Network Working Group
Request for Comments: 5704
Category: Informational

S. Bryant, Ed.
M. Morrow, Ed.
For the IAB

November 2009

Uncoordinated Protocol Development Considered Harmful

Abstract

This document identifies problems that may result from the absence of formal coordination and joint development on protocols of mutual interest between standards development organizations (SDOs). Some of these problems may cause significant harm to the Internet. The document suggests that a robust procedure is required prevent this from occurring in the future. The IAB has selected a number of case studies, such as Transport MPLS (T-MPLS), as recent examples to describe the hazard to the Internet architecture that results from uncoordinated adaptation of a protocol.

This experience has resulted in a considerable improvement in the relationship between the IETF and the ITU-T. In particular, this was achieved via the establishment of the "Joint working team on MPLS-TP". In addition, the leadership of the two organizations agreed to improve inter-organizational working practices so as to avoid conflict in the future between ITU-T Recommendations and IETF RFCs.

Whilst we use ITU-T - IETF interactions in these case studies, the scope of the document extends to all SDOs that have an overlapping protocol interest with the IETF.

Status of This Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Table of Contents

1. Introduction

The uncoordinated adaptation of a protocol, parameter, or code-point by a standards development organization (SDO), either through the allocation of a code-point without following the formal registration procedures or by unilaterally modifying the semantics of the protocol or intended use of the code-point itself, poses a risk of harm to the Internet [RFC4775].

The purpose of this document is to describe the various problems that may occur without formal coordination and joint development on protocols of mutual interest between SDOs. Some of the problems that arise may cause significant harm to the Internet. In particular, the IAB considers it an essential principle of the protocol development process that only one SDO maintains design authority for a given protocol, with that SDO having ultimate authority over the allocation of protocol parameter code-points and over defining the intended semantics, interpretation, and actions associated with those code-points.

There is currently a joint IETF - ITU-T development effort underway, known as the MPLS Transport Profile (MPLS-TP), which is progressing rapidly to extend MPLS in a way that is consistent with the MPLS architecture, and fully satisfies the requirements of the transport network provider [LS26]. By way of a case study, we will refer to the design and standardization process of the ITU-T protocol known as Transport MPLS (T-MPLS). Development of T-MPLS was abandoned [RFC5317] by ITU-T Study Group 15 due to inherent conflicts with the IETF MPLS design and, in particular, with the Internet architecture. These conflicts arose due to the lack of coordination with the IETF as the design authority for MPLS.

The goal of this document is to demonstrate the importance of a coordinated approach to successful collaboration between SDOs, and to explain a model for inter-SDO collaborative protocol development that is being used successfully by the ITU-T and IETF.

2. Protocol Design Rules

This section describes a number of protocol design rules needed to ensure the safe operation of a network. Whilst these rules will be familiar to many protocol designers, the rules are restated here to ensure that assumptions are clear and consistent. Differing assumptions have been at the root of many miscoordinations and miscommunications between SDOs in the past.

2.1. Protocol Safety

To understand the reasons why the IAB and IETF regard uncoordinated use of code-points and/or protocol modification as posing a risk of harm to the Internet, it is necessary to recap some important principles of protocol design in large-scale networks such as the Internet. Many end users and businesses have come to rely on the Internet as part of their critical infrastructure, thus large-scale networks, such as the Internet, represent significant economic value. Any outage in a large-scale network due to a protocol failure will therefore result in significant commercial and political damage.

When two incompatible protocols, or forms of the same protocol, are deployed without coordination, there is a serious risk that this may be catastrophic to the stability or security of the network.

Furthermore, the scale and distributed nature of the Internet is such that it may be difficult or impossible to rid the network of the long-term consequences of the protocol incompatibility. Therefore, the following issues are of critical importance.

2.2. Importance of Invariants

Invariants are core properties that are consistent across the network and do not change over extremely long time-scales. Protocol designers use such invariants as axioms in designing protocols. A protocol often places an absolute reliance on an invariant to resolve a design corner case. One example of an invariance in IP that was inherited in the design of MPLS is the invariant that a time to live (TTL) value is monotonically decreased and that a packet with TTL<=1 will not be forwarded. This is a safety mechanism to mitigate the damaging effects of packet-forwarding loops. Another example is the way that MPLS applies special semantics to the reserved label set (0..15) [RFC3032], and the notion that a Label Switched Router (LSR) is free to allocate labels with a value of 16 or greater for its own use.

2.3. Importance of Correct Identification

A special type of invariant is the allocation of a code-point. A code-point may be used to identify a packet type or a component within a packet. Without these identifiers, a packet is an opaque sequence of bits. A packet parser operates by first identifying the code-point and then using the semantics associated with that code-point to interpret other components within the packet. Once a code-point is defined, the interpretation of associated data and the consequential actions become protocol invariants. Subsequent protocol development must adhere to those invariants. The semantics for an allocated code-point must never change. If a future enhancement requires different semantics, interpretation, or action, then a new code-point must be obtained.

2.4. The Role of the Design Authority

A code-point such as an IEEE Ethertype is allocated to a design authority such as the IETF. It is this design authority that establishes how information identified by the code-point is to be interpreted to associate appropriate invariants. Modification and extension of a protocol requires great care. In particular, it is necessary to understand the exact nature of the invariants and the

consequences of modification. Such understanding may not always be possible when protocols are modified by organizations that don't have the experience of the original designers or the design authority expert pool. Furthermore, since there can only safely be a single interpretation of the information identified by a code-point, there must be a unique authority responsible for authorizing and documenting the semantics of the information and consequential protocol actions.

In the case of IP and MPLS technologies, the design authority is the IETF. The IETF has an internal process for evolving and maintaining the protocols for which it is the design authority. The IETF also has change processes in place [RFC4929] to work with other SDOs that require enhancements to its protocols and architectures. Similarly, the ITU-T has design authority for Recommendation E.164 [E.164] and allocates the relevant code-points, even though the IETF has design authority for the protocols ("ENUM") used to access E.164 numbers through the Internet DNS [RFC3245].

It is a recommendation of this document that the IETF introduces additional change mechanisms to encompass all of the technical areas for which it has design authority.

2.5. Ships in the Night

It may be tempting for a designer to assert that the protocol extensions it proposes are safe even though it breaks the invariants of the original protocol because these protocol variants will operate as ships in the night. That is, these protocol variants will never simultaneously exist in the same network domain and will never need to inter-work. This is a fundamentally unsound assumption for a number of reasons. First, it is infeasible to ensure that the two instances will never be interconnected under any circumstances. Second, even if the operators that deploy the protocols apply appropriate due diligence to ensure that the two instances do not conflict, it is infeasible to ensure that such conflicting protocols will not be interconnected under fault conditions.

This assumption of ships in the night is particularly hazardous when the instances of the protocol share the same identifying code-point. This is because a system is unable to determine which variant of the protocol it has received, and hence how to correctly interpret the associated information or to determine what protocol actions may be safely executed.

3. Examples of Miscoordination

There are a variety of examples where lack of inter-SDO coordination has led to the publication of flawed protocol designs. This section describes a number of case studies that illustrate coordination issues.

3.1. T-MPLS as a Case Study

A recent example where another SDO created a protocol based on misunderstandings of IETF protocols is T-MPLS. T-MPLS was created in ITU-T in an attempt to design a packet-transport method for transport-oriented networks. This is an example of the success that IETF protocols have enjoyed, and ITU-T's interest and selection of MPLS is a compliment to the IETF work. Quite late in the ITU-T design and specification cycle, there were a number of liaison exchanges between the ITU-T and the IETF, where the IETF became increasingly concerned about incompatibility of IETF MPLS procedures and technologies with ITU-T T-MPLS [RFC5317]. Extensive discussions took place regarding interpretation, definition, and misunderstandings regarding aspects such as MPLS Label 14, MPLS swap operation, TTL semantics, reservation of additional labels, and EXP bits. If ITU-T had worked with IETF from the start in developing T-MPLS, these problems could have been avoided. A detailed analysis of the T-MPLS case is provided in Appendix A.

3.2. PPP over SONET/SDH (Synchronous Optical Network / Synchronous Digital Hierarchy)

An example of where the IETF failed to coordinate with the ITU-T is [RFC1619], which defined PPP over SONET. In the text dealing with the SONET/SDH Synchronous Payload Envelope (SPE), the document erroneously stated that "no scrambling is needed during insertion into the SPE." It was later determined by SONET experts operating in the ITU-T and in ANSI that this error arose due to an incomplete understanding of the SONET scrambler. By not using a scrambler, the protocol was attempting to transport non-transparent data over SONET. This resulted in lost or misinterpreted data in the Packet over SONET (PoS) network. This impacted routing, signaling, and end-user data traffic. Details of this work are described in [PPPoSONET]. This problem would have been prevented if the IETF had worked with ITU-T and ANSI in initially developing [RFC1619] . The problem was resolved by working jointly with ITU-T and ANSI experts to publish [RFC2615], which mandated the use of scrambling.

Note that [RFC1619] was developed four years before the IETF and ITU-T agreed on formal procedures for cooperation, as documented in [RFC2436] (which was later obsoleted by [RFC3356]).

4. Managing Information Flow

This section recommends that intra- and inter-SDO information flows require careful management in order to prevent the accidental extension of protocols without complete coordination of the work with the relevant design authority.

4.1. Managing Information Flow within an SDO

One cannot assume that an SDO is completely familiar with the internal structure, information exchange, or internal processes of another SDO. Hence, the initial contact point and the subgroup with which a long-term working relationship is formed has a duty to ensure that the work is fully notified and coordinated to all relevant parties within the SDO.

4.2. Managing Information Flow between SDOs

A recommendation is that, as part of their document-approval process, SDOs should confirm that all protocol parameters, code-points, TLV identifiers, etc., have been authorized by the appropriate design authority (e.g., IANA, IETF, etc. in this case) and that SDO approval from the design authority has been obtained prior to publishing protocol extensions. This confirmation should be an integral part of the approval or consent process as verifying that the normative references are qualified.

5. MPLS-TP as Best Practice

In order to bridge the gap between the two organizations, the IETF and the ITU-T established a joint working team (JWT) to assess whether it was possible to enhance existing MPLS standards to provide a best-in-class solution for transport networks. The outcome of this investigation is reported in [RFC5317].

The JWT proposed a design that was acceptable to both SDOs. This has led to the creation of the MPLS-TP project. This is a joint project in which the ITU-T experts work with the IETF on protocol-development tasks, and IETF members work within the ITU-T to understand requirements and to assist in the creation of ITU-T recommendations that describe MPLS-TP in which the technical definition is provided through normative references to IETF RFCs.

Although the JWT approach allowed the IETF and the ITU-T to agree on a method of resolving the T-MPLS problem, this approach had a significant resource cost. The JWT required considerable protocol-design expertise and IETF management time to agree on a suitable technical solution. A lightweight process, starting with close

coordination during the requirements phase and continuing during the development phase, would likely reduce the resources needed to an acceptable level in the future.

6. IETF Change Process

There is an MPLS-change-process [RFC4929] . However, the IETF has not yet defined a change process that is applicable to all of its work areas. The problems described in this document indicate that the IETF needs to develop a universal change process. The MPLS-change-process would seem to be a suitable starting point.

7. Security Considerations

The uncoordinated development of protocols poses a risk of harm to the Internet and must not be permitted. The enhancement or modification of a protocol can increase attack surfaces considerably and may therefore compromise the security or stability of the Internet. The IETF has a review process that combines cross-area review with specialist security review by experts familiar with the development and deployment context of the Internet protocol suite. In particular, because of the Internet infrastructure’s reliance on the IP and MPLS protocol suites, this security review process must be exercised with considerable diligence. Failure to apply this review process exposes the Internet to increased risk along both security and stability vectors.

8. Acknowledgments

The authors wish to acknowledge Loa Andersson for his contribution to this work.

9. IAB Members at the Time of This Writing

Marcelo Bagnulo
Gonzalo Camarillo
Stuart Cheshire
Vijay Gill
Russ Housley
John Klensin
Olaf Kolkman
Gregory Lebovitz
Andrew Malis
Danny McPherson
David Oran
Jon Peterson
Dave Thaler

10. Emerging Issues

Although we have used T-MPLS as a case study, there are other ongoing ITU-T projects and core IETF specifications that could be the subject of either improved coordination or new conflicts, depending on whether or not the principles outlined in this document are adhered to by the IETF and ITU. Two current examples are [Y.2015] and [Q.Flowsig]. New areas with potential for cooperation or conflict are emerging from the work of ITU-T SG13 Question 7, "IPv6" -- for example: [Y.ipv6split] and [Y.ipv6migration].

Improved coordination, of course, is not limited to the relationship between IETF and ITU-T. This issue is present between a set of SDOs. The IETF - ITU-T relationship has simply been used because there is a recent example where a potential disaster was, through much hard work, not only prevented but turned into a net gain for all.

11. Conclusion

It is important that all SDOs developing standards that affect the operation of the Internet learn the lessons that arise from cases cited in this document. Uncoordinated parallel work between SDOs creates significant problems with potentially damaging operation impact to those that deploy and use the Internet. Both inter- and intra-SDO information flow needs to be well managed to ensure that all impacted parties are aware of work items. Finally, the IETF needs to develop a universal change process that encompasses all of its work areas.

12. Informative References

[E.164] ITU-T, "ITU Recommendation E.164: The international public telecommunication numbering plan", February 2005.

[LS26] ITU-T Study Group 15, "Cooperation Between IETF and ITU-T on the Development of MPLS-TP", Geneva, December 2008, <https://datatracker.ietf.org/documents/LIAISON/file596.pdf>.

[PPPoSONET] Manchester, J., et al., "PPP over SONET/SDH", Work in Progress, October 1997.

[Q.Flowsig] ITU-T Study Group 11, Question 5, "Signalling protocols and procedures relating to flow state aware access QoS control in an NGN", Draft Recommendation.

[RFC1393] Malkin, G., "Traceroute Using an IP Option", RFC 1393, January 1993.

[RFC1619] Simpson, W., "PPP over SONET/SDH", RFC 1619, May 1994.

[RFC2436] Brett, R., Bradner, S., and G. Parsons, "Collaboration between ISOC/IETF and ITU-T", RFC 2436, October 1998.

[RFC2615] Malis, A. and W. Simpson, "PPP over SONET/SDH", RFC 2615, June 1999.

[RFC3031] Rosen, E., Viswanathan, A., and R. Callon, "Multiprotocol Label Switching Architecture", RFC 3031, January 2001.

[RFC3032] Rosen, E., Tappan, D., Fedorkow, G., Rekhter, Y., Farinacci, D., Li, T., and A. Conta, "MPLS Label Stack Encoding", RFC 3032, January 2001.

[RFC3245] Klensin, J. and IAB, "The History and Context of Telephone Number Mapping (ENUM) Operational Decisions: Informational Documents Contributed to ITU-T Study Group 2 (SG2)", RFC 3245, March 2002.

[RFC3270] Le Faucheur, F., Wu, L., Davie, B., Davari, S., Vaananen, P., Krishnan, R., Cheval, P., and J. Heinanen, "Multi-Protocol Label Switching (MPLS) Support of Differentiated Services", RFC 3270, May 2002.

[RFC3356] Fishman, G. and S. Bradner, "Internet Engineering Task Force and International Telecommunication Union - Telecommunications Standardization Sector Collaboration Guidelines", RFC 3356, August 2002.

[RFC3429] Ohta, H., "Assignment of the 'OAM Alert Label' for Multiprotocol Label Switching Architecture (MPLS) Operation and Maintenance (OAM) Functions", RFC 3429, November 2002.

[RFC4379] Kompella, K. and G. Swallow, "Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures", RFC 4379, February 2006.

[RFC4775] Bradner, S., Carpenter, B., and T. Narten, "Procedures for Protocol Extensions and Variations", BCP 125, RFC 4775, December 2006.

[RFC4929] Andersson, L. and A. Farrel, "Change Process for Multiprotocol Label Switching (MPLS) and Generalized MPLS (GMPLS) Protocols and Procedures", BCP 129, RFC 4929, June 2007.

[RFC5129] Davie, B., Briscoe, B., and J. Tay, "Explicit Congestion Marking in MPLS", RFC 5129, January 2008.

[RFC5317] Bryant, S. and L. Andersson, "Joint Working Team (JWT) Report on MPLS Architectural Considerations for a Transport Profile", RFC 5317, February 2009.

[RFC5462] Andersson, L. and R. Asati, "Multiprotocol Label Switching (MPLS) Label Stack Entry: "EXP" Field Renamed to "Traffic Class" Field", RFC 5462, February 2009.

[RFC5654] Niven-Jenkins, B., Brungard, D., Betts, M., Sprecher, N., and S. Ueno, "Requirements of an MPLS Transport Profile", RFC 5654, September 2009.

[Y.1711-2002] ITU-T Study Group 13, "ITU-T Recommendation Y.1711: OAM mechanism for MPLS networks", November 2002.

[Y.1711-2004] ITU-T Study Group 13, "ITU-T Recommendation Y.1711: OAM mechanism for MPLS networks", February 2004.

[Y.1711am1] ITU-T Study Group 13, "ITU-T Recommendation Y.1711 Amendment 1: New Function Type Codes", October 2005.

[Y.1711cor1] ITU-T Study Group 13, "ITU-T Recommendation Y.1711 (2004) corrigendum 1", February 2005.

[Y.2015] ITU-T Study Group 13, Question 5, "General Requirements for ID/Locator Separation in NGN".

[Y.ipv6migration] ITU-T, "ITU draft Y.ipv6migration: Roadmap for IPv6 migration from NGN operators perspective", 2009.

[Y.ipv6split] ITU-T, "ITU draft Y.ipv6split: Framework of ID/LOC separation in IPv6-based NGN", 2009.

Appendix A. A Review of the T-MPLS Case

T-MPLS was created in ITU-T in an attempt to design an MPLS-based packet-transport method for transport-oriented networks. This appendix describes the technical issues that the IETF identified with the T-MPLS documents and their consequences.

A.1. Multiple Definitions of Label 14

To appreciate why the use of MPLS Reserved Label 14 by the T-MPLS protocol represented a safety concern to the Internet, it is important to understand the current standards that use MPLS Reserved Label 14.

The governing standard on the use of MPLS Reserved Label 14 is [RFC3429], "Assignment of the 'OAM Alert Label' for Multiprotocol Label Switching Architecture (MPLS) Operation and Maintenance (OAM) Functions".

Label 14 is assigned to a specific protocol, namely, ITU-T Recommendation [Y.1711-2002].

ITU-T Recommendation [Y.1711-2002] has been superseded by newer versions, specifically: [Y.1711-2004], [Y.1711cor1], and [Y.1711am1].

All three documents are currently in force as ITU-T Recommendations.

The problem is that the changes made to Y.1711 were never reflected in an update to RFC 3429, which only defines the protocol as specified by the now superseded 2002 Recommendation. So for example, MPLS equipment responding to an MPLS packet containing Label 14 would expect to see the 2002 version of the Y.1711 [Y.1711-2002] protocol and would not recognize any of the new function codes specified in Y.1711 Amendment 1. This problem arises because Y.1711 does not have a version field, and RFC 3429 offers no other method to disambiguate non-interoperable versions of Y.1711. Having a version number in the protocol permits an implementer to codify non-interoperability. Furthermore, the IETF as the authority over Label 14 semantics has the final say over maintaining the interoperability of the protocol employing that code-point, unless the IETF explicitly delegates such authority.

With regard to T-MPLS, there was a lack of coordination between the ITU-T and the IETF over the redefinition of the semantics of MPLS Label 14, which resulted in protocol definitions that conflicted with the IETF MPLS architecture.

The MPLS architecture [RFC3031], defines a swap operation as an atomic function that replaces the top label in an MPLS label stack with another label, which provides context for the next hop LSR. However, the ITU-T Recommendations that specified the new OAM functions defined by Label 14 redefined the label-swap operation as a POP, followed by a PUSH, thereby causing all LSRs to inspect the label stack for the presence of Label 14 at each hop. This proposed new behaviour conflicts with the IETF definition of a swap operation.

The behaviour proposed in these specifications would have had major consequences for deployed hardware designs. The outcome would have been that the equipments built according to the two different specifications would have been incompatible. It is important that the atomic procedure defined in [RFC3031] is kept unchanged.

A.2. Redefinition of TTL Semantics

The standard method of delivering an OAM message to an entity on a Label Switched Path (LSP), such that the OAM message shares its fate with the data traffic, is to use TTL expiry. The IETF's Internet Protocol (IP) utilizes this mechanism for traceroute [RFC1393], as does MPLS ping [RFC4379].

At one stage, the T-MPLS designers considered a multi-level OAM design in which the OAM packet was steered to its target by a process in which some nodes increased the TTL as they forwarded the OAM packet to its next hop. TTL is a safety device in the IETF IP and MPLS architecture that prevents a packet from continuously looping under fault conditions. Thus, the proposed extension to support an enhanced OAM mechanism violated an MPLS design invariant specifically introduced to ensure safe operation of the Internet by preventing persistent forwarding loops.

A.3. Reservation of Additional Labels

The IETF MPLS protocol uses a small number of reserved labels [RFC3032] as a mechanism to provide additional context and to trigger some special processing operations in the forwarder. All other labels used for forwarding use semantics defined by the forwarding equivalence class (FEC). In an early implementation of T-MPLS, the designers determined that they needed some additional labels to alert the forwarder that the packet needed special processing. Thus, a conflict was thereby introduced between the behaviour of an IETF MPLS LSR and LSRs that operate according to the specification in the ITU-T Recommendation. Thus, some LSRs would attribute special semantics to Labels 16..31, whilst other LSRs would perform normal forwarding on them.

A.4. Redefinition of MPLS EXP Bits

The early MPLS documents defined the form of the MPLS label stack entry [RFC3032]. This includes a three-bit field called the "EXP field". The exact use of this field was not defined by these documents, except to state that it was to be "reserved for experimental use".

Although the intended use of the EXP field was as a "Class of Service" (CoS) field, it was not named a CoS field by these early documents because the use of such a CoS field was not considered to be sufficiently defined. Today, a number of standards documents define its usage as a CoS field ([RFC3270], [RFC5129]), and hardware is deployed that assumes this exclusive usage.

The T-MPLS designers, unaware of the historic reason for the "provisional" naming of this field, assumed that they were available for any experimental use and re-purposed them to indicate the maintenance-entity level (a hierarchical maintenance mechanism).

The intended use of the EXP field was subsequently carried in [RFC5462], which reinforces this use by formally changing the name to Traffic Class (TC).

A.5. The Consequences for the Network Operators

Transport network operators need a way to realize the statistical gain inherent in packet networking while retaining the familiar operational structure of their SONET/SDH networks. T-MPLS was an attempt to provide that functionality. However, creating an incompatible variant of MPLS without tight coordination with IETF created a number of problems for network operators.

Firstly, those operators that deployed T-MPLS in production networks will need to address the risk and complexity of transitioning their network to MPLS-TP. Secondly, there has been a consequential delay of the necessary enhancements to MPLS to meet their needs [RFC5654] as the IETF and ITU-T executed a redevelopment of MPLS-based transport network protocols.

Fortunately, the two organizations are now working together to design the necessary enhancements

The resulting technology, MPLS-TP, brings significant benefits to all. However, this has not been without cost. Had things continued, we are not sure what would have happened -- at the least, the larger

MPLS community would have been denied the benefit of better OAM, and the transport community would have been denied the many benefits of an interoperable solution.

A.6. The Consequences for the SDOs

The process of resolution required considerable resources and introduced a great deal of conflict between the IETF and the ITU-T, much of which was exposed to public scrutiny, to the detriment of both organizations. In particular, this conflict-resolution process consumed the very resources required to develop an optimal architecture for MPLS in transport networks.

Authors' Addresses

Stewart Bryant (editor)

EMail: stbryant@cisco.com

Monique Morrow (editor)

EMail: mmorrow@cisco.com

Internet Architecture Board

EMail: iab@iab.org