Network Working Group B. Liu
Internet Draft Huawei Technologies
Intended status: Standards Track Bruno Decraene
Expires: March 6, 2015 Orange
I. Farrer
Deutsche Telekom AG
M. Abrahamsson
T-System
September 3, 2014

ISIS Auto-Configuration
draft-liu-isis-auto-conf-02.txt

Status of this Memo

Copyright Notice0

Abstract

This document describes mechanisms for IS-IS to be self-configuring. Such mechanisms could reduce the management burden to configure a network. One obvious environment that could benefit from these mechanisms is IPv6 home network where plug-and-play would be expected. Besides home network, some simple enterprise/ISP networks might also benefit from the self-configuring mechanisms.

Table of Contents

1. Introduction

This memo describes mechanisms for IS-IS [RFC1195][RFC5308] to be auto-configuring. Such mechanisms could reduce the management burden to configure a network. One example is home network where plug-and-play would be expected. Besides home network, some simple enterprise/ISP networks might also potentially benefit from the auto-configuring mechanisms.

In addition, this memo defines how such un-configured routers should behave, also limits the risk on existing network using IS-IS (Setcion 3.4 & 3.5).

IS-IS auto-configuration mainly contains the following aspects:

1. IS-IS Default Configuration

2. IS-IS NET self-generation

3. NET duplication detection and resolution

4. Authentication and Wide Metric TLV

2. Design Scope

The auto-configuring mechanisms are not specifically designed based on IPv4 or IPv6.

The auto-configuring mechanisms enabled interfaces are assumed to have a 48-bit MAC address.

The main targeted application scenarios are supposed to be home networks or small enterprise networks .etc. where plug-n-play is expected and complex topology/hierarchy is not needed. Sophisticate requirements from service provider networks are out of scope.

So this document does not provide a complete configuration-free alternative to the IS-IS protocol. The following features of IS-IS are NOT supported by this document:

o Auto-configuring multiple IS-IS processes. The auto-configuration mechanisms only support configuring a single process.

o Route between multiple IS-IS areas. The auto-configuration mechanisms only support routers that are within a single area.

o Auto-configuring multiple operation levels. The auto-configuration mechanisms only support level-1 operation mode.

o This document does not consider interoperability with other routing protocols.

3. Protocol Specification

3.1. IS-IS Default Configuration

o IS-IS SHOULD be enabled on all interfaces in a router that requires the IS-IS auto-configuration as default. For some specific situations, interface MAY be excluded if it is a clear that running IS-IS on the interface is not required.

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 interfaces MUST be configured with level-1.

3.2. IS-IS NET Generation

In IS-IS, a router (known as an IS) is identified by an Network Entity Title (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:

Area address: This field is 1 to 13 octets in length. In IS-IS auto-configuring, this field MUST be 0 in 13 octets length.

System ID: This field follows the area address field, and is 6 octets in length. As specified in IS-IS protocol, this field must be unique among all level-1 routers in the same area when the IS operates at Level 1. In IS-IS auto-configuring, this field SHOULD be the MAC address of one IS-IS enabled interface.

NSEL: This field is the N-selector, and is 1 octet in length. In IS-IS auto-configuring, it must be set to "00".

3.3. IS-IS NET Duplication Detection and Resolution

As described in Section 3, in IS-IS auto-configuring the NETs are distinguished by the System ID field in which it is a MAC address. So for IS-IS neighbors' NET duplication, it is equal to MAC address duplication in a LAN, which means a serious problem that devices need to be changed. So the NET duplication detection and resolution mechanism is actually used between non-neighbors which are within the same IS-IS area.

The rational of IS-IS NET duplication detection and resolution is described as the following.

3.3.1. Router-Hardware-Fingerprint TLV

The Router-Hardware-Fingerprint TLV is defined in [OSPFv3AC]. This document re-uses it to achieve NET duplication detection.

```
 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     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Router Hardware Fingerprint (Variable)               |
.                                                               .
.                                                               .
.                                                               .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1 Router-Hardware-Fingerprint TLV Format

As defined in [OSPFv3AC], the contents of the hardware fingerprint should be some combination of CPU ID, or serial number(s) that provides an extremely high probability of uniqueness. It MUST be based on hardware attributes that will not change across hard and soft restarts. The length of the Router-Hardware-Fingerprint is variable but must be 32 octets or greater.

Note that, since the TLV is to detect MAC address based NET duplication, the TLV content MUST NOT only use MAC address. MAC address plus other information are also not recommended to use.

3.3.2. NET Duplication Detection and Resolution Procedures

1) Flood the Router-Hardware-Fingerprint TLVs

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

An IS-IS auto-configuring router MUST compare a received self-originated LSP's Router-Hardware-Fingerprint TLV against its own one. If they are equal, it means the LSP was indeed originated by the router itself; if they are not equal, it means some other router has the same NET originated the LSP, thus there is a NET duplication.

3) Duplication resolution

When NET duplication occurs, the router with the numerically smaller router hardware fingerprint MUST generate a new NET.

4) Purge the LSPs containing duplicated NET

Before flooding the new NET, the LSP with the prior duplicate NET MUST be purged. And any IS-IS neighbor adjacencies MUST be reestablished.

5) Re-join the network with the new NET

After purging the LSPs with the duplicated NET, the router re-join the IS-IS auto-configuration network with the newly generated NET.

3.4. 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 because a low end CPE joining an existing IS-IS network might seriously break it or cause unnecessary management confusion.

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.

3.5. Wide Metric

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.

3.6. Adjacency Formation Consideration

ISIS does not require strict hold timers matching to form adjacency. But a reasonable range might be needed. Whether we need to specify a best practice timers in ISIS-AC is an open question.[TBD].

4. Co-existence 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, it is not proper to specify choice/interaction of multiple IGPs in any standalone IGP auto-configuration protocols. It should be done in the CPE level. Currently, there is some relevant work emerging, for example, the suggestion from [HOMENET-HNCP] is to have the proposed HNCP (Home Network Control Protocol) choose what IGP should be used.

5. Security Considerations

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 SystemID field to cause NET duplication detection and resolution vibrate thus cause the routing system vibrate.

6. IANA Considerations

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

7. Acknowledgments

Many useful comments and contributions were made by Sheng Jiang.

This document was inspired by [OSPFv3AC].

8. References

8.1. Normative References

[RFC1195] Callon, R., "Use of OSI IS-IS for routing in TCP/IP and dual environments", RFC 1195, December 1990.

[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.

8.2. Informative References

[OSPFv3AC]Lindem, A., and J. Arkko, "OSPFv3 Auto-Configuration", Work in Progress, October 2013

[HOMENET-HNCP]
Stenberg, M., and S. Barth, "Home Networking Control Protocol", Work in Progress, February 05

Authors' Addresses

Bing Liu
Huawei Technologies Co., Ltd
Q14, Huawei Campus
No.156 Beiqing Rd.
Hai-Dian District, Beijing 100095
P.R. China

Email: leo.liubing@huawei.com

Bruno Decraene
Orange
Issy-les-Moulineaux
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