

isis
Internet-Draft
Intended status: Standards Track
Expires: November 10, 2017

B. Liu, Ed.
Huawei Technologies
L. Ginsberg
Cisco Systems
B. Decraene
Orange
I. Farrer
Deutsche Telekom AG
M. Abrahamsson
T-Systems
May 9, 2017

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

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, and so are suitable for networks where plug-and-play configuration is expected.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] when they appear in ALL CAPS. When these words are not in ALL CAPS (such as "should" or "Should"), they have their usual English meanings, and are not to be interpreted as [RFC2119] key words.

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 November 10, 2017.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	3
2. Scope	3
3. Protocol Specification	3
3.1. IS-IS Default Configuration	3
3.2. IS-IS NET Generation	4
3.3. Router-Fingerprint TLV	5
3.4. Protocol Operation	6
3.4.1. Start-Up mode	6
3.4.2. Adjacency Formation	7
3.4.3. IS-IS System ID Duplication Detection	7
3.4.4. Duplicate System ID Resolution Procedures	7
3.4.5. System ID and Router-Fingerprint Generation Considerations	8
3.4.6. Duplication of both System ID and Router-Fingerprint	9
3.5. Additional IS-IS TLVs Usage Guidelines	10
3.5.1. Authentication TLV	11
3.5.2. Metric Used in Reachability TLVs	11
3.5.3. Dynamic Host Name TLV	11
4. Security Considerations	11
5. IANA Considerations	11
6. Acknowledgements	12
7. References	12
7.1. Normative References	12
7.2. Informative References	13
Authors' Addresses	13

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 configuration.
2. IS-IS System ID self-generation.
3. System ID duplication detection and resolution.
4. ISIS TLV utilization (Authentication TLV, metrics in reachability advertisements, 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.

2. Scope

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

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

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

IS-IS auto-configuration is primarily intended for use in small (i.e. 10s of devices) and unmanaged deployments. It allows IS-IS to be used without the need for any configuration by the user. It is not recommended for larger deployments.

3. Protocol Specification

3.1. IS-IS Default Configuration

- 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.

- o IS-IS auto-configuration instances MUST be configured as level-1, so that the interfaces operate as level-1 only.
- o `originatingLSPBufferSize` is set to 512.
- o `MaxAreaAddresses` is set to 3
- o Extended IS Reachability and IP Reachability TLVs [RFC5305] MUST be used i.e. a router operating in auto configuration mode MUST NOT use any of the following TLVs:
 - * IS Neighbors (2)
 - * IP Internal Reachability (128)
 - * IP External Reachability (130)

TLVs listed above MUST be ignored on receipt.

3.2. IS-IS NET Generation

In IS-IS, a router (known as an Intermediate System) is identified by a Network Entity Title (NET) which is a type of Network Service Access Point (NSAP). The NET is the address of an instance of the IS-IS protocol running on an Intermediate System (IS).

The auto-configuration mechanism generates the IS-IS NET as the following:

- o Area address

In IS-IS auto-configuration, this field MUST be 13 octets long and set to 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 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. Changes such as interface enable/disable, interface

connect/disconnect, device reboot, firmware update, or configuration changes SHOULD NOT cause the system ID to change. System ID change as part of the System ID collision resolution process MUST be supported. Implementations SHOULD allow the System ID to be cleared by a user initiated system reset.

More specific considerations for System ID generation are described in Section 3.4.5.

3.3. Router-Fingerprint TLV

The Router-Fingerprint TLV is similar to the Router-Hardware-Fingerprint TLV defined in [RFC7503]. However, the TLV defined here includes a flags field to support indicating that the router is in Start-up mode and is operating in auto-configuration mode.

```

      0               1               2               3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|      Type      |      Length      |
+-----+-----+-----+-----+-----+-----+-----+-----+
|  Flags Field  |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     Router Fingerprint (Variable)
|                                     .
|                                     .
|                                     .
+-----+-----+-----+-----+-----+-----+-----+-----+

```

Type: to be assigned by IANA.

Length: the length of the value field. Must be >= 33.

Flags field (1 octet)

```

      0 1 2 3 4 5 6 7
+-----+-----+-----+
|S|A| Reserved |
+-----+-----+-----+

```

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: 32 or more octets.

More specific considerations for Router-Fingerprint are described in Section 3.4.5.

Router Fingerprint TLV MUST be included in Intermediate System to Intermediate System Hellos (IIHs) originated by a router operating in auto-configuration mode. An auto-configuration mode router MUST ignore IIHs that don't contain the Router Fingerprint TLV.

Router Fingerprint TLV MUST be included in Link State PDU (LSP) #0 originated by a router operating in auto-configuration mode. If an LSP #0 which does NOT contain a Router Fingerprint TLV is received by a Router operating in auto-configuration mode the LSP is flooded as normal, but the entire LSP set originated by the sending router MUST be ignored when running the Decision process.

The router fingerprint TLV MUST NOT be included in an LSP with a non-zero number and when received MUST be ignored.

3.4. Protocol Operation

This section describes the operation of a router supporting auto-configuration mode.

3.4.1. Start-Up mode

When a router starts operation in auto-configuration mode, both the S and A bits MUST be set in the Router Fingerprint TLV included in both hellos and LSP #0. During this mode only LSP #0 is generated and IS or IP/IPv6 reachability TLVs MUST NOT be included in LSP #0. A router remains in Start-up mode for a minimum period of time (recommended to be 1 minute). This time should be sufficient to bring up adjacencies to all expected neighbors. A router leaves Start-up mode once the minimum time has elapsed and full LSP database synchronization is achieved with all neighbors in the UP state.

When a router exits startup-mode it clears the S bit in Router Fingerprint TLVs it sends in hellos and LSP#0. The router MAY now advertise IS neighbor and IP/IPv6 prefix reachability in its LSPs and MAY generate LSPs with a non-zero number.

The purpose of Start-up Mode is to minimize the occurrence of System ID changes for a router once it has become fully operational. Any System ID change during Start-up mode will have minimal impact on a running network because while in Start-up mode the router is not yet being used for forwarding traffic.

3.4.2. Adjacency Formation

Routers operating in auto-configuration mode MUST NOT form adjacencies with routers which are NOT operating in auto-configuration mode. The presence of the Router Fingerprint TLV with the A bit set indicates the router is operating in auto-configuration mode.

NOTE: The use of the special area address of all 0's makes it unlikely that a router which is not operating in auto-configuration mode will be in the same area as a router operating in auto-configuration mode. However, the check for the Router Fingerprint TLV with A bit set provides additional protection.

3.4.3. IS-IS System ID Duplication Detection

The System ID of each node MUST be unique. As described in Section 3.4.5, 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. Duplicate System ID may occur between neighbors or between routers in the same area which are not neighbors.

Duplicate System ID with a neighbor is detected when the System ID received in an IIH is identical to the local System ID and the Router-Fingerprint in the received Router-Fingerprint TLV does NOT match the locally generated Router-Fingerprint.

Duplicate System ID with a non-neighbor is detected when an LSP #0 is received, the System ID of the originator is identical to the local System ID, and the Router-Fingerprint in the Router-Fingerprint TLV does NOT match the locally generated Router-Fingerprint.

3.4.4. Duplicate System ID Resolution Procedures

When duplicate System ID is detected one of the systems MUST assign itself a different System ID and perform a protocol restart. The resolution procedure attempts to minimize disruption to a running network by choosing a router which is in Start-up mode to be restarted whenever possible.

The contents of the Router-Fingerprint TLVs for the two routers with duplicate System IDs are compared.

If one TLV has the S bit set (router is in Start-up mode) and one TLV has the S bit clear (router is NOT in Start-up mode) the router in Start-up mode MUST generate a new System ID and restart the protocol.

If both TLVs have the S bit set (both routers are in Start-up mode) or both TLVs have the S bit clear (neither router is in Start-up mode) then the router with numerically smaller Router-Fingerprint MUST generate a new System ID and restart the protocol.

Fingerprint comparison is performed octet by octet starting from the first received octet until a difference is detected. If the fingerprints have different lengths and all octets up to the shortest length are identical then the fingerprint with smaller length is considered smaller.

If the fingerprints are identical in both content and length (and state of the S bit is identical) and the duplication is detected in hellos then the both routers MUST generate a new System ID and restart the protocol.

If fingerprints are identical in both content and length and the duplication is detected in LSP #0 then the procedures defined in Section 3.4.6 MUST be followed.

3.4.5. 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 (some examples listed below). These resources can be used as seeds to derive identifiers.

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

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.

3.4.6. Duplication of both System ID and Router-Fingerprint

As described above, the resources for generating System ID/Fingerprint might be very constrained during the initial stages. Hence, the duplication of both System ID and Router-Fingerprint needs to be considered. In such a case it is possible that a router will receive an LSP with System ID and Router-Fingerprint identical to the local values but the LSP is NOT identical to the locally generated copy i.e. sequence number is newer or sequence number is the same but the LSP has a valid checksum which does not match. The term DD-LSP is used to describe such an LSP.

In a benign case, this will occur if a router restarts and it receives copies of its own LSPs from its previous incarnation. This benign case needs to be distinguished from the pathological case where there are two different routers with the same System ID and the same Router-Fingerprint.

In the benign case, the restarting router will generate a new version of its own LSP with higher sequence number and flood the new LSP version. This will cause other routers in the network to update their LSPDB and synchronization will be achieved.

In the pathological case the generation of a new version of an LSP by one of the "twins" will cause the other twin to generate the same LSP with a higher sequence number - and oscillation will continue without achieving LSPDB synchronization.

Note that comparison of S bit in the Router-Fingerprint TLV cannot be performed as in the benign case it is expected that the S bit will be clear. Also note that the conditions for detecting duplicate System ID will NOT be satisfied because both the System ID and the Router-Fingerprint will be identical.

The following procedure is defined:

- DD-state is a boolean which indicates if a DD-LSP #0 has been received
- DD-count is the count of the number of occurrences of reception of a DD-LSP
- DD-timer is a timer associated with reception of DD-LSPs. Recommended value is 60 seconds.
- DD-max is the maximum number of DD-LSPs allowed to be received in DD-timer interval. Recommended value is 3.

When a DD-LSP is received:

- If DD-state is FALSE:
 - DD-state is set to TRUE
 - DD-timer is started
 - DD-count is initialized to 1.
- If DD-state is TRUE:
 - DD-count is incremented
 - If DD-count is \geq DD-max:
 - Local system MUST generate a new System ID and Router-Fingerprint and restart the protocol
 - DD-state is (re)initialized to FALSE and
 - DD-timer cancelled.
- If DD-timer expires:
 - DD-state is set to FALSE.

Note that to minimize the likelihood of duplication of both System ID and Router-fingerprint reoccurring, routers SHOULD have more entropies available. One simple way to achieve this is to add the LSP sequence number of the next LSP it will send to the Router-Fingerprint.

3.5. Additional IS-IS TLVs Usage Guidelines

This section describes the behavior of selected TLVs when used by a router supporting IS-IS auto-configuration.

3.5.1. Authentication TLV

It is RECOMMENDED that IS-IS routers supporting this specification offer an option to explicitly configure a single password for HMAC-MD5 authentication as specified in[RFC5304].

3.5.2. Metric Used in Reachability TLVs

It is RECOMMENDED that IS-IS auto-configuration routers use a high metric value (e.g. 100000) as default in order to allow manually configured adjacencies to be preferred over auto-configured.

3.5.3. Dynamic Host Name TLV

IS-IS auto-configuration routers MAY advertise their Dynamic Host Name TLV (TLV 137, [RFC5301]). The host name 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 name, the System ID SHOULD be appended as a suffix in the names.

4. Security Considerations

In the absence of cryptographic authentication it is possible for an attacker to inject a PDU falsely indicating there is a duplicate system-id. This may trigger automatic restart of the protocol using the duplicate-id resolution procedures defined in this document.

Note that the use of authentication is incompatible with auto-configuration as it requires some manual configuration.

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.

5. IANA Considerations

This document requires the definition of a new IS-IS TLV to be reflected in the "IS-IS TLV Codepoints" registry:

Type	Description	IIH	LSP	SNP	Purge
----	-----	---	---	---	-----
TBA	Router-Fingerprint	Y	Y	N	Y

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 [RFC7991].
(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 10589:2002, Second Edition.", Nov 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>>.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [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>>.

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>>.

[RFC7991] Hoffman, P., "The "xml2rfc" Version 3 Vocabulary",
RFC 7991, DOI 10.17487/RFC7991, December 2016,
<<http://www.rfc-editor.org/info/rfc7991>>.

Authors' Addresses

Bing Liu (editor)
Huawei Technologies
Q10, Huawei Campus, No.156 Beiqing Road
Hai-Dian District, Beijing, 100095
P.R. China

Email: leo.liubing@huawei.com

Les Ginsberg
Cisco Systems
821 Alder Drive
Milpitas CA 95035
USA

Email: ginsberg@cisco.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