Requirements for the Resilience of Control Plane

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress".

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on April 14, 2006.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

The resilience of control plane refers to the ability of control plane to continue its operation even under failure conditions of
control components such as control entities, control nodes, and control channels. This document describes requirements for providing the resilience capability of control plane (in other words, control network) in non-(G)MPLS and (G)MPLS. This contribution, as a document that proposes a framework to provide the resilience capability of control plane, include terminologies, basic concepts of control networks, possible configurations, necessities and requirements, additional considerations including the relationship with other protocol such as LMP for the resilience of control plane.

Table of Contents

1. Introduction...................................................2
   1.1 Terminology for Resilience of Control Channels.........3
2. Terminology....................................................4
3. Control Networks...............................................4
4. Necessities for Resilience of Control Channels..............7
5. Requirements for Resilience of Control Channels............8
   5.1 Requirements for MPLS 1+1 LSPs........................8
   5.2 Requirements for LMP-CCM Extension.....................8
6. Functions for LMP-CCM Extension................................9
   6.1 Identification of PG-1 and PG-3 Control Channel......9
   6.2 Identification of Detour Control Channels.............10
   6.3 Automatic Switchover....................................10
   6.4 Forced Switchover.......................................10
   6.5 Recovery from Failure....................................10
   6.6 Notification of Control Channel Unavailability........10
   6.7 Inquiry of Switchover Attributes.......................11
   6.8 Hello Initiation.........................................11
   6.9 Notification of Protocol Errors........................11
7. Security Considerations.......................................11
8. IANA Considerations........................................11
9. References................................................................11
   9.1 Normative References.....................................11
   9.2 Informative References..................................12
Author’s Addresses....................................................12

1. Introduction

There are three components in control plane, which are control
terminologies, basic concepts of control networks, possible configurations, necessities and requirements, additional considerations including the relationship with other protocol such as LMP for the resilience of control plane.
label distribution information, and network topology and state distribution information. In addition to the exchange of control packets between nodes within a network, it may be possible to do transparent relay of routing and signaling information over those control channels between neighboring networks. A control entity is a functional process responsible for running link management, routing protocols or signaling functions. A control node means a physical node keeping various control entities.

Best-effort based IP networks use routing protocols such as OSPF and BGP in order to forward data packets. In this situation, control packets generated by routing protocols are processed in the layer 3 as the same way that data packets exchanged by ordinary users are done in the layer. It means that channels carrying data and control packets share the fate. MPLS based IP networks upgraded from the best-effort based IP networks use routing and signaling protocols to establish LSPs that are determined for more effectively forwarding data packets. However, their control packets are still processed in the layer 3, and the fate of control channels is the same to that of data channels as well.

Then, GMPLS based IP networks come to be capable of handling control channels separated from data channels. It means that channels carrying data and control packets do not have an impact upon each other. Several control channels such as SONET/SDH DCC channels and Ethernet OAM channels defined by the OIF, MPLS based LSPs applied as dedicated control channels, public IP networks, out-of-fiber based dedicated control channels, and so on can be configured independent from data channels for the purpose.

In the end, a node can configure control channels of sharing the own fate with data channels or of separating the fate from data channels according to network requirements. It is an important thing that possible alternative paths exist between the communicating entities. Here, a network can provide protection and switchover functions of various levels based on configuration schemes and physical characteristics of paths to be used to exchange control packets between adjacent nodes. To effectively use these alternative paths between nodes, this document describes requirements for the resilience of control networks, which include terminologies, basic concepts of control networks, possible configurations, necessities and requirements, additional considerations, and so on. In this current document, only the resilience part of control channels is covered, the parts of control entities and control nodes need a further study.

1.1 Terminology for Resilience of Control Channels
To provide the resilience capabilities of control channels, several terms layer should be introduced. For examples, these include control packet types, active and standby control channels, physical control channels, protection groups (PGs), and etc, which are not exhaustive.

- Control packet types: Control information such as routing, signaling, and link management in GMPLS. In more detail, Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS), and Border Gateway Protocol (BGP) variants are candidates for routing, Constraint-Based Routing Label Distribution Protocol (CR-LDP) and resource ReSerVation Protocol with Traffic Engineering (RSVP-TE) are ones for signaling, and Link Management Protocol (LMP) and the protocol proposed here are candidates for link management.

- Active control channels: Physical control channels which are currently carrying the control information. An active control channel becomes a standby control channel when it can not carry the control information due to a failure.

- Standby control channels: Physical control channels which are not currently carrying the control information, but can carry them upon the failure of active control channel. Once one of standby control channels is used to carry the control information, the standby control channel becomes an active control channel.

- Physical control channels: Physical links used to carry control information, for examples, a separate wavelength or fiber, an Ethernet link, an Internet Protocol (IP) tunnel through a separate management network, or the overhead bytes of a data link. In this proposal, as a more extended concept, all links of in-fiber in-bend, in-fiber out-of-bend, and out-of-fiber can be physical control channels.

- Protection group: A set of physical control channels using the same type of network configuration or belonging to similar aspects within the control network configuration.

2. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in BCP 14, RFC 2119 and indicate requirement levels for compliant implementations.

3. Control Networks
In current IP networks, there is no explicit concept of control network. Instead there is the implicit concept of that. However, the terminology, called "control plane", gets acquainted in the IP world. The control plane represents aspects of control networks comprising control channels, control entities and control nodes used to transport control packets of signaling, link management, and routing protocols. In a sense of terminology, control plane is a set of communicating entities that are responsible for the establishment of connections including set-up, release, supervision and maintenance. A control plane is supported by a signaling network, in other words, a control network.

In traditional IP networks or MPLS networks, there is an implicit one-to-one association of a control channel to a data channel. Under the one-to-one association between control channels and data channels, the protection of control channels may be resolved using the protection schemes for data channels such as 1+1, 1:1, and 1:N protections. In other words, where there is fate sharing, failures of data channels could instantly influence the own control channels. However, as described in [GMPLS-ARCH], a control channel can be separated from the data channel in GMPLS. To allow for the control channels between adjacent nodes to be separated from the associated data-bearing links means that there is not a one-to-one association between a control channel and a data channel. It means that failures of data channels could not influence the own control channels any more.

As indicated in [ITU-G807], a control network (as a narrow meaning, signaling network) supports control plane by the act of transferring service-related information between the user and the network and also between network entities. The control network can be constructed using common control signaling, thereby allowing a network operator to have the capability of developing a separate control network. According to this document, control channels are associated with data channels in the following ways:

- Associated mode in which control packets between network elements are transferred over control channels that directly connect the network elements such as transport channels;

- Quasi-associated mode in which control packets between nodes A and B follow a predetermined routing path over several control channels while the traffic channels are routed directly between A and B;

- Non-associated mode in which control packets between two network elements A and B are routed over several control channels, while traffic signals are routed directly between A and B. The control
channels used may vary with time and network conditions. This mode has two types of control channels, non-associated mode with internal network and non-associated mode with external network. The internal case says that control channels are connected each other under the similar configuration of its transport network, but the external case says that control channels are connected each other via other network that is definitely different from the configuration of its transport network.

On the one hand, as defined by the Optical Internet Forum (OIF), control channel configurations to carry control packets over Synchronous Optical NETwork (SONET) and Synchronous Digital Hierarchy (SDH), Optical Transport Network (OTN), and Ethernet include two types of the following:

- In-fiber configuration in which control packets are carried over a control channel embedded in the data-carrying link between network elements;

- Out-of-fiber configuration in which control packets are carried over a dedicated control channel between adjacent nodes, which is separated from the data-bearing links.

In the case of in-fiber configuration above, we can expand this configuration and apply it to the out-of-fiber configuration that a control channel within a fiber that includes transport channels can handle transport channels in the fiber itself as well as other fibers.

In addition, a similar concept to a control network can be found in the Signaling Communication Network (SCN) within the Automatic Switched Transport Network (ASTN) in [ITU-G7712]. There may be several physical implementations for the SCN. For example, Embedded Control Channels (ECC) interfaces, Local Area Network (LAN) interfaces, and Wide Area Network (WAN) interfaces are possible.

Then, there is an important indication for the resilience of control plane. Common to each topology is that alternative diverse paths exist between the entities. Although a failure occurs over a signaling link between adjacent nodes on the topology, one or more alternative paths disjointed or indifferent to the failed link can be identified. To use the most of possible control channels would have an important role for the resilience of control plane.

Here, the resilience of control plane refers to the ability of a control network to maintain an acceptable level of control services during failures of communicating entities. Also, the resilience of control channels means the protection and switchover capability that can configure one or more signaling routes between adjacent nodes within a control network or between control networks, and allow
control packets to be exchanged within a threshold against the failure of one or more control channels.

4. Necessities for Resilience of Control Channels

As recognized in the IP world, IP routing protocols have slow convergence time due to the hello interval and expiration times for the normal operation of IP networks. Under this situation, fast and reliable recovery is very difficult from one or more failures occurred over interfaces between adjacent nodes. Then, why is the fast and reliable recovery of control channels needed? There is a reason that the failure of control channels would affect new connection set-up, connection tear-down, and fault report. In addition, control channels could include control packets for link management protocol, routing protocols as well as control packets of other IP control protocols, according to the application level into those. In this circumstance, the fast and reliable communication environment would be a very important factor in controlling IP networks stably.

However, if there is no resilience capability of control channels even though there is a possibility being capable of sufficiently using the nature of a network, the early determination that there are no more control channels within a network may cause problems like the communication suspension between control entities even though data channels are running well. When RSVP variant protocols are used between adjacent nodes, if there is no self-refresh procedure, the failure of control channels may result effects such as unwanted connection teardown. In particular, as described in [ITU-G7712], such a failure that could not transport ASTN messages over the SCN may impact restoration when ASTN is used to provide restoration of existing connections. It is therefore critical for a control network to provide the resilience of control channels that could sufficiently use direct and indirect ones between adjacent nodes.

Those channels could be classified into two groups roughly, direct (similar to the associated mode) and indirect interfaces. More specifically, the indirect case could be classified into indirect interfaces using direct interfaces (similar to the quasi-associated mode) and other indirect interfaces including internal or external networks (similar to the non-associated modes).

Here, a network can provide protection and switchover functions of various levels based on configuration schemes and physical characteristics of links to be used to exchange control packets between adjacent nodes. For examples, for the resilience of control channels, the control channel management (CCM) function of LMP could
be extended, or MPLS 1+1 LSPs using the dual-feed and selection scheme could be applied.

5. Requirements for Resilience of Control Channels

To introduce resilience capabilities into control channels, several requirements have to be identified according to schemes addressed above.

5.1 Requirements for MPLS 1+1 LSPs

For this scheme, control entities should establish two LSPs to be used as control channels using signaling protocol such as a RSVP or LMP variant protocol. Control packets shall be sent with the same sequence number and the same contents over two LSPs between adjacent nodes. The sequence number shall be used as the identifier for packet 1+1 protection, and is located after the 4-bytes MPLS encapsulation header. Then, a receiving node of these control packets would ignore a control packet that arrives late with the same sequence number. This section is based on [ITU-G7712].

5.2 Requirements for LMP-CCM Extension

1) Configuration of control networks

The support of the resilience capability of control networks though the LMP extension requires either that the number of control channels between adjacent nodes has to be greater than one, and there has to be at least one active control channel and more than one standby control channel. The important point is that adjacent nodes that want to exchange control packets should in advance know their physical characteristics of control channels and control modes such as associated, non-associated, or quasi-associated.

For this scheme, it is to keep a single active control channel and one or more standby control channels. When a failure occurs at an active control channel, a node would switch the failed control channel over to the one of standby control channels using provisioning rules and negotiation results between nodes. Then, one among several standby control channels turns into an active control channel instead of the previous active control channel.

The distribution of control packet types into more than one control channel may be possible, but this case requires further study. For this case, the switchover function of control channels should in advance know control packet types that a control channel carries. In order to simplify our approach in the problem domain, it is assumed...
that a single control channel carries all control packets such as routing, signaling, and link management.

2) Protection Groups of Control Networks

We assign control channels of the associated mode to the PG-1, assign control channels of the quasi-associated mode to the PG-2, and finally assign control channels of the non-associated mode to the PG-3. Such as, a set of data channels in a transport network can be PG-1 and PG-2 control channels. In addition, the PG-3 control channels have to be able to control security options according to its network environment.

Nodes over a PG-3 route might not detect the condition of an unavailable control channel because they do not have the function of control channel management. On a failure of control channel over the detour route, there may be a situation that the availability of a control channel can not be guaranteed within a proper timing limit. Also, different addressing scheme of control channels among PGs can be applied, and the same addressing scheme of control channels within a PG should be applied.

3) Relay of Control Packets in a Transit Node

In other modes except for the associated mode, there is a possibility that control packets can be traversed via one or more transit nodes in order to guarantee the safe transfer of control packets between real adjacent nodes. In this case, if a node is not the destination node of being capable of receiving control packets, the node must relay those packets over a control channel connected with a succeeding node.

6. Functions for LMP-CCM Extension

6.1 Identification of PG-1 and PG-3 Control Channel

This function allows two adjacent nodes to configure the communication environment of PG-1 and PG-3 control channels. Its procedure to identify active and standby control channels differs from the way how to connect physical links between nodes. That is, in case of point-to-point connection, control channels are identified using a multicast address, and in other cases, they are identified using an unicast address.
6.2 Identification of Detour Control Channels

This function is used to configure a more powerful control network after the identification of PG-1 and PG-3 control channels. This is to establish a detour route using PG-1 or PG-3 control channels over one or more transit nodes between adjacent nodes. Note that the detour route is established using ACCs of the PG-1 or PG-3 configured previously between other adjacent nodes.

6.3 Automatic Switchover

When a failure on the ACC in use occurs, this function is used to switchover to a control channel that first responds to the switchover request (called multicast switchover).

Switchover messages are multicast via all standby control channels except for the current ACC between adjacent nodes. Especially, when switchover group messages are exchanged over a detour route, they have to be forwarded at the IP layer of a transit node, and have not to be gone up the application layer.

6.4 Forced Switchover

Differently from the automatic switchover, this function is used to switchover a control channel compulsorily for the purpose of operation and administration via an intervention of operator.

6.5 Recovery from Failure

On recovery from the previous failure, the control channel performs the process of connectivity verification of the control channel using the identification of PG-1 and 3 control channels. Then, the control channel becomes a SCC.

6.6 Notification of Control Channel Unavailability

This function is used to notify that there is no ACC to forward control packets towards the terminating node due to subsequent failures of other ACCs. This is called, DCC full down. A message is used for the notification. If the node that is notified the unavailability of control channels is not the original node, this process of relaying the message is repeated until the original node receives the message.
6.7 Inquiry of Switchover Attributes

This function is used to retrieve the protection and switchover attributes of control channels over an ACC between adjacent nodes, which are kept in its peer.

The protection and switchover attributes of control channels can be classified into the ACC attributes and SCC ones. Accordingly, the original node and its terminating node can identify if the own node has the same attributes with its peer except for DCC related contents.

6.8 Hello Initiation

This function is the same one to that in the LMP specification.

6.9 Notification of Protocol Errors

A functional entity for the resilience of control networks should check protocol error conditions as a general rule before acting upon a message after receiving the message from the peer entity. If there is no protocol error within the received message, resultant operations would be performed. However, if a protocol error occurs, the receiving entity should notify the sending entity of the situation using a message, and there is no action against the received message.

7. Security Considerations

This document does not introduce any new security considerations.

8. IANA Considerations

This document does not contain any IANA actions.

9. References

9.1 Normative References


9.2 Informative References


Author’s Addresses

Young Hwa Kim
yhwkim@etri.re.kr
161 Gajeong-Dong Yuseong-Gu, Deajon 305-350, Korea

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity