isis
Internet-Draft
Intended status: Standards Track
Expires: January 21, 2017

B. Liu, Ed.
Huawei Technologies
B. Decraene
Orange
I. Farrer
Deutsche Telekom AG
M. Abrahamsson
T-Systems
L. Ginsberg
Cisco Systems
July 20, 2016

# ISIS Auto-Configuration
# draft-ietf-isis-auto-conf-02

Abstract

This document specifies IS-IS auto-configuration mechanisms. The key components are IS-IS System ID self-generation, duplication detection and duplication resolution. These mechanisms provide limited IS-IS functions, thus they are fit for the networks where plug-and-play configuration 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 January 21, 2017.

Table of Contents



## 1. Introduction

This document specifies mechanisms for IS-IS [RFC1195] [ISO_IEC10589][RFC5308] to be auto-configuring. Such mechanisms could reduce the management burden for configuring a network, especially where plug-and-play device configuration is required.

IS-IS auto-configuration is comprised of the following functions:

1. IS-IS default configurations.

2. IS-IS System ID self-generation.

3. System ID duplication detection and resolution.

4. ISIS TLV utilization (Authentication TLV, Wide Metric TLV, and Dynamic Host Name TLV).

This document also defines mechanisms to prevent the unintentional interoperation of auto-configured routers with non-autoconfigured routers. See Section 3.3.1.

## 2. Scope

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

These auto-configuration mechanisms aim to cover simple deployment cases. The following important features are not supported:

- 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 as level-1, so that the interfaces operate as level-1 only.

### 3.2. IS-IS NET Generation

In IS-IS, a router (known as an Intermediate System) is identified by a 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 auto-configuration mechanism generates the IS-IS NET as the following:

- Area address

  In IS-IS auto-configuration, this field MUST be 13 octets long and set to all 0.

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

  - After its initial generation, the System ID SHOULD remain stable to improve the stability of the routing system. It SHOULD not be changed due to device status change (such as interface enable/disable, interface connect/disconnect, device reboot, firmware update etc.) or configuration change (such as changing system configuration or IS-IS configuration); but MUST support change as part of the System ID collision resolution process and SHOULD allow being cleared by a user initiated system reset.

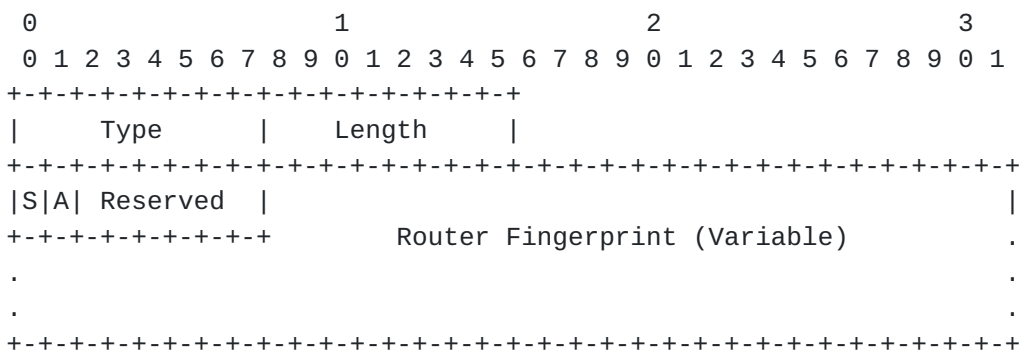
  More specific considerations for System ID generation are described in Section 3.3.3 .

## 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 (e.g. MAC address) which are generally expected to be unique. However, since there may be limitations to the available entropies, there is still the possibility of System ID duplication. This section defines how IS-IS detects and resolves System ID duplication.

### 3.3.1. Router-Fingerprint TLV

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




Router Fingerprint TLV Format

The length of the Router-Fingerprint is variable but MUST be 32 octets or greater. For correct operation, the Router-Fingerprint MUST be unique among all the routers participating in the IS-IS area.

- Type: to be assigned by IANA.
- Length: the length of the value field. As the Router Fingerprint length is variable, the field length is also variable.
- S flag: when set, indicates the router is in "start-up" mode.
- A flag: when set, indicates that the router is operating in auto-configuration mode. The purpose of the flag is so that two routers can identify if they are both using auto-configuration. If the 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 by the receiver.
- Router Fingerprint: uniquely identifies a router, variable length.

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

### 3.3.2. Duplicate System ID Detection and Resolution Procedures

This section describes the duplicate System ID detection and resolution process between two neighbors and two non-neighbors respectively. This is due to difference in the the routing messages between neighbors and non-neighbors.

#### 3.3.2.1. Start-up Mode

While in Start-up 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 a duplicate System ID is detected while in Start-up Mode stage, the Start-up Mode router MUST clear all adjacencies, select a new System ID (subject to rules defined in Section 3.3.2.2 ), and re-enter Start-up Mode.

The purpose of 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 Start-up Mode node is not yet being used for forwarding traffic. Once duplicate System IDs have been resolved the router begins normal operation. If two routers are both in Start-up Mode and duplicate System ID is detected, they follow the duplication resolution as specified in Section 3.3.2.2 and Section 3.3.2.3.

When an IS-IS auto-configuration router boots up, it MUST operate in Startup-Mode until duplicate System ID detection has successfully completed.

#### 3.3.2.2. Duplication Between Neighbors

In the case of duplicate System IDs being detected between neighbors, an IS-IS auto-configuration router MUST include the Router-Fingerprint TLV in the Hello messages, so that the duplication can be detected before an adjacency is formed.

Start-up Mode procedures:

1. Boot up and advertisement of the Router-Fingerprint TLV in Hello messages

   The router sends Hello messages which include the Router-Fingerprint TLV. Adjacencies are formed as normal but MUST NOT be advertised in LSPs until the router exits Start-up Mode.

2. Receiving Hello message(s), and System ID duplication detection

   Received Hello messages are inspected for a possible duplicate System ID. If a duplicate 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 message was NOT generated by a Start-up Mode neighbor), then the router MUST re-generate the System ID and re-enter Start-up Mode.

+ If the S flag is set (meaning the neighbor is also in Start-up Mode),

  - The router which has a numerically smaller Router-Fingerprint MUST re-generate its System ID and re-enter Start-up Mode. Fingerprint comparison MUST be performed octet by octet starts from the left until a difference is found. Then, the numeric smaller fingerprint is the one with the lowest value. If the fingerprints have different lengths, then the shorter length fingerprint MUST be padding with zero at the left side for comparison.

  - If the Router Fingerprints are identical, both routers MUST re-generate the System ID and the Router Fingerprint, and re-enter Start-up Mode.

3. Normal operation

After the System ID duplication procedure is successfully completed, the router begins normal operation. The router MUST re-advertise the Router-Fingerprint TLV with the S flag disabled.

Non Start-up Mode procedures:

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 that System ID duplication has occurred.

If there is no Router-Fingerprint TLV in the received Hello message, this is interpreted as the attached router either does not support auto-configuration, or does not have it enabled. In this case, the auto-configuration router MUST NOT form adjacency with the non-autoconfiguration router.

2. Duplication resolution

When duplicate System IDs are detected, 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 octet by octet until difference is found.

+ If the S flag is set, no further action is necessary in the Duplication resolution process.

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

   The router that has changed its System ID advertises new Hellos containing the newly generated System ID to re-join the IS-IS auto-configuration network. The conflicting SysID-duplicated router also MUST increase the sequence number and re-advertise its own Hellos.

   The Duplication Detection process SHOULD be repeated with the newly generated System.

#### 3.3.2.3. Duplication Between Non-neighbors

System ID duplication may also occur between non-neighbors, therefore an IS-IS auto-configuration router MUST also include the Router-Fingerprint TLV in its LSP messages. The specific procedures are as follows:

Start-up Mode procedures:

1. Boot up, adjacency formation

2. Acquiring LSPDB and checking System ID duplication

   The router generates only an LSP #0 which contains only the Fingerprint TLV; and that Fingerprint is only sent in LSP #0. A router remains in Start-up 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 generated by a Non Start-up Mode node, then the router itself MUST clear all adjacencies, re-generate a new system-id and reenter Start-up 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 Start-up Mode.

3. Running 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.

Non Start-up Mode procedures:

1. Checking 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 octet by octet until difference is found.

+ If the S flag is set, then router does nothing.

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

The router changing its System ID advertises new LSPs based on the newly generated System ID to re-join the IS-IS auto-configuration network. The other SysID-duplicated router also MUST re-advertise its own LSP (after increasing the sequence number).

The newly generated System ID SHOULD perform duplication detection as well.

### 3.3.3. System ID and Router-Fingerprint Generation Considerations

As specified in this document, there are two distinguishing items that need to be self-generated: the System ID and Router-Fingerprint. In a network device, normally there are some resources which can 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(s) on an interface(s)

This document recommends the use of 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 hardware/software limitations and the lack of sufficient communication packets at the initial stage in home routers when doing ISIS auto-configuration. In this case, this document suggests using the MAC address as System ID and generating a pseudo-random number based on another seed (such as the memory address of a certain variable in the program) as the Router-Fingerprint. The pseudo-random number might not have a very high probability of uniqueness in this solution, but should be sufficient in home networks scenarios.

The considerations surrounding System ID stability described in section Section 3.2 also need to be applied.

#### 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 during the initial stages. 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 whereby 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 does not own, or IS neighbors that the router does not see), then per the 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 repeat the above behavior. After multiples iterations, the program should be able to deduce that double-duplication is occurring.

When this condition is detected, routers should have much more entropies available. Thus, the router is able 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

This section describes the TLVs that are necessary for 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 metrics 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 manually configured adjacencies over auto-configuringed.

### 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.

To guarantee the uniqueness of the host names, the System ID SHOULD be appended as a suffix in the names.

## 3.5. Routing Behavior Considerations

### 3.5.1. Adjacency Formation

Since IS-IS does not require strict hold timer 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 connection itself could be considered as an implicit authentication in that unwanted routers are usually not able to connect (i.e. there is some kind of physical security in place preventing the connection of rogue devices); for wireless deployment, the authentication could be achieved at the lower wireless link layer.

A malicious router could modify the System ID field to keep causing System ID duplication detection and resolution thus cause the routing system to oscillate. However, this is not a new attack vector as without this document the consequences would be higher as other routers would not have a mechanism to try and resolve this case.

## 5. IANA Considerations

IANA is kindly requested to assign a new TLV for the Router-Fingerprint from the IS-IS TLV Codepoint registry.

## 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 Thomann, 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

[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
Q10, Huawei Campus, No.156 Beiqing Road
Hai-Dian District, Beijing, 100095
P.R. China

Email: leo.liubing@huawei.com

Bruno Decraene
Orange
France

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