International Telecommunication Union

ITU-T G.8032/Y.1344

(06/2008)

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

SERIES G: TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

Packet over Transport aspects – Ethernet over Transport aspects

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Internet protocol aspects – Transport

Ethernet ring protection switching

Recommendation ITU-T G.8032/Y.1344

ITU-T G-SERIES RECOMMENDATIONS

TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

INTERNATIONAL TELEPHONE CONNECTIONS AND CIRCUITS	G.100–G.199
GENERAL CHARACTERISTICS COMMON TO ALL ANALOGUE CARRIER-TRANSMISSION SYSTEMS	G.200–G.299
INDIVIDUAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON METALLIC LINES	G.300–G.399
GENERAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON RADIO-RELAY OR SATELLITE LINKS AND INTERCONNECTION WITH METALLIC LINES	G.400–G.449
COORDINATION OF RADIOTELEPHONY AND LINE TELEPHONY	G.450–G.499
TRANSMISSION MEDIA AND OPTICAL SYSTEMS CHARACTERISTICS	G.600–G.699
DIGITAL TERMINAL EQUIPMENTS	G.700–G.799
DIGITAL NETWORKS	G.800–G.899
DIGITAL SECTIONS AND DIGITAL LINE SYSTEM	G.900–G.999
MULTIMEDIA QUALITY OF SERVICE AND PERFORMANCE – GENERIC AND USER-RELATED ASPECTS	G.1000–G.1999
TRANSMISSION MEDIA CHARACTERISTICS	G.6000–G.6999
DATA OVER TRANSPORT – GENERIC ASPECTS	G.7000–G.7999
PACKET OVER TRANSPORT ASPECTS	G.8000–G.8999
Ethernet over Transport aspects	**G.8000–G.8099**
MPLS over Transport aspects	G.8100–G.8199
Quality and availability targets	G.8200–G.8299
Service Management	G.8600–G.8699
ACCESS NETWORKS	G.9000–G.9999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T G.8032/Y.1344

Ethernet ring protection switching

Summary

Recommendation ITU-T G.8032/Y.1344 defines the automatic protection switching (APS) protocol and protection switching mechanisms for ETH layer Ethernet ring topologies. Included are details pertaining to Ethernet ring protection characteristics, architectures and the ring APS protocol.

Source

Recommendation ITU-T G.8032/Y.1344 was approved on 22 June 2008 by ITU-T Study Group 15 (2005-2008) under Recommendation ITU-T A.8 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Recommendation ITU-T G.8032/Y.1344

Ethernet ring protection switching

1 Scope

This Recommendation defines the automatic protection switching (APS) protocol and protection switching mechanisms for ETH layer Ethernet ring topologies. The protection protocol defined in this Recommendation enables protected point-to-point, point-to-multipoint and multipoint-to-multipoint connectivity within the ring or interconnected rings, called "multi-ring/ladder network" topology.

The ETH layer ring maps to physical layer ring structure.

Protection schemes for the other layers, including ETY layer, are out of scope of this Recommendation.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation

[ITU-T G.805] Recommendation ITU-T G.805 (2000), *Generic functional architecture of transport networks.*

[ITU-T G.806] Recommendation ITU-T G.806 (2004), *Characteristics of transport equipment – Description methodology and generic functionality.*

[ITU-T G.808.1] Recommendation ITU-T G.808.1 (2006), *Generic protection switching – Linear trail and subnetwork protection.*

[ITU-T G.809] Recommendation ITU-T G.809 (2003), *Functional architecture of connectionless layer networks.*

[ITU-T G.870] Recommendation ITU-T G.870/Y.1352 (2004), *Terms and definitions for optical transport networks (OTN).*

[ITU-T G.8010] Recommendation ITU-T G.8010/Y.1306 (2004), *Architecture of Ethernet layer networks.*

[ITU-T G.8021] Recommendation ITU-T G.8021/Y.1341 (2007), *Characteristics of Ethernet transport network equipment functional blocks.*

[ITU-T Y.1731] Recommendation ITU-T Y.1731 (2008), *OAM functions and mechanisms for ethernet based networks.*

[IEEE 802.1Q] IEEE 802.1Q-2005, *IEEE Standard for local and metropolitan area networks – virtual bridged local area networks.* <http://www.ieee802.org/1/pages/802.1Q.html>

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 Terms defined in [ITU-T G.805]:

a) adapted information
b) characteristic information
c) link
d) tandem connection
e) trail

3.1.2 Terms defined in [ITU-T G.806]:

a) defect
b) failure
c) Server signal fail (SSF)
d) Signal degrade (SD)
e) Signal fail (SF)
f) Trail signal fail (TSF)

3.1.3 Term defined in [ITU-T G.808.1]:

a) transfer time (T_t):

3.1.4 Terms defined in [ITU-T G.809]:

a) adaptation
b) flow
c) layer network
d) network
e) port
f) transport
g) transport entity

3.1.5 Terms defined in [ITU-T G.870]:

a) APS protocol
b) holdoff time
c) non-revertive operation
d) protection
e) protected domain
f) revertive operation
g) signal
h) switch
i) switching time

j) Transport entity:
   – Transport protection entity
   – Working transport entity

k) wait-to-restore time

3.1.6 Terms defined in [ITU-T G.8010]:

a) Ethernet characteristic information (ETH_CI)

b) Ethernet flow point (ETH_FP)

3.1.7 Terms defined and described in [ITU-T G.8010] and [ITU-T Y.1731]:

a) maintenance entity (ME)

b) maintenance entity group (MEG)

c) maintenance entity group end point (MEP)

d) maintenance entity group level (MEL)

3.1.8 Terms defined in [ITU-T G.8021]:

a) Ethernet connection function (ETH_C)

b) Ethernet MAC characteristic information server signal fail (ETH_CI_SSF)

c) Ethernet flow forwarding function (ETH_FF)

d) ETH to ETH multiplexing adaptation function (ETHx/ETH-m_Sk)

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 Ethernet ring: An Ethernet ring is a collection of Ethernet ring nodes forming a closed loop, whereby each node is connected to two adjacent nodes via a duplex communications facility.

3.2.2 Ethernet ring node: An Ethernet ring node is a network element which implements at least the following functionalities:

– One Ethernet connection function (ETH_C) with a dedicated Ethernet flow forwarding function (ETH_FF) for forwarding R-APS control traffic.

– Two ring ports, including ETHDi/ETH Adaptation function at the ring maintenance entity group level (MEL).

– Ethernet ring protection (ERP) control process controlling blocking and unblocking of traffic over the ring ports.

3.2.3 ring protection link (RPL): The ring protection link is the ring link which under normal conditions, i.e., without any failure or request, is blocked (at one end or both ends) for traffic channel, to prevent the formation of loops.

3.2.4 RPL owner: The RPL owner is an Ethernet ring node adjacent to the RPL that is responsible for blocking its end of the RPL under normal conditions (i.e., the ring is established and no requests are present in the ring).

3.2.5 ring MEL: The ring MEL is the maintenance entity group (MEG) level providing a communication channel for ring automatic protection switching (R-APS) information.

4 Abbreviations

This Recommendation uses the following abbreviations:

AI Adapted Information

APS Automatic Protection Switching

CCM Continuity Check Message

CI Characteristic Information

DNF Do Not Flush

ETH Ethernet layer network

ERP Ethernet Ring Protection

FDB Filtering Database

LSB Least Significant Bit

MEG Maintenance Entity Group

MEL Maintenance Entity group Level

MEP Maintenance Entity group End Point

MI Management Information

MIP Maintenance entity group Intermediate Point

NR No Request

OAM Operation, Administration and Maintenance

PDU Protocol Data Unit

R-APS Ring APS

RB RPL Blocked

RPL Ring Protection Link

SD Signal Degrade

SF Signal Fail

VID VLAN Identifier

VLAN Virtual LAN

WTR Wait to Restore

5 Conventions

5.1 Representation of octets

Octets are represented as defined in [ITU-T Y.1731].

When consecutive octets are used to represent a binary number, the lower octet number has the most significant value.

The bits in an octet are numbered from 1 to 8, where 1 is the least significant bit (LSB) and 8 is the most significant bit (MSB).

6 Introduction

This Recommendation specifies protection switching mechanisms and protocol for Ethernet layer network (ETH) Ethernet rings. Ethernet rings can provide wide-area multipoint connectivity more economically due to their reduced number of links. The mechanisms and protocol defined in this Recommendation achieve highly reliable and stable protection; and never form loops, which would fatally affect network operation and service availability.

Each ring node is connected to adjacent nodes participating in the same ring, using two independent links. A ring link is bounded by two adjacent nodes and a port for a ring link is called a ring port. The minimum number of nodes on a ring is two.

The fundamentals of this ring protection switching architecture are:

- the principle of loop avoidance, and
- the utilization of learning, forwarding, and address table mechanisms defined in the Ethernet flow forwarding function (ETH_FF).

Loop avoidance in the ring is achieved by guaranteeing that, at any time, traffic may flow on all but one of the ring links. This particular link is called the ring protection link (RPL), and under normal conditions this link is blocked, i.e., not used for traffic. One designated node, the RPL owner, is responsible to block traffic over the RPL. Under a ring failure condition, the RPL owner is responsible to unblock the RPL, allowing the RPL to be used for traffic.

NOTE – Blocking traffic on the RPL by both of its adjacent nodes is for further study.

The event of a ring failure results in protection switching of the traffic. This is achieved under the control of the ETH_FF functions on all ring nodes.

An APS protocol is used to coordinate the protection actions over the ring.

The Ethernet rings could support a multi-ring/ladder network that consists of conjoined Ethernet rings. The protection switching mechanisms and protocol defined in this Recommendation shall be applicable for multi-ring/ladder network. Details of this topology are for further study.

7 Ring protection characteristics

7.1 Monitoring methods and conditions

Ring protection switching occurs based on the detection of defects on the transport entity of each ring link. The defects are defined within equipment Recommendations [ITU-T G.8021]. For the purpose of the protection switching process, a transport entity within the protected domain has a condition of failed (i.e., signal fail (SF)) or non failed.

Ethernet ring protection may adopt any of the following monitoring methods:

Inherent – The fault condition status of each link connection is derived from the status of the underlying server layer trail.

Sub-layer – Each ring link is monitored using tandem connection monitoring (TCM).

Test Trail – Defects are detected using an extra test trail, i.e., an extra test trail is set up along the ring.

The protection switching is agnostic to the monitoring method used, as long as it can be given (OK or SF) information for the transport entity of each ring link.

7.2 Ethernet traffic and bandwidth consideration

It is desirable that ring bandwidth accommodates all traffic that is protected, regardless of the ring protection switching state. Being different from linear protection, ERP does not separate working and protection transport entities, but reconfigures the transport entity during protection switching. Therefore, care should be taken that ring link capacity can continue to support all ring traffic that is protected after protection switching.

7.3 Protection switching performance

In an Ethernet ring, without congestion, with all nodes in the idle state (i.e., no detected failures, no active automatic or external commands, and receiving only "NR, RB" R-APS frames), with less than 1'200 km of ring fibre circumference, and fewer than 16 nodes, the switch completion time (transfer time) for a failure on a ring link shall be less than 50 ms. On rings under all other conditions, the switch completion time may exceed 50 ms (the specific interval is under study), to allow time to negotiate and accommodate coexisting APS requests.

8 Ring protection conditions and commands

This Recommendation supports the following conditions of the Ethernet ring:

Signal failure (SF) – When a SF condition is discovered on the ring link, and it is determined to be a "stable" failure, this condition causes the nodes adjacent to the failed ring link to initiate the protection mechanism described in this Recommendation.

Wait to restore – In a revertive operation, after the clearing of an SF condition on a ring link with a defect, maintains the position of the blocked port of the ring link until a wait to restore (WTR) timer expires. An RPL owner will initiate reversion when the WTR timer expires, prior to any other higher priority event or command. This is used to prevent frequent switching operations that may be caused by intermittent failures.

No request – The condition entered by the local priority under all conditions where no local protection switching requests (including wait-to-restore and do-not-revert) are active.

The following commands are for further study:

Lockout of protection – This command disables the protection group.

Force switch – This command moves the blocking role of the RPL by blocking a different ring link followed by unblocking the RPL.

Manual switch – In the absence of a failure, this command moves the blocking role of the RPL by blocking a different ring link and unblocking the RPL.

Replace the RPL – This command moves the RPL by blocking a different ring link and unblocking the RPL permanently.

Exercise signal – Exercise of the APS protocol. The signal is chosen so as not to modify the position of the blocked port.

Do not revert – In non-revertive operation, this is used to maintain the position of the blocked port.

Clear – Clears the active near commands.

9 Ring protection architectures

In the ring protection architecture defined in this Recommendation, protection switching is performed at all ring nodes.

The ring protection architecture relies on the existence of an APS protocol to coordinate ring protection actions around the ring.

9.1 Revertive and non-revertive switching

In revertive operation, the traffic channel is restored to the working transport entity, i.e., blocked on the RPL, after the condition(s) causing a switch has cleared. In the case of clearing of a defect, the traffic channel reverts after the expiry of a "Wait to Restore" timer, which is used to avoid toggling protection states in the case of intermittent defects.

In non-revertive operation, the traffic channel is allowed to use the RPL, if it is not failed, after a switch condition has cleared.

Since in Ethernet ring protection the working transport entity resources may be more optimized, in some cases it is desirable to revert to the normal path once all ring links are available. This is performed at the expense of an additional traffic interruption.

In some cases, there may be no advantage to revert to the normal working transport entities immediately. In this case, a second traffic interruption is avoided by not reverting the protection switching.

The non-revertive switching mechanism is for further study.

9.2 Protection switching triggers

Protection switching shall be performed when:

– SF is declared on one of the ring links, and the detected SF condition has a higher priority than any other local request or far-end request; or

– The received APS protocol requests to switch and it has a higher priority than any other local request.

NOTE – Protection switching initiated by operator control (e.g., manual switch) is for further study.

9.2.1 Signal fail declaration conditions

SF is declared when an ETH trail signal fail condition is detected. ETH trail signal fail is specified in [ITU-T G.8021].

9.3 Protection switching models

Figure 9-1 depicts an example of the ring protection model defined in this Recommendation. Other network scenarios are permissible. In this example, four ring nodes are depicted.

If the ring is in its normal condition, one node adjacent to the RPL is configured to block the transmission and reception of traffic over the RPL when there is no request on the ring. This node is called the *RPL Owner*.

In Figure 9-1, Node D is responsible for blocking the traffic channel on the RPL. Figure 9-1 presents the case when no failures are present on any ring links. In this case, the ETH characteristic information (ETH_CI) traffic may be transferred over both ring links of any node, except for the RPL on the node where the RPL is blocked. In this figure, the traffic channel is shown as arrows being transmitted and received from the ring links. In the following figures, only the ETH_FF function for one VLAN is represented.

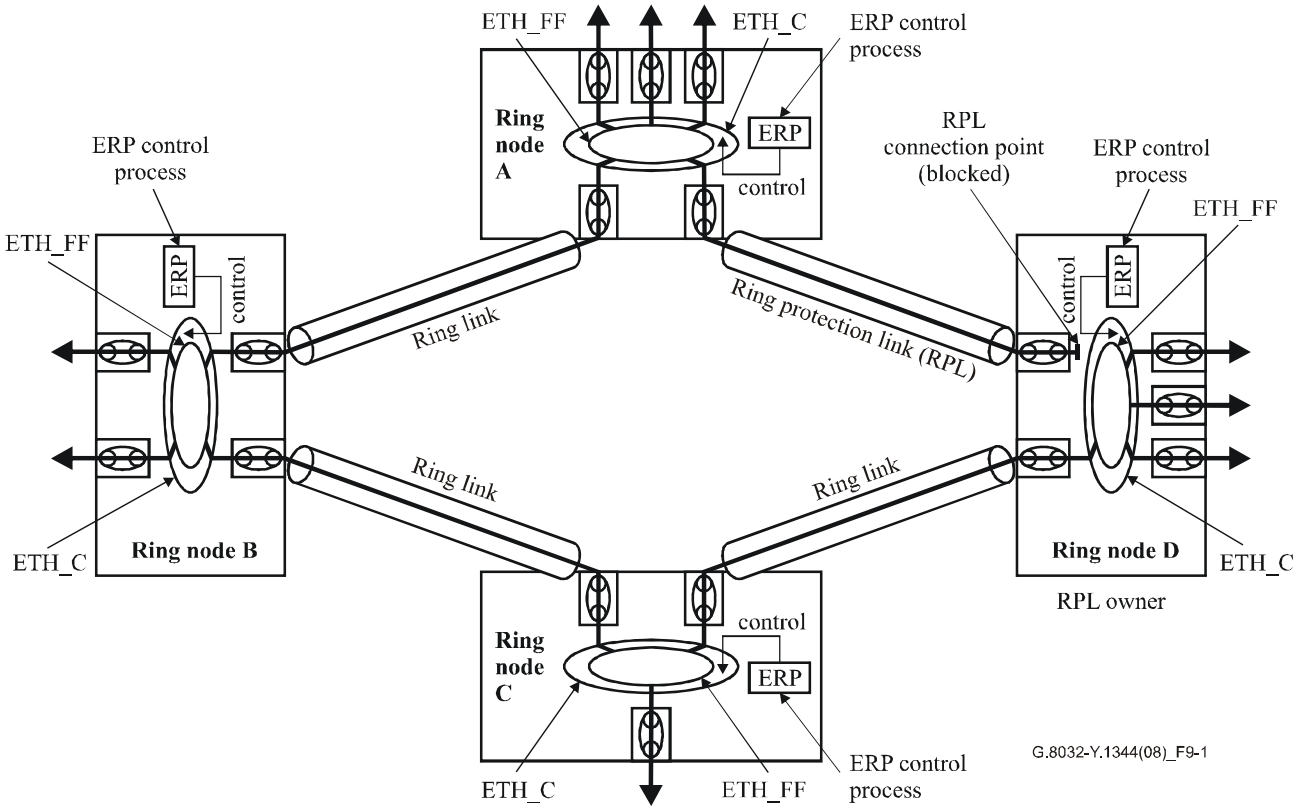

Figure 9-1 – Ethernet ring protection switching architecture – Normal condition

Figure 9-2 illustrates a situation where a protection switch has occurred due to a signal-fail condition on one ring link. In this case, traffic channel is blocked bidirectionally on the ports where the failure is detected and bidirectionally unblocked at the RPL connection point.

In a revertive operation, when the failure is recovered from, the traffic channel will resume the use of the recovered ring link only after the traffic channel has been blocked on the RPL.

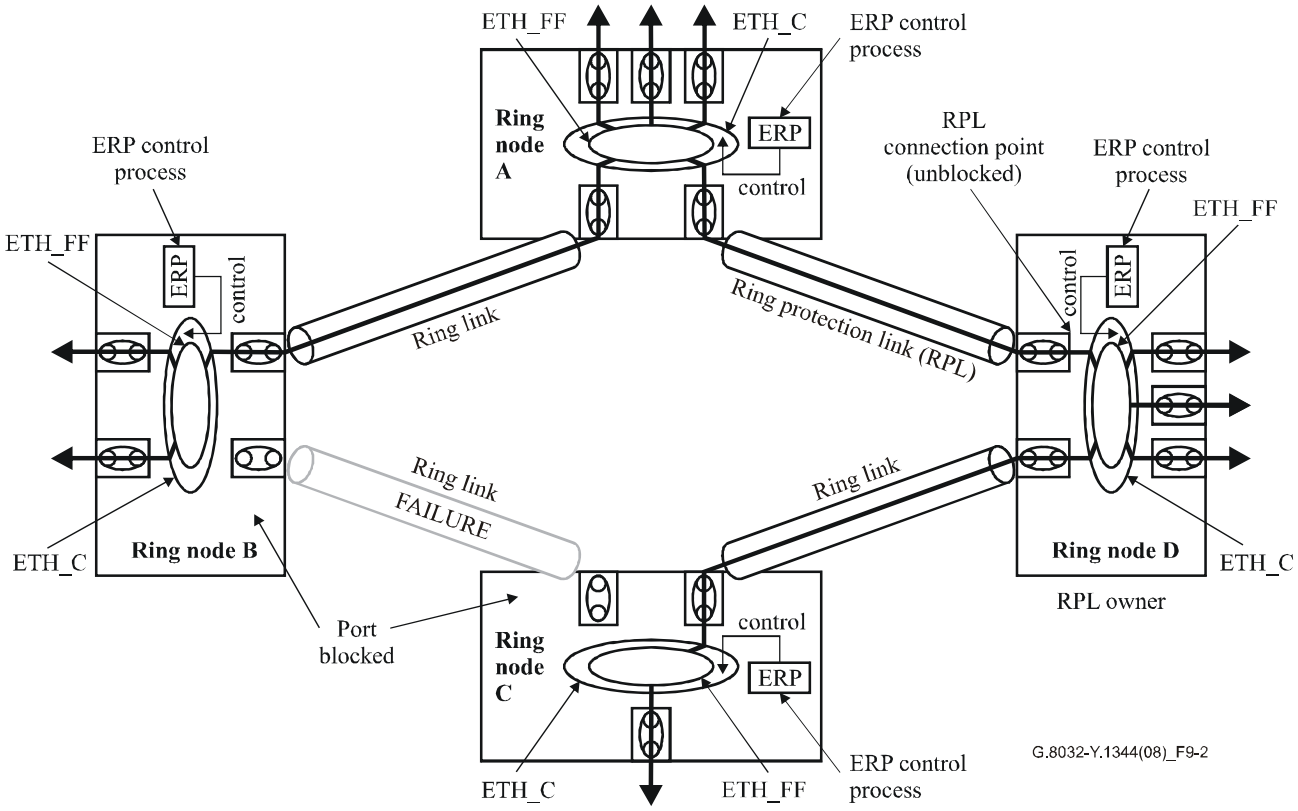

Figure 9-2 – Ethernet ring protection switching architecture – Signal fail condition on one ring link

A model for the functionality of a ring node is presented in Figures 9-3 and 9-4.

The Ethernet ring protection control process is instantiated to protect normal traffic over the ring. Each instantiated ETH_FF function determines the specific output Ethernet flow point (ETH_FP) over which the ETH_CI is transferred. The ETH_CI may be forwarded over any ETH_FP corresponding to the ring links or to non-ring links.

The ERP control process controls the ETH_FF function so as to perform actions such as to disable forwarding over any ETH_FP corresponding to blocked ring links, and to flush the learned MAC address table.

As an example, the ring links of each node may be monitored by individually exchanging continuity check messages (CCM) defined in [ITU-T Y.1731] on the maintenance entity group end points (MEP) shown in Figure 9-3.

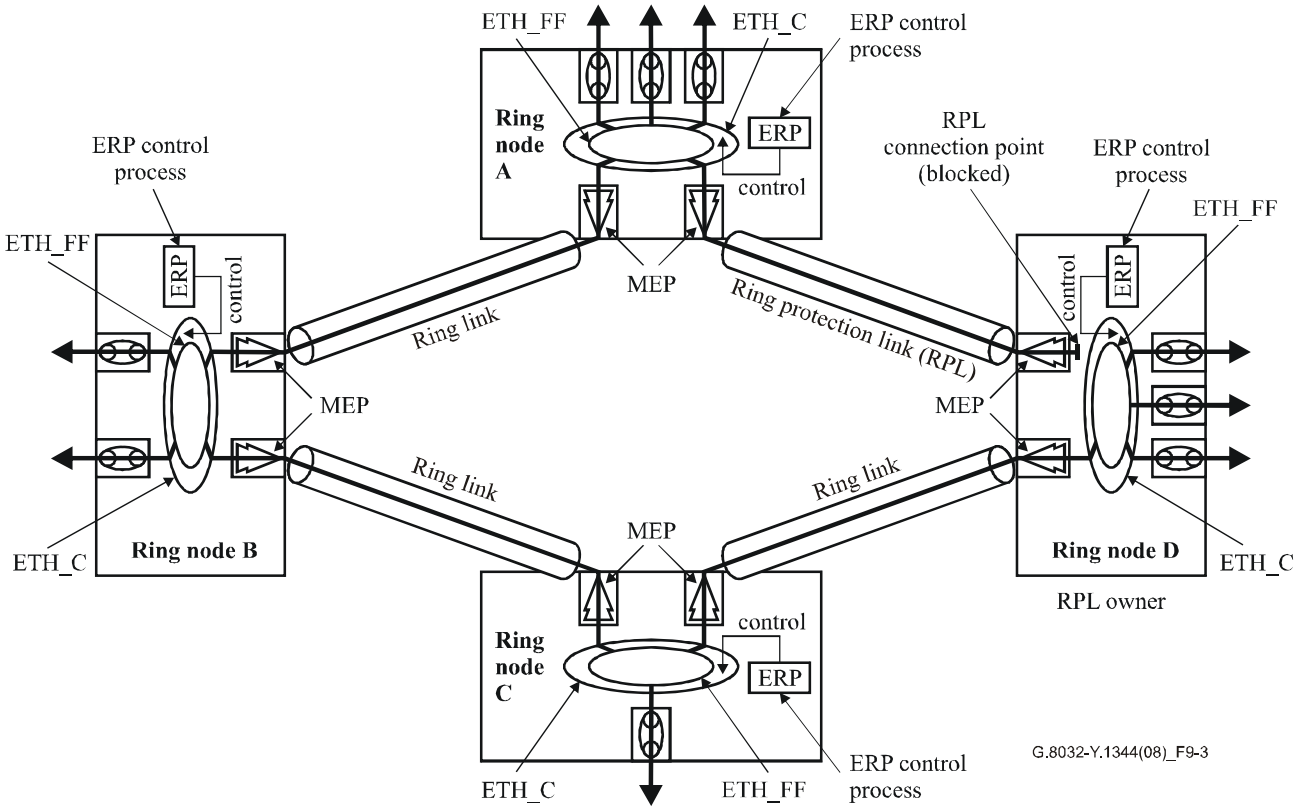

Figure 9-3 – MEPs in Ethernet ring protection switching architecture

Figure 9-4 represents the model of a ring node. The MEPs represented on each ring port are used for monitoring the ring link.

If a MEP detects a defect, which contributes to an SF defect condition, this will inform the ERP control process that a failure condition has been detected. An ERP control function uses the ETH_CI_SSF information, forwarded from the ETHx/ETH-m_A_Sk, to assert the signal-fail condition of the ring link.

The ring protection mechanism requires the APS protocol to coordinate the switching behaviour among all ring nodes. The ring APS protocol communication is performed using R-APS PDUs. R-APS PDUs are transmitted and received at an ERP control process. The ETHDi/ETH_A function (see Appendix III) extracts ETH_CI_RAPS information from the received RAPS_PDUs and sends the ETH_CI_RAPS information to the ERP control process. The received RAPS_PDU is also forwarded towards the ETH_FF. The ETHDi/ETH_A function also generates RAPS_PDUs using the ETH_CI_RAPS information received from the ERP control process.

Ring APS messages are forwarded using an ETH_FF function for R-APS traffic, represented in Figure 9-4 as R-APS_FF. Other traffic is forwarded by use of other ETH_FF functions, represented in Figure 9-4 as Service_FF. R-APS messages use a dedicated VLAN. Only one traffic VLAN is depicted in Figure 9-4. More traffic VLANs could be supported using multiple service_FFs.

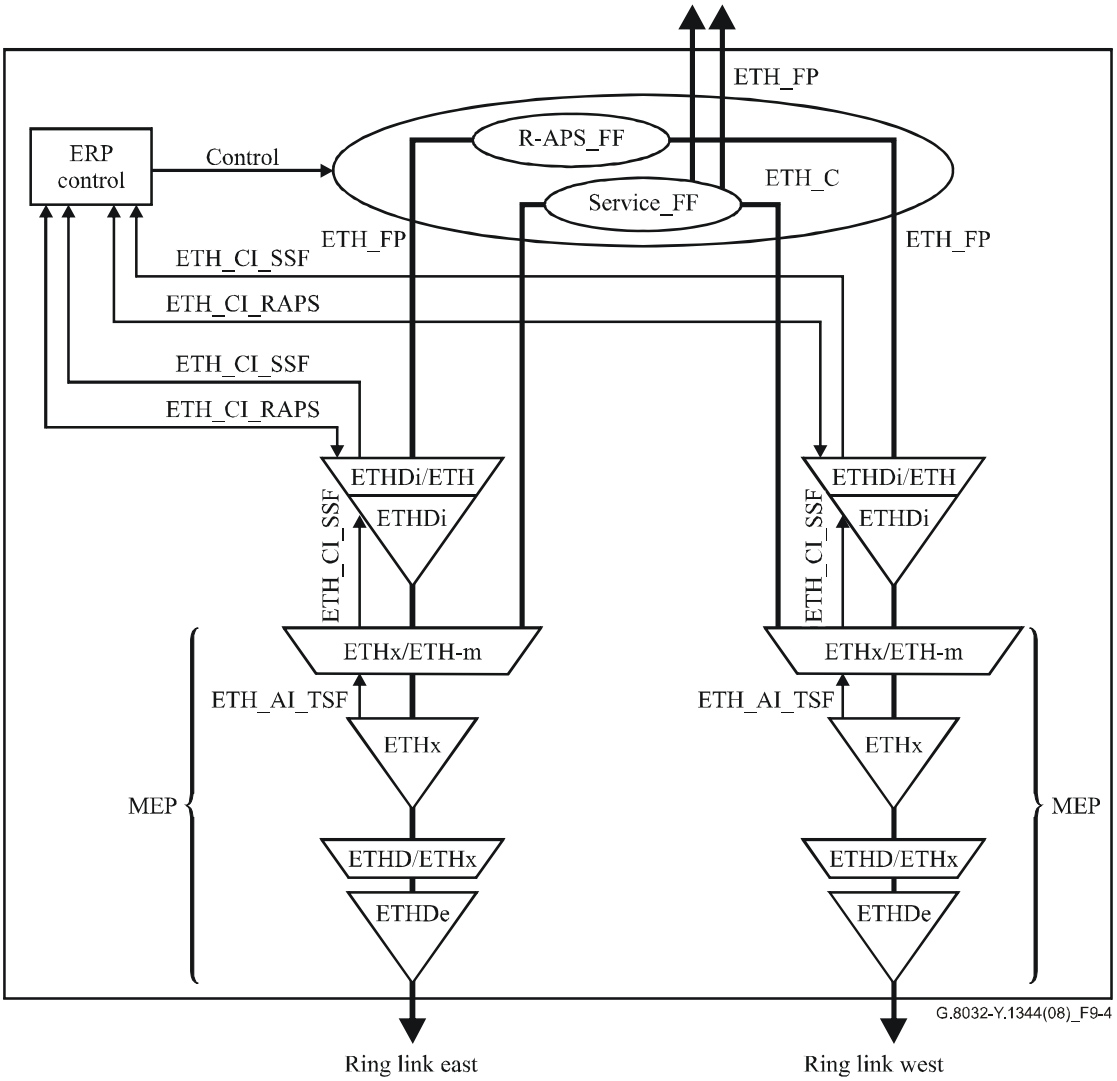

Figure 9-4 – MEPs and R-APS insertion function in ring node

9.4 Traffic channel blocking

Blocking traffic is supported by excluding the connection point from the ETH_FF functions for one or more VLAN IDs of the (service) traffic channel. This is equivalent to VID filtering as defined in [IEEE 802.1Q], c8.13.10. This results in blocking the transmission and reception of traffic on one ring port.

9.5 R-APS channel blocking

R-APS channel VLAN traffic forwarding is always blocked at the same ports where traffic channel is blocked. It is supported by excluding the connection point from the ETH_FF function for the VLAN ID of the R-APS traffic and is equivalent to perform VID filtering as defined in [IEEE 802.1Q], c8.13.10. This only prevents R-APS messages received at one ring port from being forwarded to the other ring port. This, however, does not prevent R-APS messages, locally generated at the ERP control process, from being transmitted over both ring ports, and also allows R-APS messages received at each port to be delivered to the ERP control process.

9.6 FDB flush

A filtering database (FDB) flush consists of removing the learned MAC addresses of the ring ports from the node's filtering database.

NOTE – The inclusion of the completion of FDB flush operation within the transfer time is for further study.

9.7 Multi-ring/ladder networks

Multi-ring/ladder networks are for further study.

10 Protection control protocol

Ring protection is based on loop avoidance. This is achieved by guaranteeing that at any time traffic may flow on all but one of the ring links. From this principle, the following rule is derived for the protocol:

Once a port has been blocked, it may be unblocked only if it is known that there remains at least one other blocked port in the ring.

This rule is taken as the basis to control all actions of traffic channel unblocking in the ring, as well as to define the information that is necessary to distribute between all ring nodes.

10.1 Principles of operations

Figure 10-1 shows a decomposition of the Ethernet ring protection control process. This process is performed at all ring nodes.

The protection algorithm is based on the transmission of local switch requests and local status to all ring nodes via the R-APS specific information. Format and content for the R-APS PDU are described in clause 10.3.

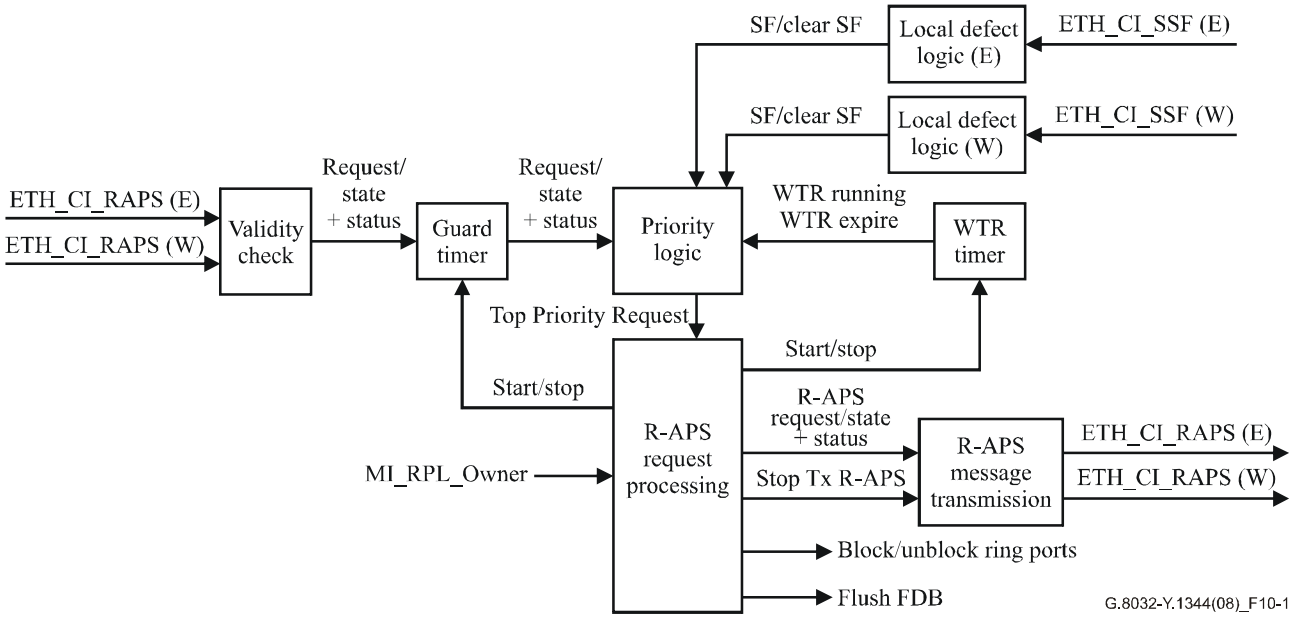

Figure 10-1 – Decomposition of Ethernet ring protection control process

The following is an overview of the Ethernet ring protection control process. The behaviour of each sub-process is described in detail in the following subclauses.

The status of the local ring node's ring ports is evaluated according to the methods defined in clause 9.2.1. This information is passed on to the local defect logic for each of the node's ports. The local defect logic evaluates these signals, processes the holdoff timer and passes them to the priority logic.

The local ring node receives information from the other ring nodes via R-APS messages. Validity check, as described in clause 10.1.6, verifies that the R-APS message is correctly constructed. The received Request/State and Status information (which indicates the top priority request and status of other ring nodes) is then passed to the guard timer.

The guard timer functionality is described in clause 10.1.5. While the guard timer is running the received R-APS Request/State and Status information is not forwarded to the priority logic entity. If the guard timer is not running, the R-APS Request/State and Status information is forwarded to the priority logic entity.

The functionality of a WTR timer entity is described in clause 10.1.4. While the WTR timer is running, the WTR running information is input to the priority logic. The expiration of the WTR timer is indicated as the event WTR expire to the priority logic entity.

An R-APS message is defined as accepted if the message passes the validity check, is passed by the guard timer to the priority logic, and is the current highest priority request signalled to the R-APS request processing logic.

The priority logic accepts as inputs:

a) the R-APS Request/State and Status information (after screening by the validity check and the guard timer);

b) status and events from the WTR timer; and

c) status of the local ring node's ring ports.

It processes the priority according to Table 10-1 to determine the highest priority signal.

The MI_RPL_Owner represents the management information describing if the local node is an RPL owner or not, and in the case that this is an RPL owner it specifies which port is the RPL.

The R-APS request processing will receive the current top priority request and defines the necessary actions to take based on the local ring node state. These actions include transmission of R-APS frames, blocking or unblocking ring ports, flushing the FDB, starting or stopping the WTR timer and the guard timer. The decision logic of the R-APS request processing is defined in clause 10.1.2, and represents the ring protection behaviour described in the remaining subclauses of clause 10.

The Ethernet ring protection switching algorithm commences immediately after any of the input signals (see Figure 10-1) changes, i.e., when the status of any local request changes, or when a different R-APS specific information is received.

10.1.1 Priority logic

This process receives requests from multiple sources. The request with the highest priority, according to Table 10-1, will be declared as the top priority request.

The evaluation of the top priority request is repeated every time a local request changes or an R-APS message is received.

Ring protection requests, commands and R-APS signals have the priorities as defined in Table 10-1.

Table 10-1 – Request/State priority

Request/State + Status	Type	Priority
local SF	local	highest
local clear SF	local	|
R-APS (SF)	remote	|
WTR Expires	local	|
WTR Running	local	|
R-APS(NR, RB)	remote	|
R-APS(NR)	remote	lowest

NOTE – Other requests, such as Manual Switch are for further study.

As a result of this process, once an SF condition is declared at one of the ring ports, the priority logic retains the local SF request as the current top priority request, until the local clear SF condition is signalled. Clearing of SF condition on one port is declared as the top priority request only if neither port is declaring local SF.

Received R-APS Request/State and Status are not stored in this process. As a result, after the change of a local request, R-APS Request/State and Status received previously are not taken into consideration for the definition of the new highest priority request.

10.1.2 R-APS request processing

The R-APS request processing logic receives the current high priority request and defines the necessary actions to take, based on the local ring node state.

The R-APS request processing logic is defined in the format of a state machine. The table has the following fields:

– Node state: the current state of the node.

– High priority request: the current highest priority request as defined in clause 10.1.1. Each possible trigger is represented in a separate row.

– Actions: a list of protection switching actions, in order of execution.

– Next node state: the state to which the state machine will transit.

Table 10-2 – State machine representation of the APS request processing logic

	Inputs		Outputs	
Node state	**High priority request**	**Row**	**Actions**	**Next node state**
–	State machine initialization	0	Stop guard timer Stop WTR timer If RPL Owner: Block RPL port Unblock non-RPL port Tx R-APS (NR, RB) Else: Block both ports Stop Tx R-APS	A

Table 10-2 – State machine representation of the APS request processing logic

	Inputs		Outputs	
Node state	**High priority request**	**Row**	**Actions**	**Next node state**
A (Idle)	local SF	1	Block failed port Unblock non-failed port Tx R-APS(SF) Flush FDB	B
	local clear SF	2	No action	A
	R-APS (SF)	3	Unblock non-failed port Stop Tx R-APS If not DNF flush FDB	B
	WTR Expires	4	No action	A
	WTR Running	5	No action	A
	R-APS (NR, RB)	6	Unblock non-RPL port	A
	R-APS(NR)	7	No action	A
B (Protection)	local SF	8	Block failed port Unblock non-failed port Stop WTR Tx R-APS(SF)	B
	local clear SF	9	Start guard timer Tx R-APS(NR)	B
	R-APS (SF)	10	Stop WTR Unblock non-failed port Stop Tx R-APS	B
	WTR Expires	11	Block RPL port Unblock non-RPL port Tx R-APS (NR,RB) Flush FDB	A
	WTR Running	12	No action	B
	R-APS (NR, RB)	13	If not RPL Owner: Unblock both ports Stop Tx R-APS If not DNF flush FDB	A
	R-APS(NR)	14	If RPL Owner: Start WTR	B

Row 0 represents the actions being triggered at the initialization of the state machine. Once those actions are performed, the state machine shall transit to State A.

The possible actions triggered by this process are:

- Block failed port – Blocks traffic channel and R-APS channel on ring ports which have an SF condition. If a port is already blocked, it remains blocked.
- Unblock non-failed port – Unblock traffic channel and R-APS channel on both ring ports if they do not have an SF condition. If a port is already unblocked, it remains unblocked.
- Block RPL port – Block traffic channel and R-APS channel on the port which is defined as the RPL. If the RPL port is already blocked, it remains blocked.

- Block both ports – Blocks traffic channel and R-APS channel on both ring ports. If a port is already blocked, it remains blocked.
- Unblock non-RPL port – Unblock traffic channel and R-APS channel on both ring ports if they are not the RPL port. If a port is already unblocked, it remains unblocked.
- Unblock both ports – Unblock traffic channel and R-APS channel on both ring ports. If a port is already unblocked, it remains unblocked.
- Start WTR – Starts the WTR timer if it is stopped. If the WTR timer is already running, then no action.
- Stop WTR – Stop the WTR timer if it is running.
- Start guard timer – Starts the guard timer. While the guard timer is running, received R-APS messages are not forwarded to the priority logic.
- Stop guard timer – Stops the guard timer if it is running.
- Stop Tx R-APS – Stop transmission of any R-APS messages.
- Tx R-APS (msgtype, status_bits) – Start transmission of R-APS message as described in clause 10.1.3.
- Flush FDB – Flush the FDB as described in clause 9.6.

10.1.3 R-APS message transmission

R-APS messages are transmitted with the Request/State and Status information defined by the R-APS request process.

The input Tx R-APS (msgtype, status_bits) starts the transmission of an R-APS PDU with the Request/State field set to the value defined by msgtype and with the status bits enumerated in status_bits with value 1, and the remaining status bits with value 0. R-APS messages are transmitted over both ring ports if they are operational. This also stops the continuous transmission of any other message.

The input Stop Tx R-APS results in stopping message transmission of any R-APS messages.

Traffic units which carry ring APS PDUs are called R-APS frames. The R-APS frames are transported via an R-APS specific VLAN.

A new R-APS frame must be transmitted immediately when required as an output action of Table 10-2.

R-APS frames are continuously transmitted. The first three R-APS frames should be transmitted as quickly as possible, if the R-APS information to be transmitted has been changed. This ensures that fast protection switching is possible even if one or two R-APS frames are lost or corrupted. For protection switching within 50 ms, the interval between the first three R-APS frames should be not more than 3.33 ms, which is the same interval as CCM frames for fast defect detection. R-APS frames after the first three frames are transmitted with an interval of 5 seconds.

10.1.4 Wait-to-restore timer

In the revertive mode of operation, to prevent frequent operation of the protection switch due to an intermittent defect, a failed working transport entity must become stable in a fault-free state. After the failed working transport entity meets this criterion, a fixed period of time shall elapse before traffic channel uses it again. This period, called the wait-to-restore (WTR) period, may be configured by the operator in 1 minute steps between 5 and 12 minutes; the default value is 5 minutes.

In the revertive mode, when the protection is no longer requested, i.e., the failure condition has been cleared, a wait-to-restore state will be activated on the RPL owner node. This state shall normally

time out and become a no-request state. The wait-to-restore timer is deactivated when any request of higher priority pre-empts this state.

The WTR timer may be started and stopped. A request to start running the WTR timer does not restart the timer.

This process has as output an indication of whether the timer is running and the expiration of the timer. While the timer is running, the WTR running signal is continuously generated. After the timer expires, the WTR running signal is stopped and the WTR expire signal is generated.

10.1.5 Guard timer

R-APS messages are continuously transmitted as defined in clause 10.1.3. This, combined with the R-APS messages forwarding method, in which messages are copied and forwarded at every ring node around the ring, can result in a message corresponding to an old request, which is no longer relevant, being received by ring nodes. The reception of messages with outdated information could result in erroneous interpretation of the existing requests in the ring and lead to erroneous protection switching decisions.

The guard timer is used to prevent ring nodes from receiving outdated R-APS messages. During the duration of the guard timer, all received R-APS messages are ignored by the ring protection control process. This allows that old messages still circulating on the ring may be ignored. This, however, has the side effect that, during the period of the guard timer, a node will be unaware of new or existing ring requests transmitted from other nodes.

The period of the guard timer may be configured by the operator in 10 ms steps between 10 ms and 2 seconds, with a default value of 500 ms. This time should be greater than the maximum expected forwarding delay for which one R-APS message circles around the ring.

The guard timer may be started and stopped. While the guard timer is running, the received R-APS Request/State and Status information is not forwarded. If the guard timer is not running, the R-APS Request/State information is forwarded unchanged.

10.1.6 Validity check

The validity check verifies that the Request/State field of the received R-APS message is one of the "Request/States" defined in this Recommendation in Table 10-3. R-APS messages with Request/State fields defined as "Reserved for future international standardization" are filtered.

10.1.7 Local defect logic

Local defect logic asserts the SF condition of one ring link based on the received ETH_CI_SSF information and the holdoff timer process. The reception of ETH_CI_SSF results in continuously signalling SF after the holdoff timer process, until the ETH_CI_SSF is cleared.

Clearance of the ETH_CI_SSF results in producing the clear SF signal.

10.1.8 Holdoff timer

In order to coordinate timing of protection switches at multiple layers, a holdoff timer may be required. Its purpose is to allow, for example, a server layer protection switch to have a chance to fix the problem before switching at a client layer.

Each protection group should have a provisionable holdoff timer. The suggested range of the holdoff timer is 0 to 10 seconds in steps of 100 ms with an accuracy of ±5 ms.

When a new defect or more severe defect occurs (new SF), this event will not be reported immediately to protection switching if the provisioned holdoff timer value is non-zero. Instead, the holdoff timer will be started. When the holdoff timer expires, whether a defect still exists on the trail that started, the timer will be checked. If one does exist, that defect will be reported to protection switching. The reported defect need not be the same one that started the timer.

10.2 Protection switching behaviour

Protection switching behaviours on failure and recovery conditions are described in this clause.

NOTE – Scenarios illustrating the sequence of events in protection switching are included in Appendix IV.

10.2.1 Protection switching – Link signal failure

A ring with no SF request will have a topology with the traffic channel blocked at the RPL and unblocked in all other ring links. In this situation, the detection of a signal-fail condition in a ring link will trigger protection switching as follows:

– A node detecting an SF condition on one of its ring ports will block the traffic channel and R-APS channel on the failed ring port.

– The node detecting an SF condition will transmit an R-APS message indicating *SF* over both ring ports. The R-APS SF message informs other ring nodes of the SF condition and that the traffic channel is blocked on one port. R-APS (SF) message shall be continuously transmitted by the node detecting the SF condition while this condition persists.

– Assuming the node was in an idle state before the SF condition occurred, upon detection of this SF condition, the node will trigger a local FDB Flush.

– A node accepting an R-APS (SF) message, without any local higher priority requests, will unblock any blocked port which does not have an SF condition. This action will unblock the traffic channel over the RPL.

– The node accepting an R-APS (SF) message, without any local higher priority requests, will stop transmission of R-APS messages.

– Assuming the node was in idle state before the SF condition occurred, a ring node accepting an R-APS (SF) message without a DNF indication will perform a Flush FDB operation.

– While a node remains in the protection state, the acceptance of subsequent R-APS (SF) messages does not re-trigger an FDB flush.

Protection switching is completed when the above actions are performed by each ring node. At this point the conditions are created to allow the traffic flows to be steered around the ring.

Bidirectional link failures are detected by the two nodes adjacent to the failed link. These two nodes trigger protection switching and will keep traffic channel blocked at both ends of the failed link. Unidirectional link failures are detected by only one of the nodes adjacent to the failed link. This node is the only node triggering protection switching and keeps traffic channel blocked at its end of the failed link. These port blocking behaviours are essential to prevent the ring from forming loops when the link failure is recovered. A node failure situation is handled as the failure of both ring links of the node. The two nodes adjacent to the failed node will initiate protection switching by detecting the SF condition on the link connected to the failed node.

10.2.2 Protection switching – Signal degrade on link

Protection switching behaviour in case of signal degrade condition is for further study.

10.2.3 Protection switching – Recovery

A node that has one or more ring ports in an SF condition, upon detection of clearance of the SF condition, will keep at least one of these ports blocked for traffic channel and for the R-APS channel, until the RPL is blocked as a result of ring protection reversion, or until there is another higher priority request (e.g., an SF condition) in the ring.

A node that has one ring port in an SF condition and detects clearing this SF condition will continuously transmit the R-APS message *no request* (NR) over both ring ports, informing that no request is present at the node and initiates a guard timer as described in clause 10.1.5. The nodes will stop transmission of R-APS (NR) messages when they accept an R-APS (NR, RB), or when another higher priority request is received.

10.2.3.1 Revertive behaviour

When all ring links and nodes have recovered and no external requests are active, reversion is the action to be taken. Reversion is handled in the following way:

– The reception of NR message triggers the RPL owner node to start the WTR timer.

– The WTR timer is cancelled, if during the WTR period a higher priority request than NR is accepted by the RPL owner, or is declared locally at the RPL owner.

– When the WTR timer expires, without the presence of any other higher priority request, the RPL owner initiates reversion by blocking traffic channel over the RPL, transmitting an R-APS message *NR, RB* over both ring ports, informing the ring that the RPL is blocked, and performing a flush FDB operation.

– The acceptance of the R-APS (*NR, RB)* message without a DNF indication triggers all ring nodes to unblock any blocked non-RPL which does not have SF condition, and to perform a flush FDB operation.

– The acceptance of subsequent R-APS (*NR, RB*) messages shall not re-trigger flush FDB operations on the ring nodes.

10.2.3.2 Non-revertive behaviour

Non-revertive behaviour is for further study.

10.2.4 Protection switching – Manual switch

Manual switch behaviour is for further study.

10.3 R-APS format

R-APS information is carried within the R-APS PDU, which is one of a suite of Ethernet OAM PDUs. The OAM PDU format for each type of Ethernet OAM operation is defined in [ITU-T Y.1731]. R-APS specific information is transmitted within specific fields in the R-APS PDU. The R-APS PDU is identified by the Ethernet OAM OpCode 40.

R-APS messages use a MAC destination address within the range of 01-19-A7-00-00-00 to 01-19-A7-00-00-FF. This MAC address range is allocated within ITU OUI for G.8032 R-APS communication. In this Recommendation, the destination MAC address 01-19-A7-00-00-01 is used, other MAC addresses are for further study.

In this Recommendation, 32 octets in the R-APS PDU are used to carry R-APS specific information. This is illustrated in Figure 10-2 below. In addition, the TLV offset field is required to be set to 32.

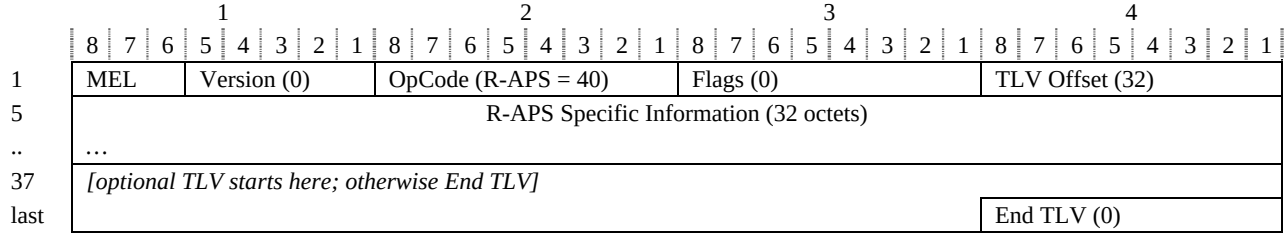

Figure 10-2 – R-APS PDU format

For other fields such as version, OpCode, flags, and end TLV, the following values shall be used, as defined in [ITU-T Y.1731].

– **Version**: 0x00 shall be transmitted in the current version of this Recommendation. This field should be ignored upon reception.

– **OpCode**: 40 shall be transmitted as defined within [ITU-T Y.1731].

– **Flags**: 0x00 shall be transmitted in the current version of this Recommendation. This field should be ignored upon reception.

– **End TLV**: 0x00 shall be transmitted.

This Recommendation does not define any ring APS specific TLVs.

In the MEL field, the MEG level of the R-APS PDU is inserted.

The format of the R-APS specific information within each R-APS PDU is defined as per the following Figure 10-3:

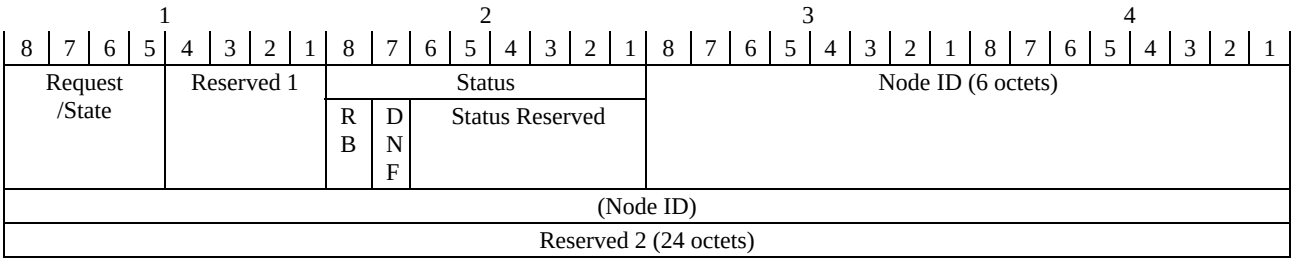

Figure 10-3 – R-APS specific information format

The fields of R-APS specific information:

– Request/State (4 bits) – This field represents a request or state, and is encoded as described in Table 10-3.

Table 10-3 – Request/State values

Field	Value	Description
Request/State	1011	Signal fail (SF)
	0000	No request (NR)
	Other	Reserved for future international standardization

– Reserved 1 (4 bits) – This field is reserved for future extension of requests or for indication of protection type. In the current version of this Recommendation, this field shall be encoded as "0000". This field should be ignored upon reception.

– Status field – This includes the following status information.

- RB – RPL Blocked
  - RB = 1 – represents that the RPL is blocked
  - RB = 0 – represents that the RPL is unblocked.

  This bit should be 0 when transmitted by non-RPL owner nodes.
- DNF – Do not flush
  - DNF = 1 – represents that an FDB flush should not be triggered by the reception of this message.

  - DNF = 0 – represents that an FDB flush may be triggered by the reception of this message.
- Status reserved (6 bits) – For future specification. This field shall be transmitted encoded all zeroes. This field should be ignored upon reception.

– Node ID (6 octets) – A MAC address unique to the ring node. This field is informational; it does not impact protection switching operation in this Recommendation.

– Reserved 2 (24 octets) – This field is reserved for future extensions of the R-APS protocol. In the current version of this Recommendation, this field shall be transmitted encoded all zeroes. This field should be ignored upon reception.

Appendix I

Ring protection network objectives

(This appendix does not form an integral part of this Recommendation)

The following are network objectives of Ethernet ring protection.

I.1 The Ethernet ring protection mechanism shall prevent the creation of loops in a ring topology under any circumstances (starting up the network, failure condition, and switchover).

I.2 The ETH layer connectivity of ring links should be periodically monitored.

I.3 The ring link ETH layer monitoring should inform the Ethernet ring protection mechanism of SF or SD conditions (e.g., link bandwidth degradation and excessive error).

I.4 Server Layer SF and SD conditions should be informed to Ethernet ring protection mechanism.

Service Restoration

I.5 Ethernet ring protection shall not contend with the protection mechanisms of the server layer.

General

I.6 The ring shall successfully recover multipoint connectivity in the event of a single ring link failure.

I.7 The ring shall successfully recover multipoint connectivity in the event of a single node failure, except for the traffic at that node.

I.8 In the event of more than a single failure (e.g., of links or nodes), the result should be ring segmentation with full connectivity within each segment.

I.9 Ethernet ring protection shall operate under all network load conditions.

I.10 Ethernet ring protection shall be independent of the capability of the server layer.

I.11 Ethernet ring protection shall support protection over multi-ring/ladder networks.

a) The protection mechanism shall enable the interconnection of rings using a single node or dual nodes (a shared link). The mechanism shall protect services that are traversing interconnected rings. In the case of interconnected rings using dual nodes, the mechanism shall ensure that a super loop is not formed in the event that the shared link fails.

I.12 Ethernet ring protection control communication shall be performed using standard Ethernet frames (802.3/802.1). The control messages of the Ethernet ring protection mechanism shall use the OAM frame format defined in [ITU-T Y.1731]. The OAM messages defined in [ITU-T Y.1731] may be extended to support the protection control messages.

I.13 The protection process shall be deterministic. All nodes in the Ethernet ring shall have the same view of the protection state.

I.14 The total communication bandwidth consumed by the protection mechanism shall be a very small fraction of the total available bandwidth, and shall be independent of the total traffic supported by the network.

I.15 The protection mechanism shall not impose any limitation or requirements on the Ethernet relay and filtering function.

I.16 The mechanism should not impose any limitation on the number of nodes that may form the Ethernet ring. From an operational perspective, the maximum number of nodes supported should be in the range of 16 to 255 nodes.

I.17 A switchover may be administratively triggered.

I.18 Revertive mode shall be supported.

I.19 Non-revertive mode should be supported.

I.20 In the event of a single ring node or link failure, Ethernet ring protection shall support protection switching time (i.e., transfer time, T_t in clause 13 of [ITU-T G.808.1]) of no more than 50 ms.

I.21 Ethernet ring protection may support configurable holdoff times before triggering protection operation.

I.22 Ethernet ring protection may support configurable wait-to-restore times.

I.23 In the event of reversion, Ethernet ring protection shall support revertive switching time (i.e., transfer time, T_t in clause 13 of [ITU-T G.808.1]) of no more than 50 ms.

I.24 In the event of administratively triggered switchover, Ethernet ring protection shall support switching time (i.e., transfer time, T_t in clause 13 of [ITU-T G.808.1]) of no more than 50 ms.

Appendix II

Ethernet ring network objectives

(This appendix does not form an integral part of this Recommendation)

The following are Ethernet ring network objectives:

II.1 An Ethernet ring shall be constructed from a set of Ethernet ring nodes, as defined in clause 3.2.2, which form a ring topology (i.e., a ring).

II.2 Traffic forwarding in an Ethernet ring and between a non-ring port and a ring port shall be based entirely on the forwarding rules defined by the IEEE 802.1 specifications.

II.3 Each ring node shall have exactly two ring ports per logical ring.

II.4 The nodes shall be connected in a closed loop.

II.5 The ring shall provide direct or indirect communication between all nodes in the ring.

II.6 In Ethernet ring topology, each node shall be connected to two other nodes utilizing ring ports based on 802.3 MAC.

II.7 The Ethernet MAC may be transported over any server Layer.

a) Ethernet ring shall not preclude the use of any transport technology (e.g., SDH VCs using GFP mapping, Ethernet physical layer interfaces ETY, MPLS ETH pseudo-wires, Ethernet link aggregation [b-IEEE 802.3]).

b) The capacity of each span in the ring (link) is dependent on the transport technology used. It shall not be a requirement that all links need to provide the same capacity.

II.8 The definition of an Ethernet ring shall be applicable to both physical ring topologies and logical ring topologies. Note these are not independent.

II.9 Shall support increased bandwidth utilization via concurrent transmissions, spatial reuse.

II.10 Shall utilise [ITU-T Y.1731], [b-IEEE 802.1ag] and may use other Ethernet OAM specifications.

II.11 Each Ethernet ring node shall support MAC services and QoS according to the [IEEE 802.1Q]. The use of ring resources at each link is controlled by the same rules.

II.12 Ethernet rings shall support E-Line, E-LAN and E-Tree services including EPL & EVPL [b-ITU-T G.8011].

II.13 Ethernet ring topology shall support all types of communication: Unicast, Multicast, and Broadcast.

II.14 Normal ring behaviour (i.e., without protection) shall prevent mis-ordering and/or duplication of transported client frames.

II.15 End-to-end services may traverse multiple interconnected rings.

II.16 Ethernet rings may be interconnected through a shared node (as depicted in Figure II.1), or through dual shared nodes with a shared link (as depicted in Figure II.2) or a multi-ring/ladder network that consists of conjoined Ethernet rings (as depicted in Figure II.3).

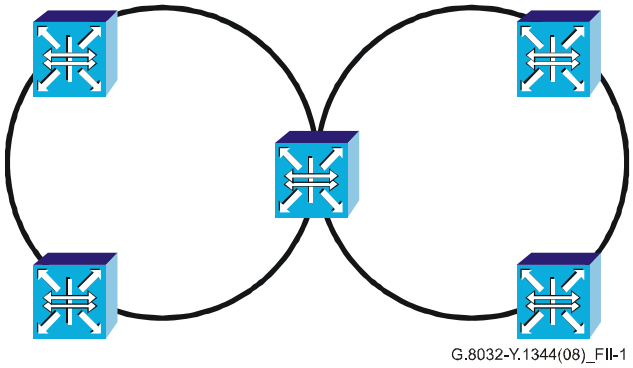

Figure II.1 – Interconnected Ethernet rings via a shared node

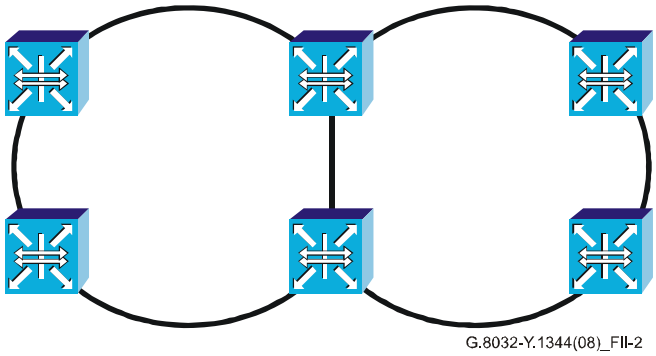

Figure II.2 – Interconnected Ethernet rings via dual nodes with a shared link

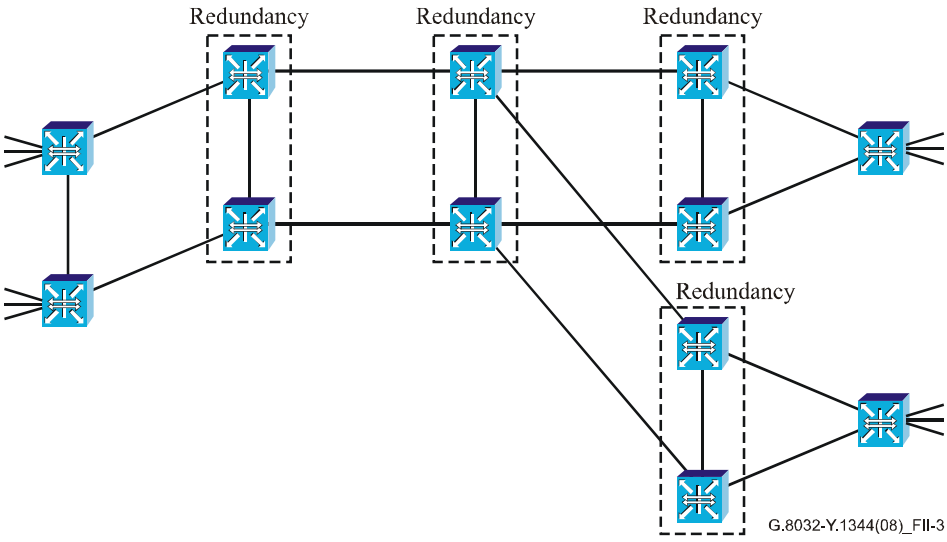

Figure II.3 – Example of multi-ring/ladder network

II.17 The logical rings shall be identifiable for management purposes.

Appendix III

Description of the ETHDi/ETH adaptation function

(This appendix does not form an integral part of this Recommendation)

This appendix gives a description of the ETHDi/ETH adaptation function that is used to transmit and receive R-APS PDUs on/from the ring. This information belongs to [ITU-T G.8021] and will be included in a future update. As soon as it is included in [ITU-T G.8021], this appendix can be removed from this Recommendation.

III.1 ETHDi/ETH adaptation function source (ETHDi/ETH_A_So)

This function allows the insertion of R-APS information into a stream of ETH_CI.

Symbol

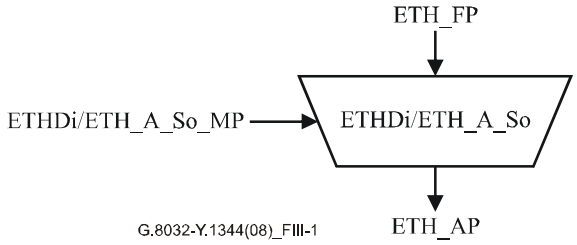

Figure III.1 – ETHDi/ETH_A_So function

Interfaces

Table III.1 – ETHDi/ETH_A_So Interfaces

Inputs	Outputs
ETH_FP: ETH_CI_D ETH_CI_P ETH_CI_DE ETH_CI_RAPS *ETHDi/ETH_A_So_MP:* ETHDi/ETH_A_So_MI_MEL ETHDi/ETH_A_So_MI_RAPS_Pri ETHDi/ETH_A_So_MI_MIP_MAC	*ETH_AP:* ETH_AI_D ETH_AI_P ETH_AI_DE

Process

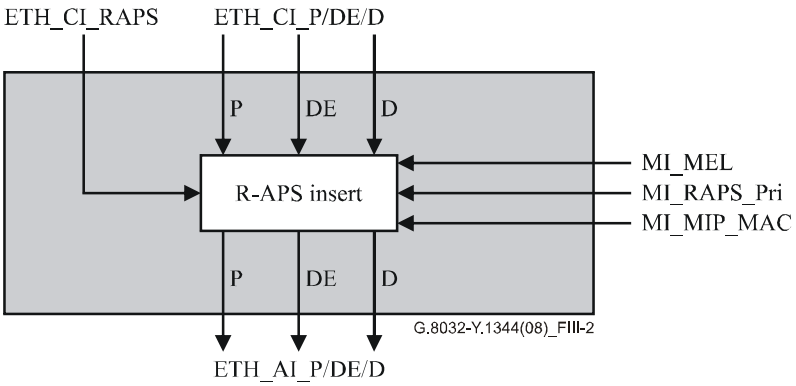

Figure III.2 – ETHDi/ETH_A_So process

R-APS insert

The R-APS insert process encodes the ETH_CI_RAPS signal into the ETH_CI_D signal of an ETH_CI traffic unit; the resulting R-APS traffic unit is inserted into the stream of incoming traffic units, i.e., the outgoing stream consists of the incoming traffic units and the inserted R-APS traffic units. The ETH_CI_RAPS signal contains the R-APS specific information as defined in this Recommendation.

The ETH_CI_D signal contains a source and destination address field and an M_SDU field. The format of the M_SDU field for R-APS traffic units is determined by the ETH_CI_RAPS signal. The MEL in the M_SDU field is determined by the MI_MEL input parameter.

The value of the source and destination address fields in the M_SDU field is determined by the local MAC address of the maintenance entity group intermediate point (MIP) (MI_MIP_MAC) and the ring multicast address, as described in this Recommendation. The value of the ring multicast MAC address is 01-19-A7-00-00-01. The value of MI_MEP_MAC should be a valid unicast MAC address.

The value of the ETH_CI_P signal associated with the generated R-APS traffic units is determined by the MI_RAPS_Pri input parameter.

The value of the ETH_CI_DE signal associated with the generated R-APS traffic units is set to drop ineligible.

III.2 ETHDi/ETH adaptation function sink (ETHDi/ETH_A_Sk)

This function extracts the R-APS information from the R-APS traffic units, without filtering the traffic unit.

Symbol

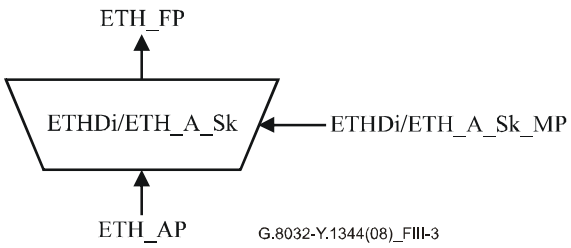

Figure III.3 – ETHDi/ETH_A_Sk function

Interfaces

Table III.2 – ETHDi/ETH_A_Sk interfaces

Inputs	Outputs
ETH_AP: ETH_AI_D ETH_AI_P ETH_AI_DE ETH_AI_TSF *ETHDi/ETH_A_Sk_MP:* ETHDi/ETH_A_Sk_MI_MEL	*ETH_FP:* ETH_CI_D ETH_CI_P ETH_CI_DE ETH_CI_RAPS ETH_CI_SSF

NOTE – Currently in [ITU-T G.8021], for the ETHDi_FT_Sk, no consequent action for the ETH_CI_SSF input has been defined. However, the consequent action should be ETH_AI_TSF output, to propagate the failure information.

Process

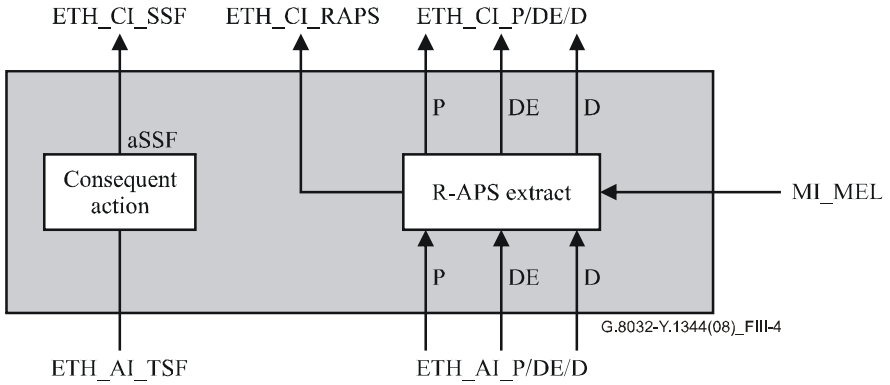

Figure III.4 – ETHDi/ETH_A_Sk process

R-APS extract

The R-APS extract process extracts ETH_CI_RAPS signals from the incoming stream of ETH_CI traffic units, without filtering the R-APS traffic unit. ETH_CI_RAPS signals are only extracted if they belong to the MEL, as defined by the MI_MEL input parameter.

If an incoming traffic unit is an R-APS traffic unit belonging to the MEL defined by MI_MEL, the traffic unit will be duplicated. The original R-APS traffic unit will be transparently forwarded and the ETH_CI_RAPS signal will be extracted from the duplicate. The ETH_CI_RAPS is the R-APS specific information contained in the received traffic unit. All other traffic units will be transparently forwarded, without being duplicated. The encoding of the ETH_CI_D signal for R-APS frames is defined in clause 9.10 of [ITU-T Y.1731].

The criteria for filtering are based on the values of the fields within the M_SDU field of the ETH_CI_D signal:

- length/type field equals the OAM Ethertype (89-02), and
- MEL field equals MI_MEL, and
- OAM type equals R-APS (40), as defined in clause 9.1 of [ITU-T Y.1731]

Defects None.

Consequent actions

aSSF ← AI_TSF

Defect correlations None.

Performance monitoring None.

Appendix IV

Ring protection scenarios

(This appendix does not form an integral part of this Recommendation)

The following scenarios represent a ring composed of seven ring nodes. The RPL link is the link between nodes A and G. Node G is the RPL owner node.

The following symbols are used:

● Message source

▶ R-APS block

▭ Client block

Scenario A – Single link failure

The following scenario represents protection switching in case of a single link failure.

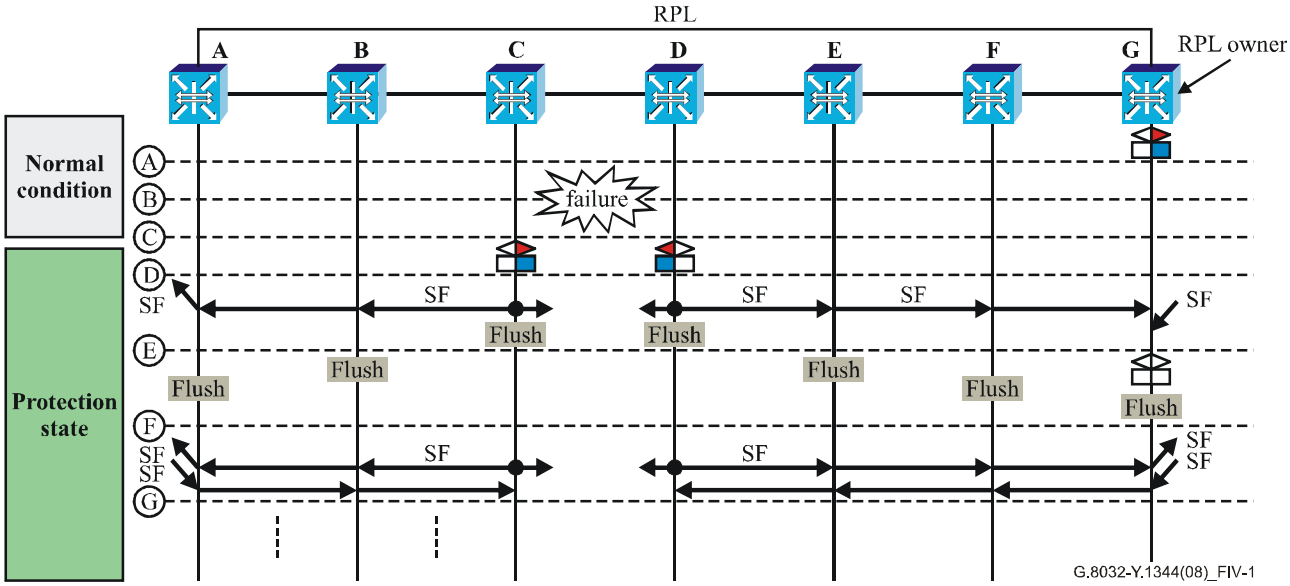

Figure IV.1 – Single link failure

The following sequence describes the steps in Figure IV.1:

A Normal condition

B Failure occurs

C Nodes C and D detect local signal failure condition and after respecting holdoff time, block failed port and perform FDB flush

D Nodes C and D periodically send SF message, on both ring ports, while SF condition persists

E All nodes receiving SF message flush FDB. RPL owner receives SF message, unblocks its end of RPL link and flushes FDB

F Stable state – SF messages on the ring

G Further SF messages trigger no further action

The following scenario represents the reversion in case of a single link failure.

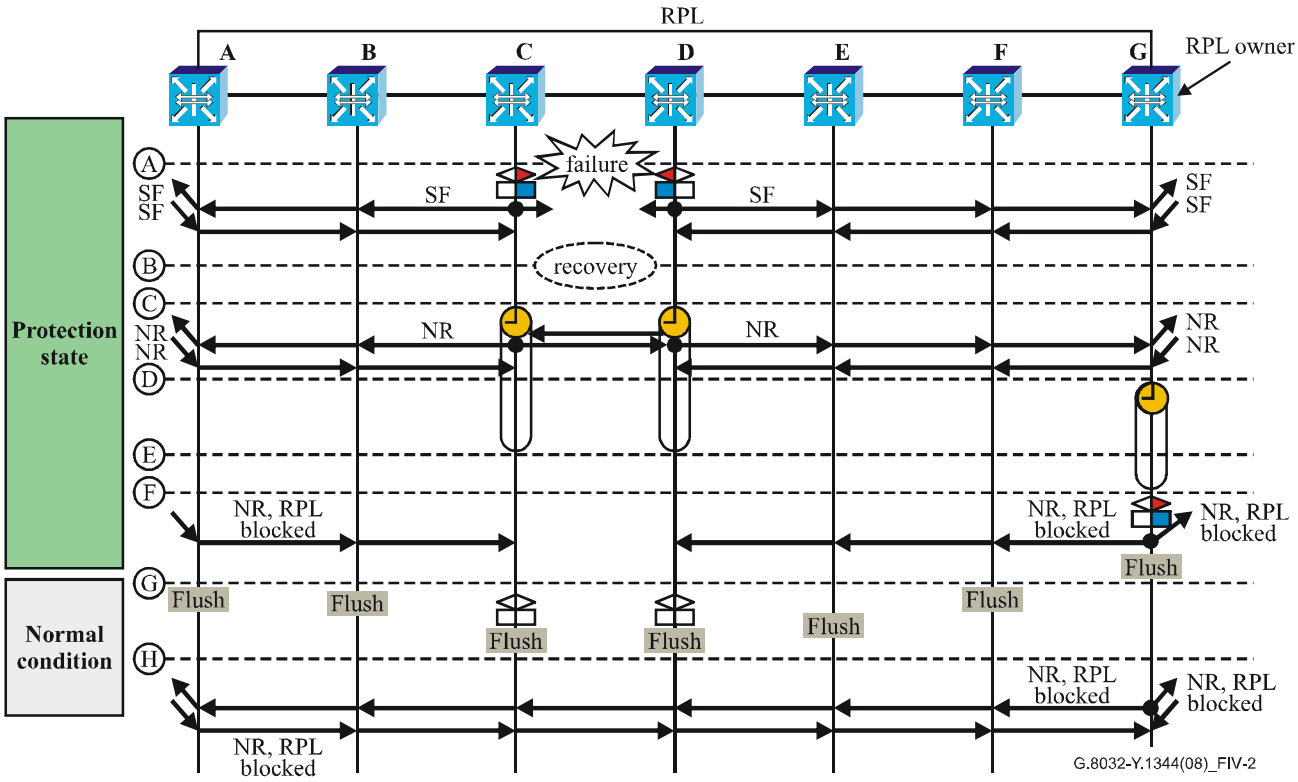

Figure IV.2 – Single link failure recovery

The following sequence describes the steps in Figure IV.2:

A Stable SF condition

B Recovery of link failure

C Nodes C and D detect clearing of SF condition, start guard timer and initiate periodical transmission of NR message on both ring ports. (Guard timer prevents reception of R-APS messages)

D When the RPL owner receives NR message, it starts the WTR timer

E When nodes C and D expire the guard timer, they may accept the new R-APS messages that they receive. [in guard timer]

F At expiration of WTR timer, RPL owner blocks its end of the RPL, sends *NR RB* message and flushes FDB

G When nodes C and D receive *NR RB* message, they remove block on their blocked ports and stop sending NR message. In addition to this, nodes A to F will flush FDB when receiving *NR RB* message

Scenario B – Single unidirectional link failure

This scenario is similar to scenario A with the difference that the link failure is unidirectional.

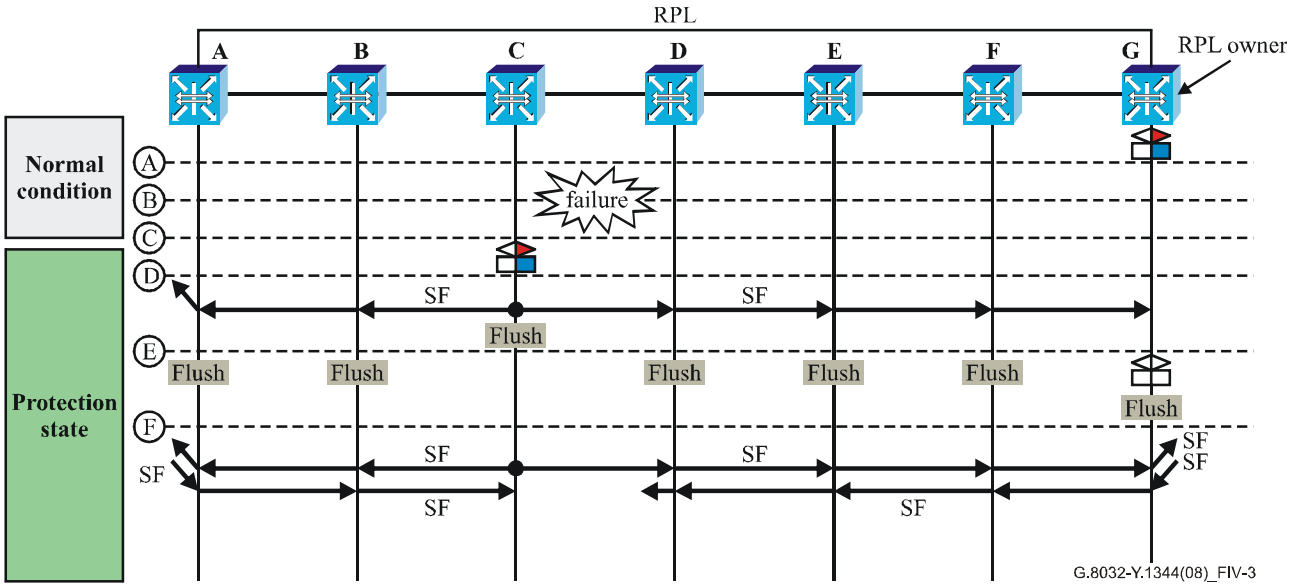

Figure IV.3 – Single link failure unidirectional

The following sequence describes the steps in Figure IV.3:

A Normal condition

B Failure occurs in direction of D to C, direction C to D is unaffected

C Node C detects local signal failure condition and after respecting holdoff time, blocks failed port (node D performs no action)

D Node C starts sending SF message on both ring ports and performs FDB flush. Subsequently, it periodically sends SF message while SF condition persists

E RPL owner receiving SF message, unblocks its end of RPL link, and flushes FDB. All non-RPL owner nodes receiving SF message will flush the FDB

F Stable state – SF messages on the ring

The reversion for the unidirectional case is represented by Figure IV.4:

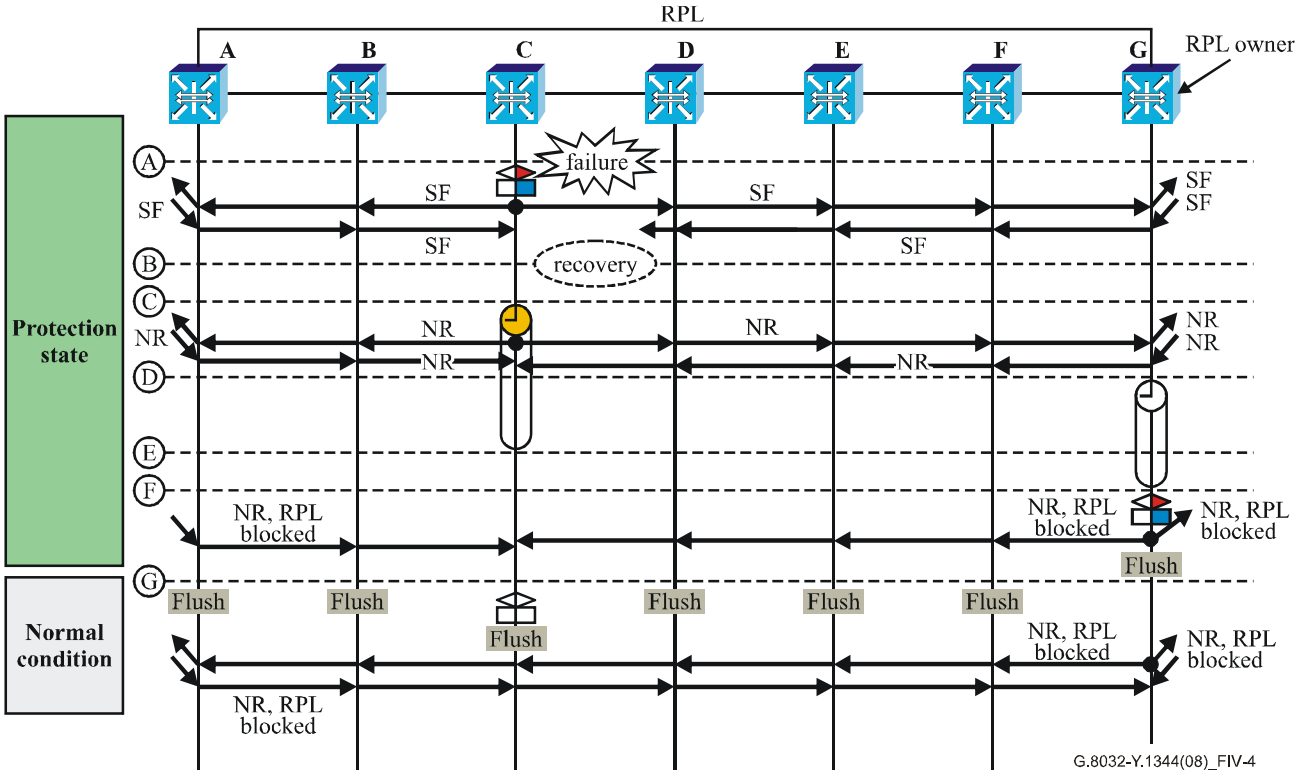

Figure IV.4 – Single link failure unidirectional recovery

The following sequence describes the steps in Figure IV.4:

A Stable SF condition

B Recovery of link failure

C Node C detects clearing of SF condition, starts guard timer and initiates periodical transmission of NR message on both ring ports. (Guard timer prevents reception of R-APS messages)

D When the RPL owner receives NR message, it starts the WTR timer

E When the guard timer of node C expires, it may accept the new R-APS messages that they receive

F At expiration of WTR timer, RPL owner blocks its end of the RPL, sends *NR RB* message and flushes the FDB

G When node C receives *NR RB* message, it removes block on its blocked port and stop sending NR message. All non-RPL owner nodes receiving this message will flush the FDB

Scenario C – RPL link failure

Figure IV.5 represents the behaviour in case of RPL failure, and shows an example of the possible use of the DNF status bit.

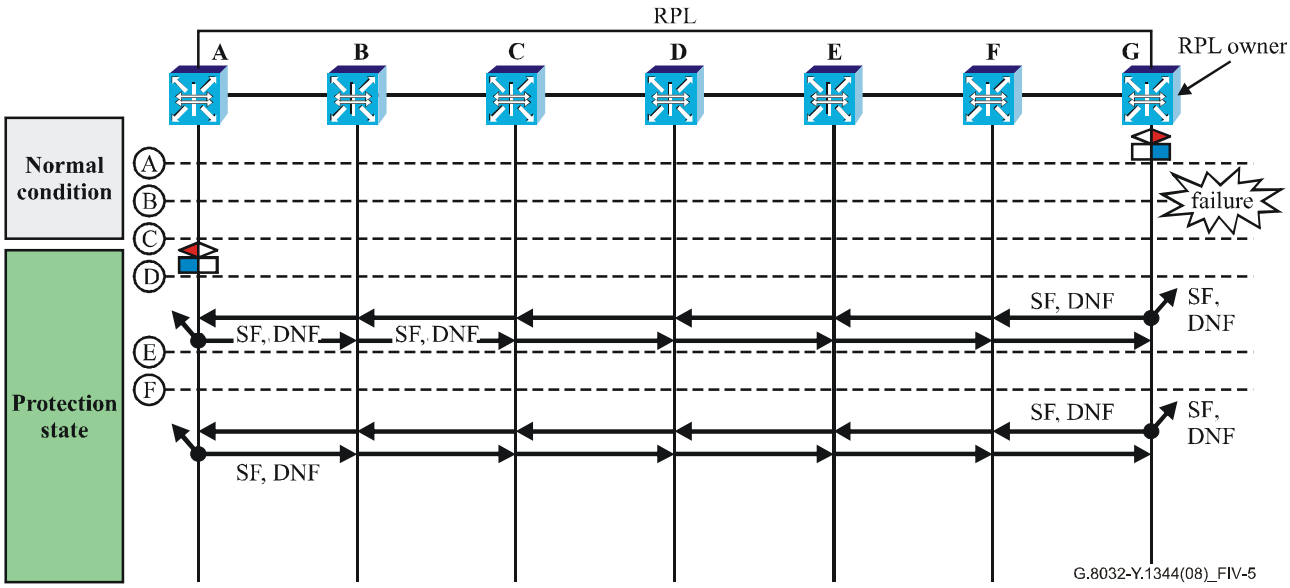

Figure IV.5 – RPL link failure

The following sequence describes the steps in Figure IV.5:

A Normal condition

B Failure occurs

C Nodes A and G detect local signal failure condition and after respecting holdoff time, block failed port

D Nodes A and G periodically send SF message, on both ring ports, while SF condition persists. The SF message includes "Don't Flush" – DNF indication and this will prevent all nodes from performing FDB flushing, despite the transition from idle to protection state

E RPL owner receives SF message, but it is ignored as there is a local higher priority request (local SF) [no transition]. All other nodes receiving the SF message with "don't Flush indication" DNF (flush is not performed), despite the transition from normal to protection state without flushing FDB

F Stable state – SF messages on the ring with "don't Flush" DNF indication

The actions after the repair of the RPL are represented in Figure IV.6:

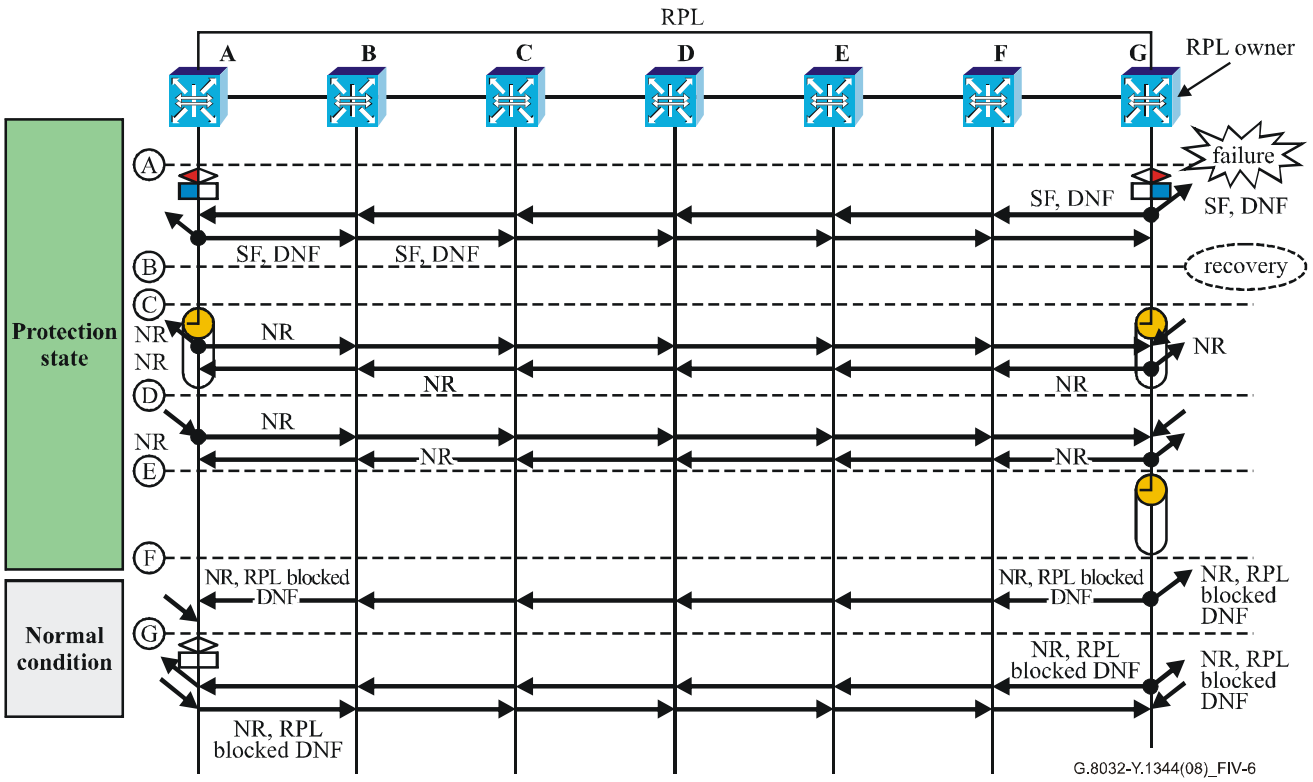

Figure IV.6 – RPL link failure – Recovery

The following sequence describes the steps in Figure IV.6:

A Stable SF condition

B Recovery of link failure

C Nodes A and G detect clearing of SF condition, start guard timer and initiate periodical transmission of NR message on both ring ports. (Guard timer prevents reception of R-APS messages)

D When the guard timer of nodes A and G expire, they may accept the new R-APS messages that they receive

E When the RPL owner receives NR message, it starts the WTR timer

F At expiration of WTR timer, RPL owner blocks its end of the RPL (it was already blocked), and sends *NR RPL Blocked* message. This message includes "DNF" indication and this will prevent all nodes from performing FDB flushing, despite the transition from idle to protection state

G When node A receives *NR RPL Blocked* message, it removes block on its blocked port and stops sending NR message. All nodes receiving this message will not flush FDB as the message includes the "DNF" indication, despite the transition from protection to normal state without flushing FDB

Scenario D – Multiple failure case – Recovery

The following scenario represents the case of sequential repair of multiple failures. In this case, the failures between nodes A and B and between nodes E and F recover almost simultaneously. The SF condition remains in the link between nodes C and D.

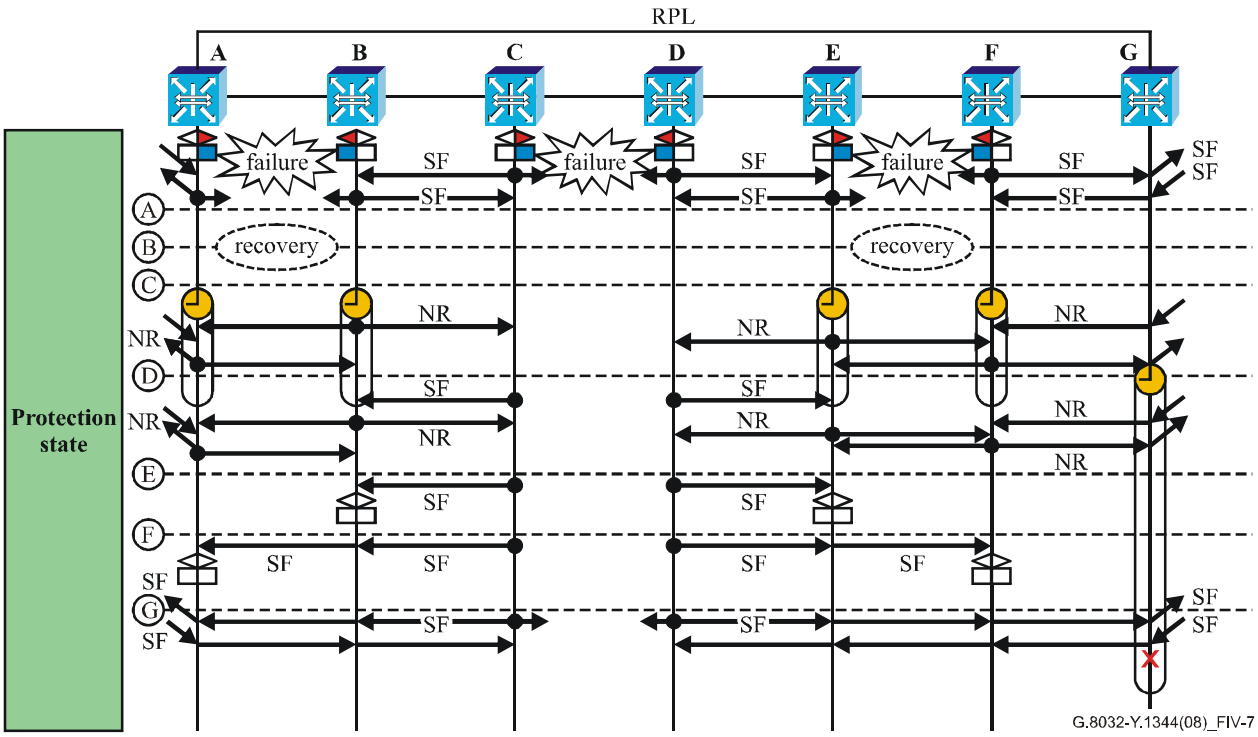

Figure IV.7 – Multiple link failure

The following sequence describes the steps in Figure IV.7:

A Stable SF condition

B Recovery of link failure

C Nodes A, B, E and F detect clearing of SF condition, start guard timer and initiate periodical transmission of NR message on both ring ports. Guard timer prevents reception of R-APS messages, as is the case of SF message transmitted by nodes C and D, which is ignored by nodes B and E

D When the RPL owner receives NR message, it starts the WTR timer

E After nodes A, B, E and F expire the guard timer, they may accept the new R-APS messages that they receive. The reception of SF message will trigger unblocking of blocked port and stop sending NR message at nodes B and E

F The reception of SF message will trigger unblocking of blocked port and stop sending NR message at nodes A and F

G The reception of SF message informs the RPL owner that an error still occurs in the ring. This will result in stopping the WTR timer.

Bibliography

[b-ITU-T G.8011] Recommendation ITU-T G.8011/Y.1307 (2004), *Ethernet over Transport – Ethernet services framework.*

[b-IEEE 802.1ag] IEEE 802.1ag-2007, *IEEE Standard for local and metropolitan area networks – Virtual Bridged Local Area Networks – Amendment 5: Connectivity Fault Management.* <http://www.ieee802.org/1/pages/802.1ag.html>

[b-IEEE 802.3] IEEE 802.3-2005, *Information Technology – Local and Metropolitan Area Networks – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.* <http://standards.ieee.org/getieee802/802.3.html>

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	**Y.1300–Y.1399**
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899

For further details, please refer to the list of ITU-T Recommendations.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	**Transmission systems and media, digital systems and networks**
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2009