              Inclusion of Manageability Sections in
         Path Computation Element (PCE) Working Group Drafts

Abstract

   It has often been the case that manageability considerations have
   been retrofitted to protocols after they have been specified,
   standardized, implemented, or deployed. This is sub-optimal.
   Similarly, new protocols or protocol extensions are frequently
   designed without due consideration of manageability requirements.

   The Operations Area has developed "Guidelines for Considering
   Operations and Management of New Protocols and Protocol Extensions"
   (RFC 5706), and those guidelines have been adopted by the Path
   Computation Element (PCE) Working Group.

   Previously, the PCE Working Group used the recommendations contained
   in this document to guide authors of Internet-Drafts on the contents
   of "Manageability Considerations" sections in their work. This
   document is retained for historic reference.

Status of This Memo

   This document is not an Internet Standards Track specification; it is
   published for the historical record.

   This document defines a Historic Document for the Internet community.
   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). Not all documents
   approved by the IESG are a candidate for any level of Internet
   Standard; see Section 2 of RFC 5741.

   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/rfc6123.

Copyright Notice

1. Introduction

   This document is produced for historic reference.

   When new protocols or protocol extensions are developed, it is often
   the case that not enough consideration is given to the manageability
   of the protocols or to the way in which they will be operated in the
   network. The result is that manageability considerations are only
   understood once the protocols have been implemented and sometimes not
   until after they have been deployed.

   The resultant attempts to retrofit manageability mechanisms are not
   always easy or architecturally pleasant. Furthermore, it is possible
   that certain protocol designs make manageability particularly hard to
   achieve.

   Recognizing that manageability is fundamental to the utility and
   success of protocols designed within the IETF, and that simply
   defining a MIB module does not necessarily provide adequate
   manageability, this document was developed to define recommendations
   for the inclusion of Manageability Considerations sections in all
   Internet-Drafts produced within the PCE Working Group. It was the
   intention that meeting these recommendations would ensure that proper
   consideration was given to the support of manageability at all stages
   of the protocol development process from Requirements and
   Architecture through Specification and Applicability.

   It is clear that the presence of such a section in an Internet-Draft
   does not guarantee that the protocol will be well-designed or
   manageable. However, the inclusion of this section will ensure that
   the authors have the opportunity to consider the issues, and, by
   reading the material in this document, they will gain some guidance.

This document was developed within the PCE Working Group and was used
to help guide the authors and editors within the working group to
produce Manageability Considerations sections in the Internet-Drafts
and RFCs produced by the working group.

[RFC5706] presents general guidance from the IETF's Operations Area
for considering Operations and Management of new protocols and
protocol extensions. It has been adopted by the PCE Working Group to
provide guidance to editors and authors within the working group, so
this document is no longer required. However, the working group
considers that it will be useful to archive this document as Historic
for future reference.

1.1. Requirements Notation

This document is not a protocol specification. The key words "MUST",
"MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT",
"RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be
interpreted as described in [RFC2119] in order that the contents of a
Manageability Considerations section can be clearly understood.

1.2. What Is Manageability?

In this context, "manageability" is used to refer to the interactions
between a network operator (a human or an application) and the
network components (hosts, routers, switches, applications, and
protocols) performed to ensure the correct operation of the network.

Manageability issues are often referred to under the collective
acronym, FCAPS [X.700], which stands for the following:

- Fault management
- Configuration
- Accounting
- Performance
- Security

Conventionally, Security is already covered an Internet-Draft in its
own Security Considerations section, and this document does not in
any way diminish the need for that section. Indeed, as pointed out
in Section 6, a full consideration of other aspects of manageability
may increase the text that should be supplied in the Security
Considerations section.

The author of a Manageability Considerations section should certainly
consider all aspects of FCAPS. The author should reflect on how the
manageability of a new protocol impacts the manageability and
operation of the entire network. Specific optional subsections (see

   Section 2.3) should be added as necessary to describe features of
   FCAPS that are pertinent but are not covered by the recommended
   subsections. More discussion of what manageability is and what may
   be included in a Manageability Considerations section can be found in
   [RFC5706].

   As part of documenting the manageability considerations for a new
   protocol or for protocol extensions, authors should consider that one
   of the objectives of specifying protocols within the IETF is to
   ensure interoperability of implementations. This interoperability
   extends to the manageability function so that it is an ideal that
   there should be implementation independence between management
   applications and managed entities. This may be promoted by the use
   of standardized management protocols and by the specification of
   standard information models.

   Note that, in some contexts, reference is made to the term
   "management plane". This is used to describe the exchange of
   management messages through management protocols (often transported
   by IP and by IP transport protocols) between management applications
   and the managed entities such as network nodes. The management plane
   may use distinct addressing schemes, virtual links or tunnels, or a
   physically separate management control network. The management plane
   should be seen as separate from, but possibly overlapping with, the
   control plane, in which signaling and routing messages are exchanged,
   and the forwarding plane (sometimes called the data plane or user
   plane), in which user traffic is transported.

2. Presence and Placement of Manageability Considerations Sections

   Note that examples of the sections described here can be found in the
   documents listed in Appendix A.

2.1. Null Manageability Considerations Sections

   In the event that there are no manageability requirements for an
   Internet-Draft, the draft SHOULD still contain a Manageability
   Considerations section. The presence of this section indicates to
   the reader that due consideration has been given to manageability and
   that there are no (or no new) requirements.

   In this case, the section SHOULD contain a simple statement such as
   "There are no new manageability requirements introduced by this
   document" and SHOULD briefly explain why that is the case with a
   summary of manageability mechanisms that already exist.

   Note that a null Manageability Considerations section may take some
   effort to compose. It is important to demonstrate to the reader that
   no additional manageability mechanisms are required, and it is often
   hard to prove that something is not needed. A null Manageability
   Considerations section SHOULD NOT consist only of the simple
   statement that there are no new manageability requirements.

   If an Internet-Draft genuinely has no manageability impact, it should
   be possible to construct a simple null Manageability Considerations
   section that explains why this is the case.

2.2. Recommended Subsections

   If the Manageability Considerations section is not null, it SHOULD
   contain at least the following subsections. Guidance on the content
   of these subsections can be found in Section 3 of this document.

   - Control of Function through Configuration and Policy
   - Information and Data Models, e.g., MIB modules
   - Liveness Detection and Monitoring
   - Verifying Correct Operation
   - Requirements on Other Protocols and Functional Components
   - Impact on Network Operation

   In the event that one or more of these subsections is not relevant,
   it SHOULD still be present and SHOULD contain a simple statement
   explaining why the subsection is not relevant. That is, null
   subsections are allowed, and each should be formed following the
   advice in Section 2.1.

2.3. Optional Subsections

   The list of subsections above is not intended to be prescriptively
   limiting. Other subsections can and SHOULD be added according to the
   requirements of each individual Internet-Draft. If a topic does not
   fit comfortably into any of the subsections listed, the authors
   should be relaxed about adding new subsections as necessary.

2.4. Placement of Manageability Considerations Sections

   The Manageability Considerations section SHOULD be placed immediately
   before the Security Considerations section in any Internet-Draft.

3. Guidance on the Content of Subsections

   This section gives guidance on the information to be included in each
   of the recommended subsections listed above. Note that, just as
   other subsections may be included, so additional information MAY also
   be included in these subsections.

3.1. Control of Function through Configuration and Policy

   This subsection describes the functional elements that may be
   controlled through configuration and/or policy.

   For example, many protocol specifications include timers that are
   used as part of the operation of the protocol. These timers often
   have default values suggested in the protocol specification and do
   not need to be configurable. However, it is often the case that the
   protocol requires that the timers can be configured by the operator
   to ensure specific behavior by the implementation.

   Even if all configurable items have been described within the body of
   the document, they SHOULD be identified in this subsection, but a
   reference to another section of the document is sufficient if there
   is a full description elsewhere.

   Other protocol elements are amenable to control through the
   application of local or network-wide policy. It is not the intention
   that this subsection should give details of policy implementation
   since that is covered by more general policy framework specifications
   such as [RFC3060] and [RFC3460]. Additionally, specific frameworks
   for policy as applicable within protocol or functional architectures
   are also normally covered in separate documents, for example,
   [RFC5394].

   However, this section SHOULD identify which protocol elements are
   potentially subject to policy and should give guidance on the
   application of policy for successful operation of the protocol.
   Where this material is already described within the body of the
   document, this subsection SHOULD still identify the issues and
   reference the other sections of the document.

3.2. Information and Data Models

   This subsection SHOULD describe the information and data models
   necessary for the protocol or the protocol extensions. This
   includes, but is not necessarily limited to, the MIB modules
   developed specifically for the protocol functions specified in the
   document.

Where new or extended MIB modules are recommended, it is helpful if
this section can give an overview of the items to be modeled by the
MIB modules. This does not require an object-by-object description
of all of the information that needs to be modeled, but it could
explain the high-level "object groupings" (perhaps to the level of
suggesting the MIB tables) and certainly should explain the major
manageable entities. For example, a protocol specification might
include separate roles for "sender" and "receiver" and might be
broken into a "session" and individual "transactions"; if so, this
section could list these functionalities as separate manageable
entities.

[RFC3444] may be useful in determining what information to include in
this section.

The description in this section can be by reference where other
documents already exist.

It should be noted that the significance of MIB modules may be
decreasing, but there is still a requirement to consider the managed
objects necessary for successful operation of the protocol or
protocol extensions. This means that due consideration should be
given not only to what objects need to be managed but also to what
management model should be used. There are now several options,
including the MIB/SNMP (Simple Network Management Protocol) model and
the Network Configuration Protocol (NETCONF) model, being developed
by the NETCONF Data Modeling Language (NETMOD) Working Group [YANG].

3.3. Liveness Detection and Monitoring

Liveness detection and monitoring apply both to the control plane and
the data plane.

Mechanisms for detecting faults in the control plane or for
monitoring its liveness are usually built into the control plane
protocols or inherited from underlying data plane or forwarding plane
protocols. These mechanisms do not typically require additional
management capabilities but are essential features for the protocol
to be usable and manageable. Therefore, this section SHOULD
highlight the mechanisms in the new protocol or protocol extensions
that are required in order to ensure liveness detection and
monitoring within the protocol.

Further, when a control plane fault is detected, there is often a
requirement to coordinate recovery action through management
applications or at least to record the fact in an event log. This
section SHOULD identify the management actions expected when the
protocol detects a control plane fault.

Where the protocol is responsible for establishing data or user plane
connectivity, liveness detection and monitoring usually need to be
achieved through other mechanisms. In some cases, these mechanisms
already exist within other protocols responsible for maintaining
lower layer connectivity, but it will often be the case that new
procedures are required so that failures in the data path can be
detected and reported rapidly, allowing remedial action to be taken.
This section SHOULD refer to other mechanisms that are assumed to
provide monitoring of data plane liveness and SHOULD identify
requirements for new mechanisms as appropriate.

This section SHOULD describe the need for liveness and detection
monitoring, SHOULD highlight existing tools, SHOULD identify
requirements and specifications for new tools (as appropriate for the
level of the document being written), and SHOULD describe the
coordination of tools with each other, with management applications,
and with the base protocol being specified.

3.4. Verifying Correct Operation

An important function that Operations and Management (OAM) can
provide is a toolset for verifying the correct operation of a
protocol. To some extent, this may be achieved through access to
information and data models that report the status of the protocol
and the state installed on network devices. However, it may also be
valuable to provide techniques for testing the effect that the
protocol has had on the network by sending data through the network
and observing its behavior.

Thus, this section SHOULD include details of how the correct
operation of the protocols described by the Internet-Draft can be
tested, and, in as far as the Internet-Draft impacts on the operation
of the network, this section SHOULD include a discussion about how
the correct end-to-end operation of the network can be tested and how
the correct data or forwarding plane function of each network element
can be verified.

There may be some overlap between this section and that describing
liveness detection and monitoring since the same tools may be used in
some cases.

3.5. Requirements on Other Protocols and Functional Components

The text in this section SHOULD describe the requirements that the
new protocol puts on other protocols and functional components as
well as requirements from other protocols that have been considered

   in designing the new protocol. This is pertinent to manageability
   because those other protocols may already be deployed and operational
   and because those other protocols also need to be managed.

   It is not appropriate to consider the interaction between the new
   protocol and all other protocols in this section, but it is important
   to identify the specific interactions that are assumed for the
   correct functioning of the new protocol or protocol extensions.

3.6. Impact on Network Operation

   The introduction of a new protocol or extensions to an existing
   protocol may have an impact on the operation of existing networks.
   This section SHOULD outline such impacts (which may be positive),
   including scaling concerns and interactions with other protocols.

   For example, a new protocol that doubles the number of active,
   reachable addresses in use within a network might need to be
   considered in the light of the impact on the scalability of the IGPs
   operating within the network.

   A very important feature that SHOULD be addressed in this section is
   backward compatibility. If protocol extensions are being introduced,
   what impact will this have on a network that has an earlier version
   of the protocol deployed? Will it be necessary to upgrade all nodes
   in the network? Can the protocol versions operate side by side? Can
   the new version of the protocol be tunneled through the old version?
   Can existing services be migrated without causing a traffic hit or is
   a "maintenance period" required to perform the upgrade? What are the
   configuration implications for the new and old protocol variants?

   Where a new protocol is introduced, issues similar to backward
   compatibility may exist and SHOULD be described. How is migration
   from an old protocol to the new protocol achieved? Do existing
   protocols need to be interfaced to the new protocol?

3.7. Other Considerations

   Anything that is not covered in one of the recommended subsections
   described above but is needed to understand the manageability
   situation SHOULD be covered in an additional section. This may be a
   catch-all section named "Other Considerations" or may be one or more
   additional optional sections as described in Section 2.3.

4. IANA Considerations

   This document does not introduce any new codepoints or name spaces
   for registration with IANA. It makes no request to IANA for action.

   Internet-Drafts SHOULD NOT introduce new codepoints, name spaces, or
   requests for IANA action within the Manageability Considerations
   section.

5. Manageability Considerations

   This document defines Manageability Considerations sections
   recommended for inclusion in all PCE Working Group Internet-Drafts.
   As such, the whole document is relevant to manageability.

   Note that the impact of the application of this document to Internet-
   Drafts produced within the PCE Working Group should be that PCE
   protocols and associated protocols are designed and extended with
   manageability in mind. This should result in more robust and more
   easily deployed protocols.

   However, since this document does not describe any specific protocol,
   protocol extensions, or protocol usage, no manageability
   considerations need to be discussed here.

   (This is an example of a null Manageability Considerations section).

6. Security Considerations

   This document is Historic and describes the format and content of
   Internet-Drafts. As such, it introduces no new security concerns.

   However, there is a clear overlap between security, operations, and
   management. The manageability aspects of security SHOULD be covered
   within the mandatory Security Considerations of each Internet-Draft.
   New security considerations introduced by the Manageability
   Considerations section MUST be covered in the Security Considerations
   section.

   Note that fully designing a protocol before it is implemented
   (including designing the manageability aspects) is likely to result
   in a more robust protocol. That is a benefit to network security.
   Retrofitting manageability to a protocol can make the protocol more
   vulnerable to security attacks, including attacks through the new
   manageability facilities. Therefore, the use of this document is
   RECOMMENDED in order to help ensure the security of all protocols to
   which it is applied.

7. Acknowledgements

   This document is based on earlier work exploring the need for
   Manageability Considerations sections in all Internet-Drafts produced
   within the Routing Area of the IETF. That document was produced by
   Avri Doria and Loa Andersson working with the current author. Their
   input was both sensible and constructive.

   Peka Savola provided valuable feedback on an early versions of the
   original document. Thanks to Bert Wijnen, Dan Romascanu, David
   Harrington, Lou Berger, Spender Dawkins, Tom Petch, Matthew Meyer,
   Dimitri Papdimitriou, Stewart Bryant, and Jamal Hadi Salim for their
   comments.

   Thanks to the PCE Working Group for adopting the ideas contained in
   this document and for including Manageability Considerations sections
   in their Internet-Drafts and RFCs.

8. References

8.1. Normative References

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
             Requirement Levels", BCP 14, RFC 2119, March 1997.

8.2. Informative References

   [RFC3060] Moore, B., Ellesson, E., Strassner, J., and A. Westerinen,
             "Policy Core Information Model -- Version 1 Specification",
             RFC 3060, February 2001.

   [RFC3460] Moore, B., Ed., "Policy Core Information Model (PCIM)
             Extensions", RFC 3460, January 2003.

   [RFC3444] Pras, A. and J. Schoenwaelder, "On the Difference between
             Information Models and Data Models", RFC 3444, January
             2003.

   [RFC5394] Bryskin, I., Papadimitriou, D., Berger, L., and J. Ash,
             "Policy-Enabled Path Computation Framework", RFC 5394,
             December 2008.

   [RFC5706] Harrington, D., "Guidelines for Considering Operations and
             Management of New Protocols and Protocol Extensions", RFC
             5706, November 2009.

   [X.700]   CCITT Recommendation X.700 (1992), Management framework for
             Open Systems Interconnection (OSI) for CCITT applications.

   [YANG]   Bjorklund, M., Ed., "YANG - A Data Modeling Language for
              the Network Configuration Protocol (NETCONF)", RFC 6020,
              October 2010.

Appendix A.   Example Manageability Considerations Sections

   Readers are referred to the following documents for example
   Manageability Considerations sections that received positive comments
   during IESG review:

   Farrel, A., Vasseur, J.-P., and J. Ash, "A Path Computation Element
   (PCE)-Based Architecture", RFC 4655, August 2006.

   Le Roux, J., Ed., "Requirements for Path Computation Element (PCE)
   Discovery", RFC 4674, October 2006.

   Le Roux, JL., Ed., Vasseur, JP., Ed., Ikejiri, Y., and R. Zhang,
   "OSPF Protocol Extensions for Path Computation Element (PCE)
   Discovery", RFC 5088, January 2008.

   Vasseur, JP., Ed., and JL. Le Roux, Ed., "Path Computation Element
   (PCE) Communication Protocol (PCEP)", RFC 5440, March 2009.

   Bradford, R., Ed., Vasseur, JP., and A. Farrel, "Preserving Topology
   Confidentiality in Inter-Domain Path Computation Using a Path-Key-
   Based Mechanism", RFC 5520, April 2009.

   Oki, E., Takeda, T., Le Roux, JL., and A. Farrel, "Framework for PCE-
   Based Inter-Layer MPLS and GMPLS Traffic Engineering", RFC 5623,
   September 2009.

Author's Address

   Adrian Farrel
   Old Dog Consulting
   EMail: adrian@olddog.co.uk