Internet Engineering Task Force (IETF)
Request for Comments: 8196
Category: Standards Track
ISSN: 2070-1721

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

July 2017

IS-IS Autoconfiguration

Abstract

This document specifies IS-IS autoconfiguration mechanisms. The key components are IS-IS System ID self-generation, duplication detection, and duplication resolution. These mechanisms provide limited IS-IS functions and are therefore suitable for networks where plug-and-play configuration is expected.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc8196.

Table of Contents

1. Introduction

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

IS-IS autoconfiguration 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. IS-IS TLV utilization (authentication TLV, metrics in reachability advertisements, and Dynamic Name TLV)

This document also defines mechanisms to prevent the unintentional interoperation of autoconfigured routers with non-autoconfigured routers. See Section 3.3.

1.1. 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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here. 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.

2. Scope

The autoconfiguration mechanisms support both IPv4 and IPv6 deployments.

These autoconfiguration 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

IS-IS autoconfiguration 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

This section defines the default configuration for an autoconfigured router.

- IS-IS interfaces MUST be autoconfigured to an interface type corresponding to their Layer 2 capability. For example, Ethernet interfaces will be autoconfigured as broadcast networks and Point-to-Point Protocol (PPP) interfaces will be autoconfigured as Point-to-Point interfaces.

- IS-IS autoconfiguration instances MUST be configured as level-1 so that the interfaces operate as level-1 only.

- originatingLSPBufferSize is set to 512.

- MaxAreaAddresses is set to 3.

- Extended IS reachability (TLV 22) and IP reachability (TLV 135) TLVs [RFC5305] MUST be used, i.e., a router operating in autoconfiguration mode MUST NOT use any of the following TLVs:

  * IIS Neighbors (TLV 2)

  * IP Int. Reach (TLV 128)

  * IP Ext. Address (TLV 130)

  The 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 IS.

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

- Area address

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

- 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:

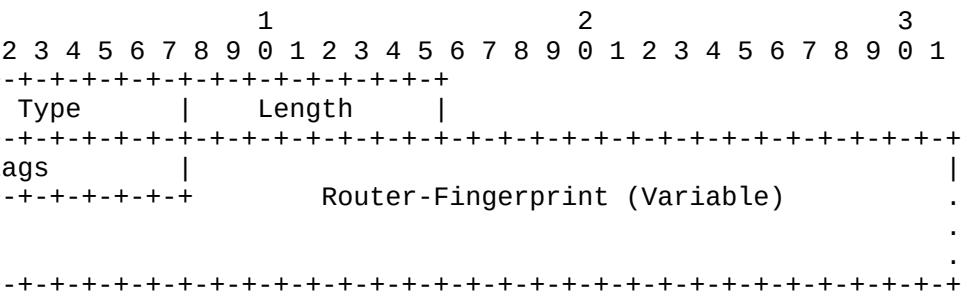
  - As specified by the IS-IS protocol, this field must be unique among all routers in the same area.

  - 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

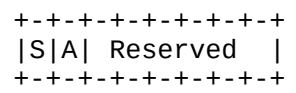
The Router-Fingerprint TLV is similar to the Router-Hardware-Fingerprint TLV defined in [RFC7503]. However, the TLV defined here includes a Flags field to support indicating that the router is in startup mode and is operating in autoconfiguration mode.



Type: 15.

Length: The length, in octets, of the "Flags" and "Router-Fingerprint" fields.

Flags: 1 octet.



S flag: When set, indicates the router is in "startup" mode.

A flag: When set, indicates that the router is operating in autoconfiguration mode. The purpose of the flag is so that two routers can identify if they are both using autoconfiguration. If the A flag setting does not match in hellos, then no adjacency should be formed.

Reserved: These flags 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.

The Router-Fingerprint TLV with the A flag set MUST be included in IS-IS Hellos (IIHs) originated by a router operating in autoconfiguration mode. An autoconfiguration mode router MUST ignore IIHs that don't contain the Router-Fingerprint TLV with the A flag set.

The Router-Fingerprint TLV with the A flag set MUST be included in Link State PDU (LSP) #0 originated by a router operating in autoconfiguration mode. If an LSP #0 is received by a router operating in autoconfiguration mode and the LSP either does NOT contain a Router-Fingerprint TLV or it does contain a Router-Fingerprint TLV but the A flag is NOT set, then 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 autoconfiguration mode.

3.4.1. Startup Mode

When a router starts operation in autoconfiguration mode, both the S and A flags 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 startup 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 startup 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 flag in Router-Fingerprint TLVs that it sends in hellos and LSP #0. The router MAY now advertise the IS neighbor and IP/IPv6 prefix reachability in its LSPs and MAY generate LSPs with a non-zero number.

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

3.4.2. Adjacency Formation

Routers operating in autoconfiguration mode MUST NOT form adjacencies with routers that are NOT operating in autoconfiguration mode. The presence of the Router-Fingerprint TLV with the A flag set indicates the router is operating in autoconfiguration mode.

NOTE: The use of the special area address of all 0s makes it unlikely that a router that is not operating in autoconfiguration mode will be in the same area as a router operating in autoconfiguration mode. However, the check for the Router-Fingerprint TLV with the A flag 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., Media Access Control (MAC) address) that 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. A duplicate system ID may occur between neighbors or between routers in the same area that are not neighbors.

A 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.

A 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 a 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, whenever possible, to restart a router that is in startup mode.

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

If one TLV has the S flag set (the router is in startup mode) and one TLV has the S flag clear (the router is NOT in startup mode), the router in startup mode MUST generate a new System ID and restart the protocol.

If both TLVs have the S flag set (both routers are in startup mode) or both TLVs have the S flag clear (neither router is in startup mode), then the router with the 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 on the whole.

If the fingerprints are identical in both content and length (and the state of the S flag is identical), and the duplication is detected in hellos, then 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 that can provide an extremely high probability of uniqueness (some examples listed below). These resources can be used as seeds to derive identifiers:

- 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 regenerate the System ID when duplication happens.

This document also does not specify a 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 IS-IS autoconfiguration. In this case, this document suggests using the MAC address as the System ID and generating a pseudorandom number based on another seed (such as the memory address of a certain variable in the program) as the Router-Fingerprint. The pseudorandom number might not have a very high probability of uniqueness in this solution but should be sufficient in home network scenarios.

The considerations surrounding System ID stability described in 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 a System ID / Router-Fingerprint might be very constrained during the initial stages. Hence, the duplication of both System ID and Router-Fingerprint need to be considered. In such a case, it is possible that a router will receive an LSP with a System ID and Router-Fingerprint identical to the local values, but the LSP is NOT identical to the locally generated copy, i.e., the sequence number is newer or the sequence number is the same, but the LSP has a valid checksum that does not match. The term DD-LSP (Duplication Detection 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 a higher sequence number and flood the new LSP version. This will cause other routers in the network to update their LSP Database (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 a comparison of the S flag in the Router-Fingerprint TLV cannot be performed, as in the benign case it is expected that the S flag will be clear. Also note that the conditions for detecting a 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 that 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; the recommended value is 60 seconds.
    DD-max is the maximum number of DD-LSPs allowed
     to be received in DD-timer interval;
     the 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 >= DD-max:
       The 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 is canceled.

  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 autoconfiguration.

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 autoconfiguration routers use a high metric value (e.g., 100000) as default in order to allow manually configured adjacencies to be preferred over autoconfigured.

3.5.3. Dynamic Name TLV

IS-IS autoconfiguration routers MAY advertise their Dynamic Name TLV (TLV 137 [RFC5301]). The hostname 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 hostname, 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 autoconfiguration 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 details a new IS-IS TLV reflected in the "IS-IS TLV Codepoints" registry:

Value	Name	IIH	LSP	SNP	Purge
15	Router-Fingerprint	Y	Y	N	Y

6. References

6.1. Normative References

[ISO_IEC10589] International Organization for Standardization, "Information technology -- Telecommunications and information exchange between systems -- 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, 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>.

[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>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <http://www.rfc-editor.org/info/rfc8174>.

6.2. 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>.

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.

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
United States of America

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