Internet Engineering Task Force (IETF)
Request for Comments: 8500
Category: Standards Track
ISSN: 2070-1721
N. Shen
Cisco Systems
S. Amante
Apple Inc.
M. Abrahamsson
T-Systems Nordic
February 2019

IS-IS Routing with Reverse Metric

Abstract

This document describes a mechanism to allow IS-IS routing to quickly and accurately shift traffic away from either a point-to-point or multi-access LAN interface during network maintenance or other operational events. This is accomplished by signaling adjacent IS-IS neighbors with a higher reverse metric, i.e., the metric towards the signaling IS-IS router.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The IS-IS [ISO10589] routing protocol has been widely used in Internet Service Provider IP/MPLS networks. Operational experience with the protocol combined with ever increasing requirements for lossless operations have demonstrated some operational issues. This document describes the issues and a mechanism for mitigating them.

This document defines the IS-IS "Reverse Metric" mechanism that allows an IS-IS node to send a Reverse Metric TLV through the IS-IS Hello (IIH) PDU to the neighbor or pseudonode to adjust the routing metric on the inbound direction.

1.1. Node and Link Isolation

The IS-IS routing mechanism has the overload bit, which can be used by operators to perform disruptive maintenance on the router. But in many operational maintenance cases, it is not necessary to divert all the traffic away from this node. It is necessary to avoid only a single link during the maintenance. More detailed descriptions of the challenges can be found in Appendices A and B of this document.

1.2. Distributed Forwarding Planes

In a distributed forwarding platform, different forwarding line cards may have interfaces and IS-IS connections to neighbor routers. If one of the line card's software resets, it may take some time for the forwarding entries to be fully populated on the line card, in particular if the router is a PE (Provider Edge) router in an ISP's MPLS VPN. An IS-IS adjacency may be established with a neighbor router long before the entire BGP VPN prefixes are downloaded to the forwarding table. It is important to signal to the adjacent IS-IS routers to raise metric values and not to use the corresponding IS-IS adjacency inbound to this router if possible. Temporarily signaling the 'Reverse Metric' over this link to discourage the traffic via the corresponding line card will help to reduce the traffic loss in the network. In the meantime, the remote PE routers will select a different set of PE routers for the BGP best path calculation or use a different link towards the same PE router on which a line card is resetting.

1.3. Spine-Leaf Applications

In the IS-IS Spine-Leaf extension [IS-IS-SL-EXT], the leaf nodes will perform equal-cost or unequal-cost load sharing towards all the spine nodes. In certain operational cases, for instance, when one of the backbone links on a spine node is congested, a spine node can push a higher metric towards the connected leaf nodes to reduce the transit traffic through the corresponding spine node or link.

1.4. LDP IGP Synchronization

In [RFC5443], a mechanism is described to achieve LDP IGP synchronization by using the maximum link metric value on the interface. But in the case of a new IS-IS node joining the broadcast network (LAN), it is not optimal to change all the nodes on the LAN to the maximum link metric value, as described in [RFC6138]. In this case, the Reverse Metric can be used to discourage both outbound and inbound traffic without affecting the traffic of other IS-IS nodes on the LAN.

1.5. IS-IS Reverse Metric

This document uses the routing protocol itself as the transport mechanism to allow one IS-IS router to advertise a "reverse metric" in an IS-IS Hello (IIH) PDU to an adjacent node on a point-to-point or multi-access LAN link. This would allow the provisioning to be performed only on a single node, setting a "reverse metric" on a link and having traffic bidirectionally shift away from that link gracefully to alternate viable paths.

This Reverse Metric mechanism is used for both point-to-point and multi-access LAN links. Unlike the point-to-point links, the IS-IS protocol currently does not have a way to influence the traffic towards a particular node on LAN links. This mechanism provides IS-IS routing with the capability of altering traffic in both directions on either a point-to-point link or a multi-access link of an IS-IS node.

The metric value in the Reverse Metric TLV and the Traffic Engineering metric in the sub-TLV being advertised are offsets or relative metrics to be added to the existing local link and Traffic Engineering metric values of the receiver; the accumulated metric value is bounded as described in Section 2.

1.6. Specification of Requirements

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.

2. IS-IS Reverse Metric TLV

The Reverse Metric TLV is a new TLV to be used inside an IS-IS Hello PDU. This TLV is used to support the IS-IS Reverse Metric mechanism that allows a "reverse metric" to be sent to the IS-IS neighbor.

```
 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     |     Metric
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      Metric  (Continued)       | sub-TLV Len   |Optional sub-TLV
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1: Reverse Metric TLV

The Value part of the Reverse Metric TLV is composed of a 3 octet field containing an IS-IS Metric value, a 1 octet field of Flags, and a 1 octet Reverse Metric sub-TLV length field representing the length of a variable number of sub-TLVs. If the "sub-TLV Len" is non-zero, then the Value field MUST also contain one or more sub-TLVs.

The Reverse Metric TLV MAY be present in any IS-IS Hello PDU. A sender MUST only transmit a single Reverse Metric TLV in an IS-IS Hello PDU. If a received IS-IS Hello PDU contains more than one

Reverse Metric TLV, an implementation MUST ignore all the Reverse Metric TLVs.

TYPE: 16
LENGTH: variable (5 - 255 octets)
VALUE:

Flags (1 octet)
Metric (3 octets)
sub-TLV length (1 octet)
sub-TLV data (0 - 250 octets)

```
 0 1 2 3 4 5 6 7
+-+-+-+-+-+-+-+-+
|  Reserved |U|W|
+-+-+-+-+-+-+-+-+
```

Figure 2: Flags

The Metric field contains a 24-bit unsigned integer. This value is a metric offset that a neighbor SHOULD add to the existing configured Default Metric for the IS-IS link [ISO10589]. Refer to "Elements of Procedure" in Section 3 of this document for details on how an IS-IS router should process the Metric field in a Reverse Metric TLV.

The Metric field, in the Reverse Metric TLV, is a "reverse offset metric" that will either be in the range of 0 - 63 when a "narrow" IS-IS metric is used (IS Neighbors TLV / Pseudonode LSP) [RFC1195] or in the range of 0 - (2^24 - 2) when a "wide" Traffic Engineering metric value is used (Extended IS Reachability TLV) [RFC5305] [RFC5817]. As described below, when the U bit is set, the accumulated value of the wide metric is in the range of 0 - (2^24 - 1), with the (2^24 - 1) metric value as non-reachable in IS-IS routing. The IS-IS metric value of (2^24 - 2) serves as the link of last resort.

There are currently only two Flag bits defined.

W bit (0x01): The "Whole LAN" bit is only used in the context of multi-access LANs. When a Reverse Metric TLV is transmitted from a node to the Designated Intermediate System (DIS), if the "Whole LAN" bit is set (1), then a DIS SHOULD add the received Metric value in the Reverse Metric TLV to each node's existing Default Metric in the Pseudonode LSP. If the "Whole LAN" bit is not set (0), then a DIS SHOULD add the received Metric value in the Reverse Metric TLV to the existing "default metric" in the Pseudonode LSP for the single node from whom the Reverse Metric TLV was received. Please refer to "Multi-access LAN Procedures", in Section 3.3, for additional details. The W bit MUST be clear when a Reverse Metric TLV is transmitted in an IIH PDU on a point-to-point link and MUST be ignored when received on a point-to-point link.

U bit (0x02): The "Unreachable" bit specifies that the metric calculated by the addition of the reverse metric to the "default metric" is limited to the maximum value of (2^24-1). This "U" bit applies to both the default metric in the Extended IS Reachability TLV and the Traffic Engineering Default Metric sub-TLV of the link. This is only relevant to the IS-IS "wide" metric mode.

The Reserved bits of Flags field MUST be set to zero and MUST be ignored when received.

The Reverse Metric TLV MAY include sub-TLVs when an IS-IS router wishes to signal additional information to its neighbor. In this document, the Reverse Metric Traffic Engineering Metric sub-TLV, with Type 18, is defined. This Traffic Engineering Metric contains a 24-bit unsigned integer. This sub-TLV is optional; if it appears more than once, then the entire Reverse Metric TLV MUST be ignored. Upon receiving this Traffic Engineering METRIC sub-TLV in a Reverse Metric TLV, a node SHOULD add the received Traffic Engineering Metric offset value to its existing configured Traffic Engineering Default Metric within its Extended IS Reachability TLV. The use of other sub-TLVs is outside the scope of this document. The "sub-TLV Len" value MUST be set to zero when an IS-IS router does not have Traffic Engineering sub-TLVs that it wishes to send to its IS-IS neighbor.

3. Elements of Procedure

3.1. Processing Changes to Default Metric

It is important to use the same IS-IS metric type on both ends of the link and in the entire IS-IS area or level. On the receiving side of the 'reverse-metric' TLV, the accumulated value of the configured metric and the reverse-metric needs to be limited to 63 in "narrow" metric mode and to (2^24 - 2) in "wide" metric mode. This applies to both the Default Metric of Extended IS Reachability TLV and the Traffic Engineering Default Metric sub-TLV in LSP or Pseudonode LSP for the "wide" metric mode case. If the "U" bit is present in the flags, the accumulated metric value is to be limited to (2^24 - 1) for both the normal link metric and Traffic Engineering metric in IS-IS "wide" metric mode.

If an IS-IS router is configured to originate a Traffic Engineering Default Metric sub-TLV for a link but receives a Reverse Metric TLV from its neighbor that does not contain a Traffic Engineering Default

Metric sub-TLV, then the IS-IS router MUST NOT change the value of its Traffic Engineering Default Metric sub-TLV for that link.

3.2. Multi-Topology IS-IS Support on Point-to-Point Links

The Reverse Metric TLV is applicable to Multi-topology IS-IS (M-ISIS) [RFC5120]. On point-to-point links, if an IS-IS router is configured for M-ISIS, it MUST send only a single Reverse Metric TLV in IIH PDUs toward its neighbor(s) on the designated link. When an M-ISIS router receives a Reverse Metric TLV, it MUST add the received Metric value to its Default Metric of the link in all Extended IS Reachability TLVs for all topologies. If an M-ISIS router receives a Reverse Metric TLV with a Traffic Engineering Default Metric sub-TLV, then the M-ISIS router MUST add the received Traffic Engineering Default Metric value to each of its Default Metric sub-TLVs in all of its MT Intermediate Systems TLVs. If an M-ISIS router is configured to advertise Traffic Engineering Default Metric sub-TLVs for one or more topologies but does not receive a Traffic Engineering Default Metric sub-TLV in a Reverse Metric TLV, then the M-ISIS router MUST NOT change the value in each of the Traffic Engineering Default Metric sub-TLVs for all topologies.

3.3. Multi-access LAN Procedures

On a Multi-access LAN, only the DIS SHOULD act upon information contained in a received Reverse Metric TLV. All non-DIS nodes MUST silently ignore a received Reverse Metric TLV. The decision process of the routers on the LAN MUST follow the procedure in Section 7.2.8.2 of [ISO10589], and use the "Two-way connectivity check" during the topology and route calculation.

The Reverse Metric Traffic Engineering sub-TLV also applies to the DIS. If a DIS is configured to apply Traffic Engineering over a link and it receives Traffic Engineering Metric sub-TLV in a Reverse Metric TLV, it should update the Traffic Engineering Default Metric sub-TLV value of the corresponding Extended IS Reachability TLV or insert a new one if not present.

In the case of multi-access LANs, the "W" Flags bit is used to signal from a non-DIS to the DIS whether or not to change the metric and, optionally, Traffic Engineering parameters for all nodes in the Pseudonode LSP or solely the node on the LAN originating the Reverse Metric TLV.

A non-DIS node, e.g., Router B, attached to a multi-access LAN will send the DIS a Reverse Metric TLV with the W bit clear when Router B wishes the DIS to add the Metric value to the Default Metric contained in the Pseudonode LSP specific to just Router B. Other non-DIS nodes, e.g., Routers C and D, may simultaneously send a Reverse Metric TLV with the W bit clear to request the DIS to add their own Metric value to their Default Metric contained in the Pseudonode LSP.

As long as at least one IS-IS node on the LAN sending the signal to DIS with the W bit set, the DIS would add the metric value in the Reverse Metric TLV to all neighbor adjacencies in the Pseudonode LSP, regardless if some of the nodes on the LAN advertise the Reverse Metric TLV without the W bit set. The DIS MUST use the reverse metric of the highest source MAC address Non-DIS advertising the Reverse Metric TLV with the W bit set.

Local provisioning on the DIS to adjust the Default Metric(s) is another way to insert Reverse Metric in the Pseudonode LSP towards an IS-IS node on a LAN. In the case where a Reverse Metric TLV is also used in the IS-IS Hello PDU of the node, the local provisioning MUST take precedence over received Reverse Metric TLVs. For instance, local policy on the DIS may be provisioned to ignore the W bit signaling on a LAN.

Multi-topology IS-IS [RFC5120] specifies there is no change to construction of the Pseudonode LSP regardless of the Multi-topology (MT) capabilities of a multi-access LAN. If any MT capable node on the LAN advertises the Reverse Metric TLV to the DIS, the DIS should update, as appropriate, the Default Metric contained in the Pseudonode LSP. If the DIS updates the Default Metric and floods a new Pseudonode LSP, those default metric values will be applied to all topologies during Multi-topology Shortest Path First calculations.

3.4. LDP/IGP Synchronization on LANs

As described in [RFC6138], when a new IS-IS node joins a broadcast network, it is unnecessary and sometimes even harmful for all IS-IS nodes on the LAN to advertise the maximum link metric. [RFC6138] proposes a solution to have the new node not advertise its adjacency towards the pseudonode when it is not in a "cut-edge" position.

With the introduction of Reverse Metric in this document, a simpler alternative solution to the above mentioned problem can be used. The Reverse Metric allows the new node on the LAN to advertise its inbound metric value to be the maximum, and this puts the link of this new node in the last resort position without impacting the other IS-IS nodes on the same LAN.

Specifically, when IS-IS adjacencies are being established by the new node on the LAN, besides setting the maximum link metric value (2^24 - 2) on the interface of the LAN for LDP IGP synchronization as described in [RFC5443], it SHOULD advertise the maximum metric offset value in the Reverse Metric TLV in its IIH PDU sent on the LAN. It SHOULD continue this advertisement until it completes all the LDP label binding exchanges with all the neighbors over this LAN, either by receiving the LDP End-of-LIB [RFC5919] for all the sessions or by exceeding the provisioned timeout value for the node LDP/IGP synchronization.

3.5. Operational Guidelines

For the use case in Section 1.1, a router SHOULD limit the period of advertising a Reverse Metric TLV towards a neighbor only for the duration of a network maintenance window.

The use of a Reverse Metric does not alter IS-IS metric parameters stored in a router's persistent provisioning database.

If routers that receive a Reverse Metric TLV send a syslog message or SNMP trap, this will assist in rapidly identifying the node in the network that is advertising an IS-IS metric or Traffic Engineering parameters different from that which is configured locally on the device.

When the link Traffic Engineering metric is raised to (2^24 - 1) [RFC5817], either due to the Reverse Metric mechanism or by explicit user configuration, this SHOULD immediately trigger the CSPF (Constrained Shortest Path First) recalculation to move the Traffic Engineering traffic away from that link. It is RECOMMENDED also that the CSPF does the immediate CSPF recalculation when the Traffic Engineering metric is raised to (2^24 - 2) to be the last resort link.

It is advisable that implementations provide a configuration capability to disable any IS-IS metric changes by a Reverse Metric mechanism through neighbors' Hello PDUs.

If an implementation enables this mechanism by default, it is RECOMMENDED that it be disabled by the operators when not explicitly using it.

4. Security Considerations

Security concerns for IS-IS are addressed in [ISO10589], [RFC5304], [RFC5310], and with various deployment and operational security considerations in [RFC7645]. The enhancement in this document makes it possible for one IS-IS router to manipulate the IS-IS Default Metric and, optionally, Traffic Engineering parameters of adjacent IS-IS neighbors on point-to-point or LAN interfaces. Although IS-IS routers within a single Autonomous System nearly always are under the control of a single administrative authority, it is highly recommended that operators configure authentication of IS-IS PDUs to mitigate use of the Reverse Metric TLV as a potential attack vector.

5. IANA Considerations

IANA has allocated IS-IS TLV Codepoint 16 for the Reverse Metric TLV. This new TLV has the following attributes: IIH = y, LSP = n, SNP = n, Purge = n.

This document also introduces a new registry for sub-TLVs of the Reverse Metric TLV. The registration policy is Expert Review as defined in [RFC8126]. This registry is part of the "IS-IS TLV Codepoints" registry. The name of the registry is "Sub-TLVs for TLV 16 (Reverse Metric TLV)". The defined values are:

0:	Reserved
1-17:	Unassigned
18:	Traffic Engineering Metric as specified in this document (Section 2)
19-255:	Unassigned

6. References

6.1. Normative References

[ISO10589] ISO, "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, <https://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, <https://www.rfc-editor.org/info/rfc2119>.

[RFC5120] Przygienda, T., Shen, N., and N. Sheth, "M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)", RFC 5120, DOI 10.17487/RFC5120, February 2008, <https://www.rfc-editor.org/info/rfc5120>.

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

[RFC5443] Jork, M., Atlas, A., and L. Fang, "LDP IGP Synchronization", RFC 5443, DOI 10.17487/RFC5443, March 2009, <https://www.rfc-editor.org/info/rfc5443>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

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

6.2. Informative References

[IS-IS-SL-EXT] Shen, N., Ginsberg, L., and S. Thyamagundalu, "IS-IS Routing for Spine-Leaf Topology", Work in Progress, draft-ietf-lsr-isis-spine-leaf-ext-00, December 2018.

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

[RFC5310] Bhatia, M., Manral, V., Li, T., Atkinson, R., White, R., and M. Fanto, "IS-IS Generic Cryptographic Authentication", RFC 5310, DOI 10.17487/RFC5310, February 2009, <https://www.rfc-editor.org/info/rfc5310>.

[RFC5817] Ali, Z., Vasseur, JP., Zamfir, A., and J. Newton, "Graceful Shutdown in MPLS and Generalized MPLS Traffic Engineering Networks", RFC 5817, DOI 10.17487/RFC5817, April 2010, <https://www.rfc-editor.org/info/rfc5817>.

[RFC5919] Asati, R., Mohapatra, P., Chen, E., and B. Thomas, "Signaling LDP Label Advertisement Completion", RFC 5919, DOI 10.17487/RFC5919, August 2010, <https://www.rfc-editor.org/info/rfc5919>.

[RFC6138] Kini, S., Ed. and W. Lu, Ed., "LDP IGP Synchronization for Broadcast Networks", RFC 6138, DOI 10.17487/RFC6138, February 2011, <https://www.rfc-editor.org/info/rfc6138>.

[RFC7645] Chunduri, U., Tian, A., and W. Lu, "The Keying and Authentication for Routing Protocol (KARP) IS-IS Security Analysis", RFC 7645, DOI 10.17487/RFC7645, September 2015, <https://www.rfc-editor.org/info/rfc7645>.

Appendix A. Node Isolation Challenges

On rare occasions, it is necessary for an operator to perform disruptive network maintenance on an entire IS-IS router node, i.e., major software upgrades, power/cooling augments, etc. In these cases, an operator will set the IS-IS Overload Bit (OL bit) within the Link State Protocol Data Units (LSPs) of the IS-IS router about to undergo maintenance. The IS-IS router immediately floods its updated LSPs to all IS-IS routers in the IS-IS domain. Upon receipt of the updated LSPs, all IS-IS routers recalculate their Shortest Path First (SPF) tree excluding IS-IS routers whose LSPs have the OL bit set. This effectively removes the IS-IS router about to undergo maintenance from the topology, thus preventing it from receiving any transit traffic during the maintenance period.

After the maintenance activity has completed, the operator resets the IS-IS Overload Bit within the LSPs of the original IS-IS router causing it to flood updated IS-IS LSPs throughout the IS-IS domain. All IS-IS routers recalculate their SPF tree and now include the original IS-IS router in their topology calculations, allowing it to be used for transit traffic again.

Isolating an entire IS-IS router from the topology can be especially disruptive due to the displacement of a large volume of traffic through an entire IS-IS router to other suboptimal paths (e.g., those with significantly larger delay). Thus, in the majority of network maintenance scenarios, where only a single link or LAN needs to be augmented to increase its physical capacity, or is experiencing an intermittent failure, it is much more common and desirable to gracefully remove just the targeted link or LAN from service temporarily, so that the least amount of user-data traffic is affected during the link-specific network maintenance.

Appendix B. Link Isolation Challenges

Before network maintenance events are performed on individual physical links or LANs, operators substantially increase the IS-IS metric simultaneously on both devices attached to the same link or LAN. In doing so, the devices generate new Link State Protocol Data Units (LSPs) that are flooded throughout the network and cause all routers to gradually shift traffic onto alternate paths with very little or no disruption to in-flight communications by applications or end users. When performed successfully, this allows the operator to confidently perform disruptive augmentation, fault diagnosis, or repairs on a link without disturbing ongoing communications in the network.

There are a number of challenges with the above solution. First, it is quite common to have routers with several hundred interfaces and individual interfaces that move anywhere from several hundred gigabits/second to terabits/second of traffic. Thus, it is imperative that operators accurately identify the same point-to-point link on two separate devices in order to increase (and afterward decrease) the IS-IS metric appropriately. Second, the aforementioned solution is very time-consuming and even more error-prone to perform when it's necessary to temporarily remove a multi-access LAN from the network topology. Specifically, the operator needs to configure ALL devices that have interfaces attached to the multi-access LAN with an appropriately high IS-IS metric (and then decrease the IS-IS metric to its original value afterward). Finally, with respect to multi-access LANs, there is currently no method to bidirectionally isolate only a single node's interface on the LAN when performing more fine-grained diagnoses and repairs to the multi-access LAN.

In theory, use of a Network Management System (NMS) could improve the accuracy of identifying the appropriate subset of routers attached to either a point-to-point link or a multi-access LAN. It could also signal to those devices, using a network management protocol, to adjust the IS-IS metrics on the pertinent set of interfaces. The reality is that NMSs are, to a very large extent, not used within Service Provider's networks for a variety of reasons. In particular, NMSs do not interoperate very well across different vendors or even separate platform families within the same vendor.

Acknowledgments

The authors would like to thank Mike Shand, Dave Katz, Guan Deng, Ilya Varlashkin, Jay Chen, Les Ginsberg, Peter Ashwood-Smith, Uma Chunduri, Alexander Okonnikov, Jonathan Harrison, Dave Ward, Himanshu Shah, Wes George, Danny McPherson, Ed Crabbe, Russ White, Robert Raszuk, Tom Petch, Stewart Bryant, and Acee Lindem for their comments and contributions.

Contributors

Tony Li

Email: tony.li@tony.li

Authors' Addresses

Naiming Shen
Cisco Systems
560 McCarthy Blvd.
Milpitas, CA 95035
United States of America

Email: naiming@cisco.com

Shane Amante
Apple Inc.
One Apple Park Way
Cupertino, CA 95014
United States of America

Email: amante@apple.com

Mikael Abrahamsson
T-Systems Nordic
Kistagangen 26
Stockholm
Sweden

Email: Mikael.Abrahamsson@t-systems.se