenter Startup-mode.

   + If the S flag is set (which means the neighbor is also in Startup-mode),

- the router which has a numerically smaller Router-Fingerprint MUST re-generate the System ID and reenter Startup-mode. Fingerprint comparison is performed octet by octet until octets are different. Then the smaller fingerprint is the one with the smaller octet (unsigned integer). If the fingerprints have different lengths, then the shorter length fingerprint MUST be padding with zero for comparison.

- If Router Fingerprints are identical, both routers MUST re-generate the System ID and the Router Fingerprint, and reenter Startup-mode.

3. Run in normal operation

After the System ID duplication procedure is done, the router begins to run in normal operation. The router MUST re-advertise the Router-Fingerprint TLV with the S flag off.

Procedures of the nodes NOT in Start-up Mode:

1. Compare the System ID in received Hello messages

When receiving a Hello message, the router MUST check the System ID of the Hello. If the System ID is the same as its own, it indicates a System ID duplication occurs.

If there is no Router-Fingerprint TLV in the Hello message, it means a non-autoconfiguration router by accident connected to the auto-configuration domain or other unexpected bad behaviors. In this case, the auto-configuration router MUST NOT form adjacency with the non-autoconfiguration router.

2. Duplication resolution

When System ID duplication occurs, the non-startup mode router MUST check the S flag of the duplicated Router-Fingerprint TLV:

+ If the S flag is NOT set, then the router with the numerically smaller or equal Router-Fingerprint MUST generate a new System ID. Note that, the router MUST compare the two Router-Fingerprint in terms of two numeric numbers.

+ If the S flag is set, then router does nothing, because it MUST be the node which is in start-up mode re-generates the System ID.

3. Re-join the network with the new System ID (if required)

   The router with the smaller Router-Fingerprint advertise new Hellos based on the newly generated NET to re-join the IS-IS auto-configuration network. The router with the highest Router-Fingerprint MUST re-advertise its own LSP (after increasing the sequence number).

   The newly generated System ID SHOULD take a duplication detection as well.

3.3.2.3. Duplication Between Non-neighbors

System ID duplication may also occur between non-neighbors, so an IS-IS auto-configuration router MUST also include the Router-Fingerprint TLV in the LSP messages. Specific procedures are as the following.

Procedures of the nodes in Start-up Mode:

1. Boot up, form adjacency

2. Acquire LSPDB and verifies System ID duplication

   The router generates only LSP #0 which contains only the Fingerprint TLV; and that Fingerprint is only sent in LSP #0. A router remains in startup-mode until it has successfully completed LSPDB synchronization with all neighbors or until 1 minute has elapsed - whichever is longer. If duplicate system-ID is detected, the router MUST check the S flag of the Router-Fingerprint TLV of the LSP that contains the duplicated System ID.

   + If the S flag is not set, it means the LSP was not generated at the Start-up Mode, then the router itself MUST clear all adjacencies, re-generate a new system-id and reenter Startup-mode.

   + If the S flag is set, then the router which has a numerically smaller Router-Fingerprint MUST generate a new System ID and reenter Startup-mode.

3. Run in normal operation

   After the System ID duplication procedure is done, the router begins to run in normal operation. The router MUST re-advertise the Router-Fingerprint TLV with the S flag off.

Procedures of the nodes not in Start-up Mode:

1. Compare the received Router-Fingerprint TLVs

   When receiving a LSP containing its own System ID, the router MUST check the Router-Fingerprint TLV. If the Router-Fingerprint TLV is different from its own, it indicates a System ID duplication occurs.

2. Duplication resolution

   When System ID duplication occurs, the non-startup mode router MUST check the S flag of the duplicated Router-Fingerprint TLV:

   + If the S flag is NOT set, then the router with the numerically smaller Router-Fingerprint MUST generate a new System ID. Note that, the router MUST compare the two Router-Fingerprint in terms of two numeric numbers.

   + If the S flag is set, then router does nothing, because according to the start-up mode procedure, the start-up node MUST re-generate the System ID.

3. Re-join the network with the new System ID

   The router changing its system ID advertise new LSPs based on the newly generated System ID to re-join the IS-IS auto-configuration network. The router with the highest Router-Fingerprint MUST re-advertise its own LSP (after increasing the sequence number).

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

3.3.3. System ID and Router-Fingerprint Generation Considerations

As specified in this document, there are two distinguisher need to be self-generated, which is System ID 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 recommends to use an IEEE 802 48-bit MAC address associated with the router as the initial System ID. This document does not specify a specific method to re-generate the System ID when duplication happens.

This document also does not specify a specific method to generate the Router-Fingerprint. However, the generation of System ID 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 System ID 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 System ID 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 System ID and Router-Fingerprint needs to be considered.

ISIS-autoconfiguring routers SHOULD support detecting System ID duplication by LSP war. LSP war is a phenomenon that if a router receives a LSP originated with its System ID, 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). (Optimized solution TBD.)

3.4. IS-IS TLVs Usage

This section describes several TLVs that are utilized by IS-IS auto-configuration.

3.4.1. Authentication TLV

It is RECOMMENDED that IS-IS routers supporting this specification minimally offer an option to explicitly configure a single password for HMAC-MD5 authentication, which is Type 54 authentication mode of [RFC5304]. In this case, the Authentication TLV (TLV 10) is needed.

3.4.2. Wide Metric TLV

IS-IS auto-configuration routers MUST support TLVs using wide metric as defined in [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-configuring ones.

3.4.3. Dynamic Host Name TLV

IS-IS auto-configuration routers MAY 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. Note that, the hostname needs to be unique so that it could be useful.

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, the defaults defined in [ISO_IEC10589] .)

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.

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 System ID field to keep causing System ID duplication detection and resolution thus cause the routing system oscillate. However, this is not a new attack vector as without this document the consequences would be higher as other routers would not try to adapt.

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 were made by Acee Lindem, Karsten Thomannby, Hannes Gredler, Peter Lothberg, Uma Chundury, Qin Wu, Sheng Jiang and Nan Wu, etc.

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

7. References

7.1. Normative References

[ISO_IEC10589]
"Intermediate System to Intermediate System intra-domain routeing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473)", ISO/IEC 10589", November 2002.

[RFC1195] Callon, R., "Use of OSI IS-IS for routing in TCP/IP and dual environments", RFC 1195, DOI 10.17487/RFC1195, December 1990, <http://www.rfc-editor.org/info/rfc1195>.

[RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", RFC 2629, DOI 10.17487/RFC2629, June 1999, <http://www.rfc-editor.org/info/rfc2629>.

[RFC5301] McPherson, D. and N. Shen, "Dynamic Hostname Exchange Mechanism for IS-IS", RFC 5301, DOI 10.17487/RFC5301, October 2008, <http://www.rfc-editor.org/info/rfc5301>.

[RFC5304] Li, T. and R. Atkinson, "IS-IS Cryptographic Authentication", RFC 5304, DOI 10.17487/RFC5304, October 2008, <http://www.rfc-editor.org/info/rfc5304>.

[RFC5305] Li, T. and H. Smit, "IS-IS Extensions for Traffic Engineering", RFC 5305, DOI 10.17487/RFC5305, October 2008, <http://www.rfc-editor.org/info/rfc5305>.

[RFC5308] Hopps, C., "Routing IPv6 with IS-IS", RFC 5308, DOI 10.17487/RFC5308, October 2008, <http://www.rfc-editor.org/info/rfc5308>.

[RFC6232] Wei, F., Qin, Y., Li, Z., Li, T., and J. Dong, "Purge Originator Identification TLV for IS-IS", RFC 6232, DOI 10.17487/RFC6232, May 2011, <http://www.rfc-editor.org/info/rfc6232>.

7.2. Informative References

[I-D.ietf-homenet-hncp]
Stenberg, M., Barth, S., and P. Pfister, "Home Networking Control Protocol", draft-ietf-homenet-hncp-09 (work in progress), August 2015.

[RFC7503] Lindem, A. and J. Arkko, "OSPFv3 Autoconfiguration", RFC 7503, DOI 10.17487/RFC7503, April 2015, <http://www.rfc-editor.org/info/rfc7503>.

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
38 rue du General Leclerc
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

Les Ginsberg
Cisco Systems
510 McCarthy Blvd.
Milpitas CA 95035
USA

Email: ginsberg@cisco.com