

INTERNATIONAL STANDARD

NORME INTERNATIONALE

**Industrial communication networks – High availability automation networks –
Part 4: Cross-network Redundancy Protocol (CRP)**

**Réseaux de communication industriels – Réseaux d'automatisation à haute
disponibilité –
Partie 4: Protocole de redondance inter-réseau (CRP)**

IECNORM.COM : Click to view the full PDF of IEC 62439-4:2010



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2010 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.

Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you to find IEC publications by a variety of criteria (reference number, text, technical committee,...).

It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Liens utiles:

Recherche de publications CEI - www.iec.ch/searchpub

La recherche avancée vous permet de trouver des publications CEI en utilisant différents critères (numéro de référence, texte, comité d'études,...).

Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

Just Published CEI - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications de la CEI. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (VEI) en ligne.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

INTERNATIONAL STANDARD

NORME INTERNATIONALE

**Industrial communication networks – High availability automation networks –
Part 4: Cross-network Redundancy Protocol (CRP)**

**Réseaux de communication industriels – Réseaux d'automatisation à haute
disponibilité –
Partie 4: Protocole de redondance inter-réseau (CRP)**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX



ICS 25.040, 35.040

ISBN 978-2-83220-534-1

**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

CONTENTS

FOREWORD.....	4
INTRODUCTION.....	6
1 Scope.....	7
2 Normative references	7
3 Terms, definitions, abbreviations, acronyms, and conventions	7
3.1 Terms and definitions	7
3.2 Abbreviations and acronyms.....	7
3.3 Conventions	7
4 CRP overview.....	8
5 CRP nodes	8
6 CRP LAN topology	8
7 CRP key components	10
7.1 CRP general protocol operation.....	10
7.1.1 Doubly-attached nodes (DANCs)	10
7.1.2 Singly attached nodes	11
7.2 CRP statistics.....	11
7.3 CRP Network_Status_Table	12
7.4 CRP recovery time	15
7.4.1 Recovery time calculation.....	15
7.4.2 Maximum repair time	16
7.5 CRP multicast messages.....	16
7.5.1 Sending.....	16
7.5.2 Receiving	16
7.6 CRP unicast messages	16
7.6.1 Sending a frame.....	16
7.6.2 Receiving a frame.....	17
7.7 CRP redundancy information.....	17
7.8 CRP redundancy statistics.....	17
8 CRP protocol.....	17
8.1 CRP singly attached node	17
8.2 CRP doubly attached node	17
8.3 CRP Installation, configuration and repair	17
8.4 CRP LRE model attributes.....	18
8.4.1 Attribute specification	18
8.4.2 Impact of LRE configuration attributes	22
8.5 CRP encoding of the DiagnosticFrame	23
8.6 CRP Encoding of the AnnunciationFrame	24
8.7 CRP common protocol.....	26
8.7.1 AnnunciationFrames	26
8.7.2 DiagnosticFrames.....	26
8.7.3 Detection of duplicate Node_Index	27
8.7.4 Detection of duplicate Node_Name.....	27
8.7.5 Failure detection based on arrival of DiagnosticFrames	27
8.7.6 Status array entries	28
8.7.7 Other failure detection	28
8.8 CRP operational messages	28

8.8.1	Load balancing	28
8.8.2	LAN and port maintenance	28
8.8.3	Selecting transmission path	29
8.8.4	Selecting reception adapter	30
8.8.5	Crossed_cable_status	30
8.8.6	Configured parameters	30
8.9	CRP services	31
8.9.1	Configuration options and services	31
8.9.2	LAN redundancy service specification	31
9	CRP Management Information Base (MIB)	38
	Bibliography	41
	Figure 1 – CRP stack architecture	8
	Figure 2 – CRP single LAN topography	9
	Figure 3 – CRP double LAN topology	9
	Figure 4 – CRP DiagnosticFrame pair approach	10
	Figure 5 – CRP example system	11
	Table 1 – CRP example Network_Status_Table for node 3	11
	Table 2 – CRP Network_Status_Table for singly connected nodes	13
	Table 3 – CRP Network_Status_Table for DANC	14
	Table 4 – CRP Path_Status_Sets	21
	Table 5 – CRP example of a Path_Status_Set	21
	Table 6 – CRP configuration attributes impact on LAN operation	22
	Table 7 – CRP DiagnosticFrame format	23
	Table 8 – CRP AnnunciationFrame	24
	Table 9 – CRP unicast destination address handling	29
	Table 10 – CRP configuration parameters	30
	Table 11 – CRP Set_Assignment_Info service parameters	31
	Table 12 – CRP Get_Redundancy_Info service	33
	Table 13 – CRP Set_Redundancy_Info service	35
	Table 14 – CRP Get_Redundancy_Statistics service	37

INTERNATIONAL ELECTROTECHNICAL COMMISSION

INDUSTRIAL COMMUNICATION NETWORKS – HIGH AVAILABILITY AUTOMATION NETWORKS –

Part 4: Cross-network Redundancy Protocol (CRP)

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

International Standard IEC 62439-4 has been prepared by subcommittee 65C: Industrial Networks, of IEC technical committee 65: Industrial-process measurement, control and automation.

This standard cancels and replaces IEC 62439 published in 2008. This first edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to IEC 62439 (2008):

- adding a calculation method for RSTP (rapid spanning tree protocol, IEEE 802.1Q),
- adding two new redundancy protocols: HSR (High-availability Seamless Redundancy) and DRP (Distributed Redundancy Protocol),
- moving former Clauses 1 to 4 (introduction, definitions, general aspects) and the Annexes (taxonomy, availability calculation) to IEC 62439-1, which serves now as a base for the other documents,
- moving Clause 5 (MRP) to IEC 62439-2 with minor editorial changes,
- moving Clause 6 (PRP) was to IEC 62439-3 with minor editorial changes,

- moving Clause 7 (CRP) was to IEC 62439-4 with minor editorial changes, and
- moving Clause 8 (BRP) was to IEC 62439-5 with minor editorial changes,
- adding a method to calculate the maximum recovery time of RSTP in a restricted configuration (ring) to IEC 62439-1 as Clause 8,
- adding specifications of the HSR (High-availability Seamless Redundancy) protocol, which shares the principles of PRP to IEC 62439-3 as Clause 5, and
- introducing the DRP protocol as IEC 62439-6.

This bilingual version (2012-12) corresponds to the monolingual English version, published in 2010-02.

The text of this standard is based on the following documents:

FDIS	Report on voting
65C/583/FDIS	65C/589/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This International Standard is to be read in conjunction with IEC 62439-1:2010, *Industrial communication networks – High availability automation networks – Part 1: General concepts and calculation methods*.

A list of the IEC 62439 series can be found, under the general title *Industrial communication networks – High availability automation networks*, on the IEC website.

The French version of this standard has not been voted upon.

This publication has been drafted in accordance with ISO/IEC Directives, Part 2.

The committee has decided that the contents of this amendment and the base publication will remain unchanged until the stability date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

INTRODUCTION

The IEC 62439 series specifies relevant principles for high availability networks that meet the requirements for industrial automation networks.

In the fault-free state of the network, the protocols of the IEC 62439 series provide ISO/IEC 8802-3 (IEEE 802.3) compatible, reliable data communication, and preserve determinism of real-time data communication. In cases of fault, removal, and insertion of a component, they provide deterministic recovery times.

These protocols retain fully the typical Ethernet communication capabilities as used in the office world, so that the software involved remains applicable.

The market is in need of several network solutions, each with different performance characteristics and functional capabilities, matching diverse application requirements. These solutions support different redundancy topologies and mechanisms which are introduced in IEC 62439-1 and specified in the other Parts of the IEC 62439 series. IEC 62439-1 also distinguishes between the different solutions, giving guidance to the user.

The IEC 62439 series follows the general structure and terms of IEC 61158 series.

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of a patent concerning a full-duplex Ethernet in which each device periodically transmits a message representing its connectivity to the other devices, allowing them to choose a redundant path in case of failure, given in 7.1 and 7.3.

IEC takes no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured the IEC that he/she is willing to negotiate licences either free of charge or under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with IEC. Information may be obtained from:

Fieldbus Foundation
9005 Mountain Ridge Drive – Bowie Bldg
Suite 190
Austin, TX 78759
USA

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. IEC shall not be held responsible for identifying any or all such patent rights.

ISO (www.iso.org/patents) and IEC (http://www.iec.ch/tctools/patent_decl.htm) maintain on-line data bases of patents relevant to their standards. Users are encouraged to consult the data bases for the most up to date information concerning patents.

INDUSTRIAL COMMUNICATION NETWORKS – HIGH AVAILABILITY AUTOMATION NETWORKS –

Part 4: Cross-network Redundancy Protocol (CRP)

1 Scope

The IEC 62439 series is applicable to high-availability automation networks based on the ISO/IEC 8802-3 (IEEE 802.3) (Ethernet) technology.

This part of the IEC 62439 series specifies a redundancy protocol that is based on the duplication of the network, the redundancy protocol being executed within the end nodes, as opposed to a redundancy protocol built in the switches. The switchover decision is taken in each node individually. The cross-network connection capability enables single attached end nodes to be connected on either of the two networks.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60050-191, *International Electrotechnical Vocabulary – Chapter 191: Dependability and quality of service*

IEC 62439-1:2010, *Industrial communication networks – High availability automation networks – Part 1: General concepts and calculation methods*

ISO/IEC 8802-3:2000, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*

3 Terms, definitions, abbreviations, acronyms, and conventions

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 60050-191, as well as in IEC 62439-1, apply.

3.2 Abbreviations and acronyms

For the purposes of this document, the abbreviations and acronyms given in IEC 62439-1, apply, in addition to the following:

DANC Doubly attached node implementing CRP

SANC Singly attached node implementing CRP

3.3 Conventions

This document follows the conventions defined in IEC 62439-1.

4 CRP overview

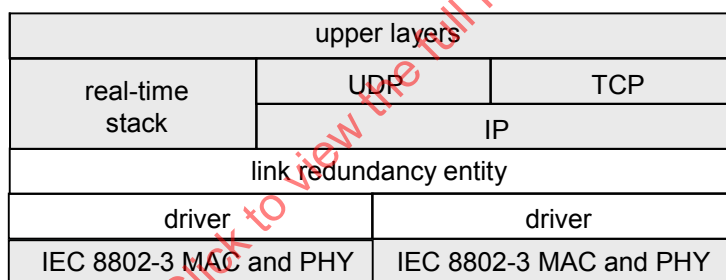
This International Standard specifies a redundancy protocol that is based on the duplication of the network, the redundancy protocol being executed within the end nodes, as opposed to a redundancy protocol built in the switches. There is no central “redundancy manager”; instead each node operates autonomously. The cross-network connection capability enables single attached end nodes to be connected on either of the two networks.

5 CRP nodes

There exists different classes of nodes that may interoperate on the same network:

- DANCs (Doubly Attached Nodes) able to execute the CRP protocol, and having two ports for the purpose of redundancy.
- SANCs (Singly Attached Nodes) able to execute the CRP protocol, and having only one port.
- SAN (Singly Attached Nodes), such as commercially available laptops or file servers that are not aware of the CRP protocol. Even though not aware, SANs can also have access to the redundancy management data for the purpose of monitoring and network management.

In DANCs, these two ports are referred to as port A and port B. They are managed by the Link Redundancy Entity (LRE), whose implementation is not prescribed, and which is conceptually located in the communication stack below the network layer, as illustrated in Figure 1.



LAN_A

LAN_B

IEC 380/10

Figure 1 – CRP stack architecture

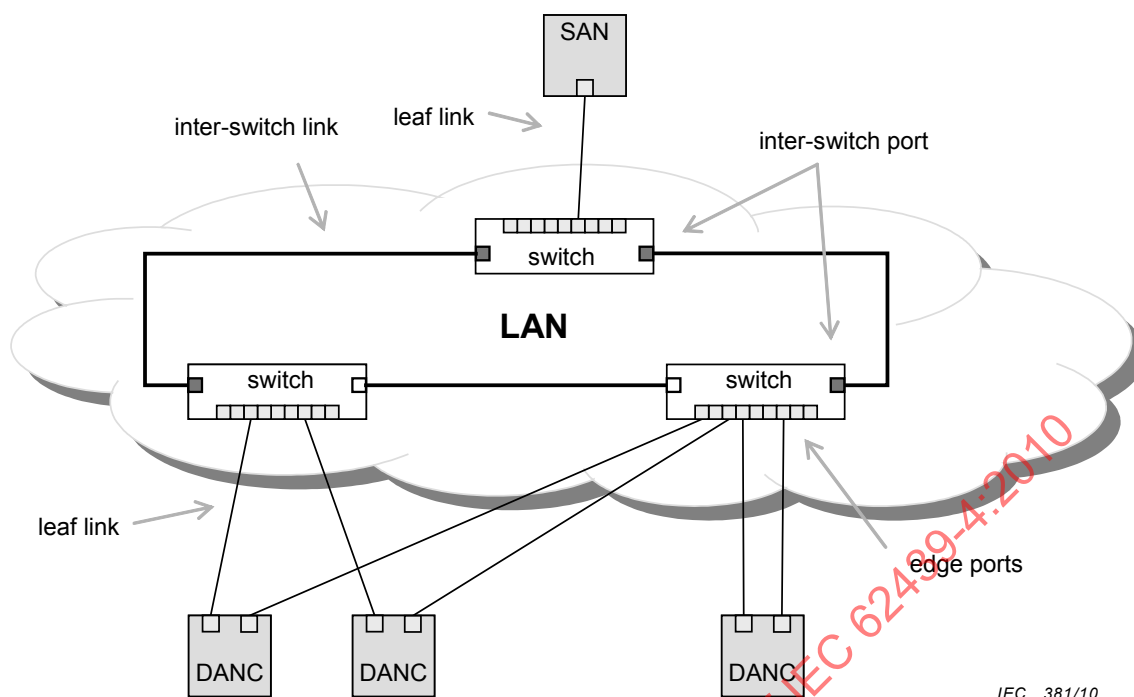
This arrangement provides application-level transparency. The LRE hides redundancy from the upper layers and manages the ports. A node can therefore operate with only one IP address.

6 CRP LAN topology

Implementing the redundancy protocol within the DANCs allows a variety of topologies, using switches that are not aware of the redundancy protocol and could implement another redundancy protocol such as RSTP.

This International Standard does not dictate the topology, but does allow for configuration of node behaviour to accommodate the characteristics of the specific LAN being used.

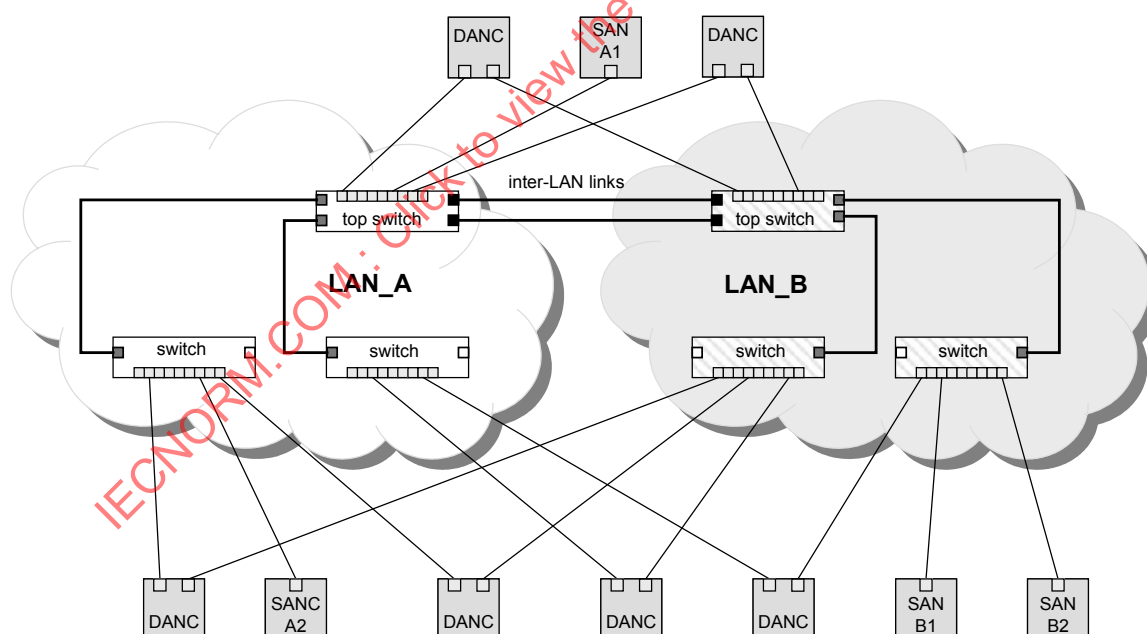
Nodes may be attached to the same or to different switches of a single LAN, which may or may not include redundant links, as Figure 2 shows. Attaching both links to the same switch only provides leaf link failure resilience.



IEC 381/10

Figure 2 – CRP single LAN topography

Nodes may be attached to separate LANs, which are basically failure-independent, but may be connected by an inter-LAN link, as Figure 3 shows.



IEC 382/10

Figure 3 – CRP double LAN topography

When there is only one LAN, a node is attached through both its ports to that LAN. In double LAN configurations, port A is normally connected to LAN_A and port B to LAN_B. Connecting a node twice to the same network tree or connecting port A to LAN_B and vice-versa may be a configuration error called “crossed cables”.

7 CRP key components

7.1 CRP general protocol operation

7.1.1 Doubly-attached nodes (DANCs)

DiagnosticFrames are used to exercise communication paths and to assess the network health. A DiagnosticFrame contains a summary of the reporting node's view of the network health and status, including its own port.

Annunciation frames are sent to announce the existence of the node. These frames are described in 8.7.1

Each DANC sends a pair of DiagnosticFrames periodically, every T_{dmi} , on both of its ports, as Figure 4 shows. Each DANC that receives one DiagnosticFrame on one port expects the other message of the pair on the other port. (On a single LAN, the node receives both messages on both ports.) If a node receives no message or if it does not receive the second DiagnosticFrame on the other port before receiving several more DiagnosticFrames on the same port, it records a fault in the row of the Network_Status_Table for the corresponding node.

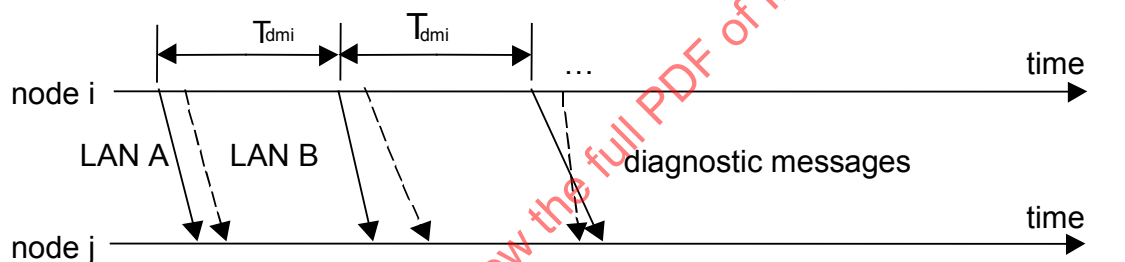


Figure 4 – CRP DiagnosticFrame pair approach

IEC 383/10

In practice the receiving node compares the Sequence_Number of the last message received on the other port with that just received. If the difference in Sequence_Number is more than the configured Max_Sequence_Number_Difference, a fault is recorded.

Based upon the diagnostic frames it receives from all other nodes, each node can select which port to use to send messages to a particular node, on a node-per-node basis.

EXAMPLE Figure 5 shows four nodes connected to two redundant LANs which are not connected with each other. Node 3 and node 4 have link failures. The diagnostic frame handling on node 3 is detailed.

Each node broadcasts its view on the port status of all nodes it detected in addition to other status information (source MAC address, Node_Index, etc.).

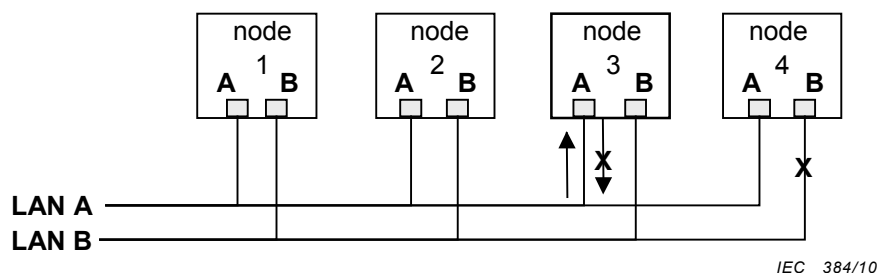
Node 3 maintains a Network_Status_Table populated by the DiagnosticFrames from nodes 1, 2, and 4, as shown in Table 1.

The port status values are OK to indicate a working condition, and X for a don't know or bad condition.

According to the first three columns of the Network_Status_Table in Table 1, node 3 sends out its Received_DiagnosticFrame for port A as [OK, OK, OK, OK] and for port B as [OK, OK, OK, X].

Similarly, node 1 sends out its view on nodes 2, 3, and 4 as [OK, OK, X, OK] for port A and [OK, OK, OK, X] for port B. Node 3's adapter A and adapter B status is populated as shown in Table 1.

The row for node 3 is set based on its own testing, but in this example there is no testing, so all appears to be OK.



Node 3: Interface A partial failure; can receive, but not transmit

Node 4: Interface B complete failure.

Figure 5 – CRP example system

Table 1 – CRP example Network_Status_Table for node 3

Node_Index Number	Received_DiagnosticFrame		Reported status extracted from DiagnosticFrame	
	Received on adapter A	Received on adapter B	Node 3 Received on adapter A	Node 3 Received on adapter B
	Received from adapter A/B ^a	Received from adapter A ^a /B	Received from adapter A/B ^a	Received from adapter A ^a /B
1	OK/X	X/OK	X/X	X/OK
2	OK/X	X/OK	X/X	X/OK
3 (this node)	OK/X	X/OK	OK/X	X/OK
4	OK/X	X/X	X/X	X/X

^a The cross statuses are all "X" for a dual LAN without inter-LAN link. That is, messages originating from a port A are never heard on a port B and vice versa.

The DiagnosticFrames provide therefore:

- minimal assurance of a working path. With each message received, the receiving node can assume that its own receiver, the reporting node's transmitter, and the path through the network are all working;
- assurance that the reverse path is working. With each message received, the receiving node can extract the reporting node's view of the receiving node and thus determine whether its own transmitter, the reporting node's receiver, and the path through the network are all working.

This allows the system administrator to construct a variety of coverage strategies such as:

- ensure that all paths between all nodes are tested;
- send to a single node. This node may be a "diagnostic node" that only provides detection of faults between each node and the diagnostic node.

7.1.2 Singly attached nodes

Singly attached nodes (SANCS) also can send and receive DiagnosticFrames. If they choose to transmit them, the DANCs and SANCS are aware of their presence and attempt to ensure that messages reach them. The Network_Status_Table built by the SANC allows it to build DiagnosticFrames and also, in a single LAN, to select a path to a node with a failed port.

7.2 CRP statistics

Statistics should be gathered and presented for each port, by a system management application. Examples of presentation methods are a graphical user interface for visual reporting of network errors or via SNMP.

7.3 CRP Network_Status_Table

Each node maintains a Network_Status_Table that holds the node's view of the network.

This table is used to assist with selection of which port(s) to use for transmission to a destination address and which port(s) to use for reception of multicast transmissions.

The Network_Status_Table is constructed from received DiagnosticFrames as well as from other locally acquired and sometimes vendor-specific diagnostic information, for example built-in tests, link integrity pulse, etc.

This table is conceptual and is described to assist with understanding of the concepts in this specification and no specific implementation is prescribed or implied. It is therefore not visible to network management; however, the contents of the table are reflected in the DiagnosticFrames.

The Network_Status_Table in each node keeps for each node, and in some cases for each port of each node the following information:

- a) for each remote reporting node,
 - remote node identification (name, index in a table, etc.);
 - diagnosis message interval;
 - apparent number of ports (1..N);
 - for each port, in nominal order (e.g., port to LAN_A before port to LAN_B) the MAC address of the remote port.
- b) for each pairing of local and remote ports (e.g., A/B, B/A, A/A or B/B)
 - time of latest message receipt;
 - sequence number of latest received message;
 - receipt of DiagnosticFrame from remote port within time;
 - remote port's link status from last received DiagnosticFrame.
- c) for assessment of remote connectivity
 - inferred status of set of ports (functioning properly, cross-connected, ...);
 - preferred port pairing.

EXAMPLE Table 2 shows a Network_Status_Table for a SANC and Table 3 a Network_Status_Table for a DANC.

Table 2 – CRP Network_Status_Table for singly connected nodes

Reporting node information			Messages received here sent from reporting node's adapter A				Messages received here sent from reporting node's adapter B			
Node_Index and Node_Name	Number of adapters	Interval (ms)	Time	Sequence number of last message received	Diagnostic Frame received	Reported status extracted from DiagnosticFrame for AA	Time	Sequence number of Last message received	Diagnostic Frame received	Reported status extracted from Diagnostic Frame for BA
1 FD001	1	2 000	Time	Number	OK	OK				
2 FD002	1	2 000	Time	Number	OK	OK				
3 LD001	1	1 000					Time	Number	OK	OK
4										
5 LD003	1	5 000	Time	Number	OK	OK				
6	2	5 000	Time	Number	OK	OK	Time	Number	OK	OK
7	1	5 000	Time	Number	OK	OK				

Reporting node information				Messages received here on adapter A					B ^a		Assessment for reporting node	
Node_Index and Node_Name	Addresses for adapters A, B	Number of adapters	Interval (ms)	A ^b	Sent from reporting node's adapter B			A ^c	B ^d			
				Time	Sequence_ Number of last message received	Diagnostic Frame received	Reported status extracted from Diagnostic Frame for BA	...	...			
1 FD001	addr1.A, addr1.B	2	2 000	...	Time	Number	OK	OK	...	...	Crossed_ cable_status	Selected transmission adapter and receiving adapter
2 FD002	addr2.A, addr2.B	2	2 000	...	Time	Number	OK	OK	...	...	OK	AA
3 LD001	addr3.A, addr3.B	2	1 000	...	Time	Number	OK	OK	...	...	OK	AA
4												
5 LD003	addr5.A, addr5.B	2	5 000	...	Time	Number	OK	OK	...	...	OK	AA
6	addr6.A, addr6.B	2	5 000	...	Time	Number	OK	OK	...	...	OK	BB
7	addr7.A	1	5 000	OK	N/A	N/A	N/A	N/A	NA	NA	OK	AA

a Messages received here on adapter B.

b Sent from reporting node's adapter A.

c Sent from reporting node's adapter A.

d Sent from reporting node's adapter B.

TECHNORM.COM

Click to view the full PDF

62439-4.12070

- a Messages received here on adapter B.
- b Sent from reporting node's adapter A.
- c Sent from reporting node's adapter A.
- d Sent from reporting node's adapter B.

7.4 CRP recovery time

7.4.1 Recovery time calculation

The maximum recovery time from a fault is:

$$t_{\text{rec}} = (1 + \text{Max_Sequence_Number_Difference}) \times t_{\text{dmi}} + t_{\text{path}} + t_{\text{proc}}$$

where

t_{rec} is the recovery time;

t_{dmi} is the time interval of diagnostic frames;

t_{path} is the latency of frame delivery of the network; and

t_{proc} is the processing time of the receiving LAN redundancy entity.

The value of t_{path} is determined by the amount of time the packet takes to travel through the network. In a switched network the worst case transition time through a FIFO based switch is dependent on the number of ports of the switch. It may be necessary to use QoS to respect this delay. The arrival of the packet of interest after all other packets bound for the destination interface of interest produces the worst case delay. In this case the delay is:

$$t_{\text{sw}} = N_{\text{ports}} \times t_{\text{rate}} \times S_{\text{pak}} \times 8$$

where

t_{sw} is the delay time in a single switch;

N_{ports} is the number of switch ports on a single switch;

t_{rate} is the 1/data rate; and

S_{pak} is the max packet size in bytes.

EXAMPLE The following are examples of recovery time for various end node speeds.

Processing time is dominated by the interrupt response time of the end node. For this example an interrupt time of 15 μs is used.

Given: $t_{\text{dmi}} = 400 \text{ ms}$, $t_{\text{proc}} = 15 \mu\text{s}$, $\text{Max_Sequence_Number_Difference} = 1$, $N_{\text{ports}} = 24$ and $S_{\text{pak}} = 1\,522 \text{ bytes}$ for all cases.

For all end nodes with 10 Mbit/s bandwidth:

$$t_{\text{sw}} = 24 \times 10^{-7} \times 1\,522 \times 8 = 0,029 \text{ s}$$

In a single redundant LAN using 6 switches of 24 ports each, and assuming the diagnostic packet traverses all switches, the total t_{path} is $6 \times t_{\text{sw}} = 0,174 \text{ s}$.

Thus,

$$t_{\text{rec}} = 2 \times 0,40 + 0,174 + 0,000\,015 \text{ s}$$

For this example the maximum processing time is negligible thus:

$$t_{\text{rec}} = 0,974 \text{ s}$$

For all end nodes with 100 Mbps bandwidth, the equation scales directly thus

$$t_{\text{sw}} = 24 \times 10^{-8} \times 1\,522 \times 8 = 0,002\,9 \text{ s and for 6 paths} = 0,014\,6 \text{ s}$$

Thus

$$t_{\text{rec}} = 2 \times 0,40 + 0,017\ 4 + 0,000\ 015$$

$$t_{\text{rec}} = 0,817\ 4\ \text{s}$$

7.4.2 Maximum repair time

For faults such as cable breaks there is no repair time. However, in a multiple interface switch topology repairing a failed interface requires replacing the entire switch. In this case powering the switch down to replace it causes additional network disruptions in nodes that have paths through that switch. So as a worst case, the repair time is identical to the recovery time from a fault described in 7.4.1.

7.5 CRP multicast messages

7.5.1 Sending

Multicast messages are always sent from both ports (if both are operational). They carry as source MAC address the address of the port over which they have been sent.

This applies in particular to the DiagnosticFrames and AnnunciationFrames

7.5.2 Receiving

On some network topologies, a single operational multicast message can be received on each of a node's ports. If a node has two ports, the node may be configured to use the Network_Status_Table to select a reception port for multicast operational messages, and so reduce its interrupt and message processing load. Duplicates still need to be detected and discarded.

7.6 CRP unicast messages

7.6.1 Sending a frame

Each unicast frame sent by a CRP redundancy participating node is sent from only one port.

When the LRE receives a frame from the IP stack (or other upper layer), it examines the frame, identifies the destination MAC address and looks up for that address in the Network_Status_Table.

If the A-A path to the destination is OK in the table, the LRE sends the frame to port A, which inserts its address as a source MAC address.

If A-A path is NOT OK in the table, but the A-B path is OK, then the LRE substitutes the B MAC address of the destination node in the frame and sends the frame to port A, which inserts its address as a source MAC address.

If the A-A and A-B paths are both NOT OK, but the B-A path is OK, the LRE sends the frame to port B, which inserts its address as a source MAC address.

If the A-A, A-B and B-A paths are NOT OK, the LRE substitutes the B MAC address of the destination node in the frame and send the frame to port B, which inserts its address as a source MAC address.

If the message is broadcast or multicast, the LRE sends the frame to A if A is working and to B if A is not working.

7.6.2 Receiving a frame

When the LRE receives a frame from the physical layer over port B, it substitutes the destination MAC B to MAC A address, before forwarding the frame up to the stack. Some IP stacks are sensitive to the IP/MAC association being correct. The IP address is not manipulated/substituted in any way on neither transmit nor receive.

7.7 CRP redundancy information

Each node is configured by a user definable mechanism. The configuration determines the details of how each node transmits DiagnosticFrames and how it uses the Network_Status_Table to select transmission and reception ports. This information can be obtained from another node by listening to AnnunciationFrames.

7.8 CRP redundancy statistics

Any node (even if it is not CRP enabled) may gather and display the health of the nodes in the network by subscribing to the multicast address used for the DiagnosticFrames. The application may then generate a Network_Status_Table and use it in any way.

8 CRP protocol

8.1 CRP singly attached node

SANCs shall have one port and shall participate in the CRP redundancy protocol.

8.2 CRP doubly attached node

DANCs shall have two ports and participate in the CRP redundancy protocol.

8.3 CRP Installation, configuration and repair

DANC shall be connected to a single redundant LAN with redundant leaves or to a redundant LAN without redundant leaves as described in Clause 6.

NOTE 1 The former connection provides four possible paths to other doubly connected nodes while the latter provides only two.

In order to achieve switch and leaf link redundancy, each port of a DANC shall be connected to a different switch.

SANC and SAN may be connected to any LAN, but preferably all SANCs and SAN shall be connected to the same LAN.

The assigned Node_Index and Node_Name shall be unique in the network.

The maximum Node_Index is 2 048; the value of 0 shall not be used for Node_Index.

The maximum number of nodes is 2 047.

NOTE 2 This number is limited by the size of the array of status available in the diagnostic packet.

The maximum number of network switch layers of a single redundant LAN with redundant leaves shall be 3.

NOTE 3 This limitation maintains a spanning tree diameter of 7 hops for those networks where spanning tree is used to prevent loops.

8.4 CRP LRE model attributes

8.4.1 Attribute specification

8.4.1.1 Protocol_Version

This configured attribute specifies the CRP protocol used. It is an Unsigned8 with a value of 0x01.

Packets with higher version numbers shall be rejected by lower versions. Newer versions shall revert to compatibility mode when older version packets are received.

8.4.1.2 Number_of_ports

This configured attribute specifies the number of ports on this node for the purpose of redundancy (Unsigned8 = 1 or 2).

8.4.1.3 Max_Sequence_Number_Difference

This configured attribute specifies the maximum acceptable difference between the Sequence_Number parameters in a pair of DiagnosticFrame received from a particular sending node. It shall be an Unsigned8 greater than or equal to 1.

NOTE This attribute affects the speed and accuracy of the dual message approach. The value of Max_Sequence_Number_Difference number is at least one to ensure that faults are not detected by normal incrementing of the Sequence_Number. A number of at least two ensures that a single lost message does not cause detection of faults. Having larger numbers allows tolerance of the loss of several successive messages but slows down speed with which the algorithm detects actual faults, as a trade-off between transient tolerance and detection speed.

8.4.1.4 Redundancy_Flags

This configured attribute specifies five flags that are not transmitted, indicating one or more of the following:

- a) SingleMulticastMessageTransmissionEnabled. This defines the transmission policy for all services with multicast destination addresses except for the DiagnosticFrame.
 - False Transmit on both ports
 - True Transmit on one port
- b) CrossedCableDetectionEnabled.
 - False Do not detect crossed cables
 - True Detect crossed cables
- c) SinglePortMulticastMessageReceptionEnabled. This defines the reception policy for all multicast frames except for the DiagnosticFrame_Addresses for ports A and B.
 - False Listen for multicast addresses on both ports
 - True Listen for multicast addresses on one port except if a fault is detected
- d) DiagnosisUsingOwnMessagesEnabled.
 - False Do not use own DiagnosticFrames for diagnosis
 - True Use own DiagnosticFrames for diagnosis
- e) LoadBalancingEnabled.
 - False Do not balance load
 - True Balance load

8.4.1.5 DiagnosticFrame_Interval

This configured attribute specifies the time interval in milliseconds between successive sending of the DiagnosticFrames as an Unsigned32.

NOTE This parameter is set individually for each end device. This allows tuning of the intervals to provide fast detection of critical end devices while reducing the traffic from other end devices.

8.4.1.6 Ageing time

This configured attribute specifies the time interval in milliseconds used by the LRE to remove silent nodes from its Network_Status_Table.

NOTE 1 The configuration ensures that the value of this attribute is larger than the value of the Max_Sequence_Number_Difference attribute multiplied by the largest value of the DiagnosticFrame_Interval attribute found in received DiagnosticFrames.

NOTE 2 Short ageing times (minutes) mean that DANCs appear and disappear if their power fails briefly. Longer ageing times (days) mean that DANCs that have been removed continue to appear in the Network_Status_Tables.

8.4.1.7 DiagnosticFrame_Address

This configured attribute specifies the 32-bit IP address for DiagnosticFrames. The address may be a broadcast or multicast IP address.

The address 224.0.0.105 has been registered for this purpose.

8.4.1.8 DiagnosticFrame_UDP_source_port

This configured attribute specifies the 16-bit UDP source port used for DiagnosticFrames.

The same port number as for AnnunciationFrames shall not be used.

8.4.1.9 DiagnosticFrame_UDP_destination_port

This configured attribute specifies the 16-bit UDP destination port used for DiagnosticFrames.

The same port number as for AnnunciationFrames shall not be used.

8.4.1.10 Annunciation_UPD_port

This fixed attribute specifies the 16-bit UDP destination source and destination port used for AnnunciationFrames as an Unsigned16 with a value of 1 089.

8.4.1.11 Node_Index

This configured attribute specifies the 16-bit Node_Index of that node.

NOTE The Node_Index is unique for each node in the scope of the DiagnosticFrame_Address.

8.4.1.12 Max_Node_Index

This configured attribute specifies the highest expected Node_Index.

NOTE This number is used to determine the length of the adapter status array and the crossed cable array in the DiagnosticFrame as well as the length of the Network_Status_Table in each end device within the network. The value of this parameter affects the size of DiagnosticFrames; therefore having a very large number adversely impacts performance.

It is recommended that the Max_Node_Index be set to the same value for all devices within the network.

8.4.1.13 Node_Name

This configured attribute is a VisibleString32 octets that specifies a Node_Name that is unique for each node in the scope of the DiagnosticFrame_Address. Unused octets in this field shall be transmitted as ASCII space characters.

8.4.1.14 Annunciation_Interval

This configured attribute specifies the time interval at which AnnunciationFrames are sent.

8.4.1.15 Operational_IP_Address

This configured attribute specifies the IP address used for application communication.

8.4.1.16 Duplicate_Detection_State

This dynamic attribute indicates possible detections of multiple addresses.

It shall be reset to all 0 by configuration or start-up and set upon detection of a conflicting network situation.

It is a bit set encoded as:

0	1	2	3	4	5	6	7
RES						DND	DID

Bit 0 — 5: Reserved

set to 0

Bit 1: DND

1: duplicate name detected,

Bit 0: DID

1: duplicate node index detected,

8.4.1.17 LRE state

This dynamic attribute specifies the state of the LRE as one octet.

0	1	2	3	4	5	6	7
CONF						SYN	

Bit 0 — 6: CONF

0 = reserved

1 = no name configured

2 = operational

3 – 127 = reserved

Bit 7: SYN

0 = Not synchronized with time server

1 = Synchronized with time server

The LRE state shall be reset to all “0” by configuration or start-up.

8.4.1.18 Sequence_Number

This dynamic attribute is a monotonically increasing 32-bit integer that shall start with 0 for the first DiagnosticFrame sent after start-up, incrementing by 1, and rolling over to 0.

8.4.1.19 Path_Status

This dynamic attribute summarizes the view of the node on its paths. It consists of four Path Status sets as Table 4 shows.

Table 4 – CRP Path_Status_Sets

	Remote node sent over	This node received over
Path_Status_A_to_A	A	A
Path_Status_B_to_A	B	A
Path_Status_A_to_B	A	B
Path_Status_B_to_B	B	B

Each Path_Status set consists of a 32-bit aligned sequence of bits, each bit representing a node, using the Node_Index as an offset and indicating the status of the transmission path from the reporting node to this node.

The following values are used for each bit:

- 0 = DiagnosticFrames successfully received
- 1 = DiagnosticFrames not received

EXAMPLE Table 5 shows a Path_Status set for the node with Node_Index 4. This node (4) indicates that it sees:

Node 1: received “A” messages over its LAN A, and “B” messages over its LAN B.

Node 2: did not receive messages for a time longer than Aging Time.

Node 3: received only "A" messages over its LAN_A (it's possibly a SAN).

Node 4: received its own messages over the same port they were sent.

Node 5: received "A" messages over its LAN_A, and "B" messages over its LAN_A – possible configuration error.

Node 6: received "A" messages over its LAN B, and "B" messages over its LAN A – possible crossed cable error.

Table 5 – CRP example of a Path_Status_Set

[illegible]

8.4.1.20 Configuration_Version

This attribute specifies the version of this object as an Unsigned16. Each time the value of any of its other attributes changes by configuration, the version number shall be incremented by 1. Version number 0 indicates that this object has not been configured. This value shall be skipped when rolling over.

8.4.2 Impact of LRE configuration attributes

The impact of the LRE configured attributes is summarized in Table 6 .

Table 6 – CRP configuration attributes impact on LAN operation

Configuration parameter	Dual LAN	Single LAN
Node_Index	Same for both, see 8.4.1.11	
Max_Node_Index	Same for both, see 8.4.1.12	
Max_Sequence_Number_Difference	Same for both, see 8.4.1.3	
DiagnosticFrame_UDP_destination_port	Same for both, see 8.4.1.9	
Redundancy_Flags	This parameter consists of the following five flags	
SingleMulticastMessageTransmissionEnabled	Normally false, allowing multicast messages to be sent on both LANs if the error conditions and presence of SANCs warrants it. Where receiving node loading is critical, however, this may be set true	Normally set true, allowing multicast messages to propagate to both adapters of other nodes. Sending on both adapters increases traffic on the LAN and the receiving nodes
CrossedCableDetectionEnabled	Normally set true. This allows detection of crossed cables	Normally false. Crossed cables have irrelevant on a single LAN
SingleMulticastMessageReceptionEnabled	Normally false, allowing reception of multicasts on either adapter. Because each multicasting node can choose which to send on, listening on both adapters is essential to hear them	Normally true, allowing operating multicast messages propagate to both adapters of other nodes. Listening on both adapters increases traffic on the receiving node
DiagnosisUsingOwnMessagesEnabled	Normally false, preventing DiagnosticFrame sent on one adapter will not be heard on the other	Normally true, allowing DiagnosticFrames sent from one adapter to be received on the other. Using this as a diagnostic improves fault detection, at the cost of processor load
LoadBalancingEnabled	May be set false on a temporary basis to facilitate system maintenance	Normally set false. Load balancing is not applicable to single LAN networks
DiagnosticFrame_Interval	Same for both, see 8.4.1.5	
Aging_Time	Same for both, see 8.4.1.6	
DiagnosticFrame adapter A send address	The address to which DiagnosticFrames are sent on adapters A and B. Usually the same address is used for both adapters	The addresses to which DiagnosticFrames are sent on adapters A and B. The same address may be used to maximize the ability to detect and recover from faults, at a cost of CPU load. Different addresses allow a reduction of traffic seen by the receiving node
DiagnosticFrame adapter B send address		
DiagnosticFrame adapter A receive address	The address to which DiagnosticFrames are received on adapters A and B. Usually the same address is used for	The addresses to which DiagnosticFrames are received on adapters A and B. The same address may be

Configuration parameter	Dual LAN	Single LAN
	both adapters	used to maximize the ability to detect and recover from faults, at a cost of CPU load

8.5 CRP encoding of the DiagnosticFrame

A DiagnosticFrame shall have the content described in Table 7.

Table 7 – CRP DiagnosticFrame format

Parameter name	Offset	Data type	Size	Description
Ethernet DLL header				
Preamble	0		8	Alternating ones and zeros
Destination address	8		6	Broadcast, multicast MAC address
Source address	14		6	Unicast source MAC address of adapter used to send this message
Type	20		2	0x800 for IP datagrams
IP header				
IP version	22		4	IP version (4 bit field) = 4
IP header length				Internet header length (4 bit field) is the length of the internet header in 32 bit words = 6
IP type of service				Type of service (8 bit field) – set all fields = 0 Bits 0-2: precedence. Bit 3: 0 = normal delay, 1 = low delay. Bits 4: 0 = normal throughput, 1 = high throughput. Bits 5: 0 = normal reliability, 1 = high reliability. Bit 6-7: reserved for future use.
IP total length				Length of IP field (16 bit field) in bytes, including IP header and data = 346
IP identifier	26		4	Identifier for fragmented packets. Set = 0
IP flags				Flags (3 bit field) Bit 0: reserved, shall be zero Bit 1: don't fragment = 1 Bit 2: 0 = last fragment
IP fragment offset				Position in original datagram. First fragment = 0
IP time to live	30	Unsigned8	4	Set to 1
IP protocol		Unsigned8		User datagram = 17 (decimal)
IP header checksum				16 bits. The checksum field is the 16 bit one's complement of the one's complement sum of all 16 bit words in the header. For purposes of computing the checksum, the value of the checksum field is zero.
IP source address	34		4	Source_IP_Address.
IP destination address	38		4	Configured DiagnosticFrame_Address, see 8.4.1.7
IP options	42		1	
IP pad	43		3	Pad header to a 32 bit boundary. Pad set = 0
UDP header				
UDP source port	46		2	See 8.4.1.8
UDP destination port	48		2	See 8.4.1.9
UDP length	50		2	Length of UDP field
UDP checksum	52		2	Checksum is the 16-bit one's complement of the one's complement sum of a pseudo header of information from the IP header, the UDP header, and the data.
CRP header				
CRP Protocol_Version	54	Unsigned8	1	see 8.4.1.1
reserved	58	Unsigned24	3	Set to 0x801001
CRP auxiliary address	58	Unsigned32	4	Not used – set to 0
CRP message length	62	Unsigned32	4	Specifies the number of octets contained in the entire message, starting immediately after the UDP header until the end of the message.

Parameter name	Offset	Data type	Size	Description
CRP Body				
CRP Node_Index	66	Unsigned16	2	See 8.4.1.11
CRP Number_of_ports	68	Unsigned8	1	See 8.4.1.2
Transmission adapter	69	Unsigned8	1	Port used to transmit this DiagnosticFrame. 0 = adapter A 1 = adapter B
CRP DiagnosticFrame_Interval	70	Unsigned 32	4	See 8.4.1.5
CRP Node_Name	74	VisibleString	32	See 8.4.1.13
Reserved	106	Unsigned8	1	Reserved, set to zero
CRP Duplicate_Detection_State	107	Unsigned8	1	See 8.4.1.16
Number_Of_Adapter_Stat uses	108	Unsigned16	2	Number of Unsigned32 entries in the Path_Status.
Path_Status_A_to_A	110	array of Unsigned32	See ^a	See Table 4
Path_Status_B_to_A	See a)	array of Unsigned32	See ^a	See Table 4
Path_Status_A_to_B	See a)	array of Unsigned32	See ^a	See Table 4
Path_Status_B_to_B	See a)	array of Unsigned32	See ^a	See Table 4
Sequence_Number	See a)	Unsigned32	4	See 8.4.1.18
Ethernet DLL trailer				
FCS	See a)		4	CRC based frame check sequence
^a The field size and offset depends on the number of adapter statuses, the size of each Path_Status field is 4 x number of adapter statuses, the offset is incremented by the size of the previous field.				

8.6 CRP Encoding of the AnnunciationFrame

An AnnunciationFrame shall have the format shown in Table 8.

Table 8 – CRP AnnunciationFrame

Parameter name	Offset	Data type	Octet length	Description
Preamble	0		8	Alternating ones and zeros
Destination_Address	8		6	Broadcast, multicast MAC address
Source_Address	14		6	Unicast source MAC address of adapter used to send this message.
EtherType	20		2	0x800 for IP datagrams
IP header				
IP Version	0		4	IP Version (4 bit field) = 4
IP header length				Internet Header Length (4 bit field) is the length of the internet header in 32 bit words = 6
IP service				Service (8 bit field) – set all fields = 0 Bits 0-2: precedence. Bit 3: 0 = normal delay, 1 = low delay. Bits 4: 0 = normal throughput, 1 = high throughput. Bits 5: 0 = normal reliability, 1 = high reliability. Bit 6-7: reserved for future use.
IP total length				Length of IP field (16 bit) in bytes, including IP header and data
IP identifier	4		4	Identifier for fragmented packets. Set = 0

Parameter name	Offset	Data type	Octet length	Description
IP flags				Flags (3 bit field) Bit 0: reserved, set to zero Bit 1: don't fragment = 1 Bit 2: 0 = last fragment
IP fragment offset				Position in original datagram. First fragment = 0
IP time to live	8		4	8 bits. Set to 1
IP protocol				8 bits. User datagram = 17 (decimal)
IP header checksum				16 bits. The checksum field is the 16 bit one's complement of the one's complement sum of all 16 bit words in the header. For purposes of computing the checksum, the value of the checksum field is zero.
IP source address	12		4	Source IP address of this node.
IP destination address	16		4	see 8.4.1.7.
IP options	20		1	IP option field
IP pad	21		3	Pad header to a 32 bit boundary. Pad set = 0
UDP header				
UDP source port	0		2	Annunciation port see 8.4.1.8
UDP destination port	2		2	Annunciation port see 8.4.1.9
UDP length	4		2	Length of UDP field
UDP checksum	6		2	Checksum is the 16-bit one's complement of the one's complement sum of a pseudo header of information from the IP header, the UDP header, and the data.
Body				
CRP LRE_State	0	Unsigned8	1	
CRP Reserved0	1	Unsigned8	1	Reserved
CRP Reserved1	2	Unsigned8	1	Reserved
CRP Duplicate_Detection_State	3	Unsigned8	1	see 8.4.1.16
CRP Node_Index	4	Unsigned16	2	see 8.4.1.11
CRP Max_Node_Index	6	Unsigned16	2	see 8.4.1.12
CRP Operational_IP_Address	8	OctetString	16	see 8.4.1.15
CRP ReservedString	24	VisibleString	32	Reserved
CRP Node_Name	56	VisibleString	32	see 8.4.1.13.
CRP Annunciation_Interval	88	Unsigned32	4	see 8.4.1.14
CRP DiagnosticFrame_UDP_Port	92	Unsigned16	2	see 8.4.1.8 and 8.4.1.9
CRP Reserved	94	Unsigned16	2	Reserved, set to 0.
CRP Configuration_Version	96	Unsigned32	4	see 8.4.1.1
CRP User_Option	100	Unsigned32	4	Reserved
CRP Number_Of_Entries	104	Unsigned32	4	Indicates the number of user-defined entries
CRP Entries	108	Unsigned32	4 x	Reserved for user-defined entries

Parameter name	Offset	Data type	Octet length	Description
			Number of entries	
Ethernet DLL trailer				
FCS	0		4	CRC based frame check sequence

8.7 CRP common protocol

8.7.1 AnnunciationFrames

8.7.1.1 Sending

A node shall send an AnnunciationFrame with the format indicated in Table 8:

- after initial power up or warm start;
- following configuration of the node parameters;
- periodically at a rate determined by the Annunciation_Interval.

A SANC shall send the AnnunciationFrame over its port A.

A DANC shall send the AnnunciationFrame over both its port A and port B.

8.7.1.2 Receiving

The receiving node shall include the node sending the AnnunciationFrame to the Network_Status_Table.

8.7.2 DiagnosticFrames

8.7.2.1 Sending

Nodes shall transmit DiagnosticFrames with the format specified in Table 7:

- at startup, or warm start provided the node is configured.
- following a successful node configuration;
- otherwise, at the rate specified by the DiagnosticFrame_Interval (8.4.1.5) attribute;
- as long as the node is in an operational state.

A SANC shall send a DiagnosticFrame over its port A, with:

- the value of the number of ports field set to 1;
- the Sequence_Number incremented by 1 for each successive message sent;
- the sending adapter set to “1” (LAN_A).

A DANC shall send a pair of DiagnosticFrame over both its port A and port B, with:

- the value of the number of ports field set to 2;
- the Sequence_Number incremented by 1 for each successive sending of a pair, and identical Sequence_Numbers fields in both messages of a pair;
- associated MAC address set;
- the sending adapter set to the value corresponding to the adapter over which the message is sent;
- a time spacing not greater than 30 % of the configured DiagnosticFrame_Interval attribute between the two messages of a pair.

8.7.2.2 Receiving

The node shall be configured to receive DiagnosticFrames on its port using the address specified by the DiagnosticFrame_Address attribute at the DiagnosticFrame_UDP_Destination_Port, see 8.4.1.9.

8.7.3 Detection of duplicate Node_Index

If a node receives a DiagnosticFrame from another node that has the same Node_Index as its own, the node shall set the Duplicate_Detection_State attribute to indicate a duplicate Node_Index was detected.

This entry shall be cleared by reconfiguration of the node with a non-duplicate Node_Index.

8.7.4 Detection of duplicate Node_Name

If a node receives a DiagnosticFrame from another node that has the same Node_Name as its own, the node shall set the Duplicate_Detection_State attribute to indicate a duplicate name detected.

This entry shall be cleared by reconfiguration of the node with a non-duplicate Node_Name.

8.7.5 Failure detection based on arrival of DiagnosticFrames

DiagnosticFrames received by a node shall be used in the construction of the Network_Status_Table unless:

- they indicate duplicate Node_Index detected,
- they have a Node_Index greater than Max_Node_Index, or
- their Node_Index is the same as that for this node.

The node shall track the messages arriving from each reporting node by their Sequence_Number.

The DiagnosticFrame_Interval shall not be considered when evaluating arriving messages.

Arrival of the message shall mark the receive status entry for that reporting node and path that did not receive the message as OK.

If a DANC receives a DiagnosticFrame with a Sequence_Number that exceeds by Max_Sequence_Number_Difference the last DiagnosticFrame received on any other path from the given reporting node, it shall mark the DiagnosticFrame received entry for that reporting node as not OK.

The status shall be returned to OK following receipt of a DiagnosticFrame from the reporting node on the path for which a failure had been recorded provided that its Sequence_Number is no smaller than Max_Sequence_Number_Difference to the highest number received. This shall be the only condition that causes the status to be reset to OK.

The DANC shall reflect the status array of the reporting node contained in the DiagnosticFrame in its Network_Status_Tables in the entry associated with the Node_Index of the reporting node.

However, when a node does not receive a DiagnosticFrame for a particular Node_Index for a time superior to Aging_Time, the adapter A and adapter B columns in the Network_Status_Table for that Node_Index shall indicate that all paths to that node are not OK.

NOTE In DiagnosticFrames sent by receiving nodes, the list of port status reflects this not OK status for that Node_Index.

When receiving nodes begin receiving DiagnosticFrames from a node with that Node_Index, it shall not update the messages received here sent from reporting node's adapter A and B columns in the Network_Status_Table for that Node_Index until Max_Sequence_Number_Difference messages are received. This ensures the DiagnosticFrame content is set correctly.

Two entries of this array shall be examined, that corresponding to the receiving node and that corresponding to the reporting node, see 8.7.6.

8.7.6 Status array entries

8.7.6.1 Receiving node entry

The list of DiagnosticFrame received status array shall indicate whether the reporting node has successfully received DiagnosticFrames on each of the four possible paths from this node. This node shall copy this information from the reporting node's DiagnosticFrame into all four of the reported status extracted from the DiagnosticFrame columns of its Network_Status_Table.

8.7.6.2 Reporting node entry

This entry shall indicate that the reporting node has determined whether there are errors on any of the four possible paths from this node. If this entry indicates any status is not OK, it shall be used to update the DiagnosticFrame received status of the Network_Status_Table for the reporting node. Entries with a status of OK shall not be used.

NOTE This may record the fault more quickly than waiting for detection based on the dual message approach.

8.7.7 Other failure detection

Nodes should provide for the option to use vendor-specific diagnostics or commonly used mechanisms to update their own row in the Network_Status_Table.

The faults detected this way should be sent with the DiagnosticFrame and should allow propagation of the detected fault. Whether or not a node detects errors in its adapters, it shall ensure that its own row is correctly initialized and maintained with an OK value.

8.8 CRP operational messages

8.8.1 Load balancing

Nodes that participate in the CRP redundancy approach are able to balance the load for unicast destination addresses between the available transmission adapters. The Redundancy_Flag [LoadBalancingEnabled] shall control the use of load balancing. 8.8.3 defines how the port is selected when load balancing is used.

8.8.2 LAN and port maintenance

Maintenance may be performed on LAN components or port with reduced impact on system operation, if the port or LAN components are not being used. To avoid use of the port or LAN components, the Redundancy_Flag LoadBalancingEnabled shall be set to false.

NOTE Setting this flag to false has the effect of reverting to the method of using the path associated with this node's operational IP address, or best path if there is a fault.

8.8.3 Selecting transmission path

8.8.3.1 General

Selected transmission paths indicate the ports used to transmit operational messages to specific destination addresses. A path shall be defined as the combination of the transmitting node's sending port and the destination address for the receiving node. Path selection shall be evaluated for a specific unicast or multicast destination address at initial use, and then shall be determined following the detection of a fault or the detection of a repaired fault as described in 8.8.3.2 and 8.8.3.3.

8.8.3.2 Unicast destination address

Path for unicast destination addresses shall be selected according to Table 9.

Table 9 – CRP unicast destination address handling

Destination address of:	Path selection
CRP redundancy participating node with DiagnosticFrame received fields and reported status extracted from DiagnosticFrame fields in Network_Status_Table all OK in the A to A and B to B columns. LoadBalancingEnabled is true	Select path randomly (see ^a) and fairly (equal probability of selection) between the adapters
CRP redundancy participating node with DiagnosticFrame received fields and reported status extracted from DiagnosticFrame fields in Network_Status_Table all OK. LoadBalancingEnabled is false.	Select path that is associated with this node's operational IP address that was configured.
CRP redundancy participating node with DiagnosticFrame received fields and reported status extracted from DiagnosticFrame fields in Network_Status_Table that have one or more not OK.	Select path with no fault
CRP redundancy participating node with Number_of_ports = 1 (singly connected node).	Select path that leads to available adapter
Node that does not have a row in the Network_Status_Table, (it is not participating in CRP redundancy).	Use existing path
Nodes that are outside the network, nodes reachable through routers	Use existing path
^a "randomly" means that the node selects for a specific path one adapter rather than the other by using a true random number generator, or a pseudo-random number generator with a different seed, each time the node initializes.	

8.8.3.3 Multicast destination address

8.8.3.3.1 Single multicast message transmission adapter enabled state is true

The single_multicast_message_transmission attribute applies to operational messages.

If there are no errors, the node should send on the adapter that has the most singly connected nodes recorded in the Network_Status_Table. This should be selected by choosing the adapter that has the least number of not applicable entries in its DiagnosticFrame received columns of the Network_Status_Table.

If there is a single error, the node shall send on the adapter that has no error recorded in its DiagnosticFrame received or nodes reporting problems columns of the Network_Status_Table.

Otherwise if there are multiple errors, the node shall send on the adapter that has fewest errors recorded in its DiagnosticFrame received and nodes reporting problems columns of the Network_Status_Table.

If the number of errors is the same for each adapter, no change should be made to the selected transmission adapter for multicast addresses.

8.8.3.3.2 Single_multicast_message_reception_adapter_enabled state is false

If all SANs and DANCs can be reached by sending on a single adapter the node shall send on that adapter. That is, if all the “not OK” and “not applicable” entries recorded in its DiagnosticFrame received and nodes reporting problems columns of the Network_Status_Table are associated with the other port.

Otherwise, the node shall send the multicast over both ports.

8.8.4 Selecting reception adapter

NOTE The intention is to reduce duplicate operational multicast messages.

Nodes shall select a reception adapter when the Redundancy_Flags [single_multicast_message_reception_adapter_enabled] is true.

If [single_multicast_message_reception_adapter_enabled] is false, the node shall listen on both adapters. If it is true, the requirements shall be as follows.

If: no LAN faults are detected, the node listens on its port A. (SANs or SANCs only have an Adapter A.)

Else: use same format as above. If a single LAN fault is detected indicating that one adapter of this node cannot correctly receive transmissions, use other adapter of this node.

If there are multiple faults associated with both adapters, listen on both adapters.

8.8.5 Crossed_cable_status

DiagnosticFrames include a field that identifies the port (A or B) on which the message was sent. For certain LAN topologies, this can be used to determine if the port is connected to the LAN correctly.

8.8.6 Configured parameters

Table 10 contains the minimum parameters that are necessary for the protocol. Additional parameters may be added at the user option.

Table 10 – CRP configuration parameters

Parameter	Description	Data type
Device_Id	descriptive string of the end node	OctetString32
Node_Name	end node name	OctetString32
Node_Index	end node's unique device index	Unsigned16
DiagnosticFrame_UDP_destination_port	UDP port used to receive CRP redundancy messages	Unsigned16
Repeat_Time	end node's annunciation message Repeat_Time.	Unsigned32
Max_Node_Index	highest device index used in the CRP network	Unsigned16
Operational_IP_Address	end node's operational IP address	OctetString16

8.9 CRP services

8.9.1 Configuration options and services

A node may obtain its configuration in three optional ways.

The first is through a local configuration page for those nodes that have a graphical user interface, such as a PC.

The second is through switch configuration where a set of switches configures the device index. The operational IP address would be the sum of a base IP address configured in the device firmware plus the device index.

The third is by a network management node using over the network services that commence upon the reception of an annunciation message. In addition, the network management node has the services to gather the statistics kept by each redundancy capable node. The services are:

- Set_Assignment_Info;
- Get_Redundancy_Info;
- Set_Redundancy_Info;
- Get_Redundancy_Statistics.

8.9.2 LAN redundancy service specification

8.9.2.1 Set_Assignment_Information service

This confirmed service shall be used to set the CRP attributes using the service parameters shown in Table 11.

Table 11 – CRP Set_Assignment_Info service parameters

Parameter name	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
Invoke_Id	M	M(=)		
Source_IP_Address		M		
Source_Port	M	M(=)		
Destination_IP_Address	M	M(=)		
FDA_Address	M	M(=)		
Device_Id	M	M(=)		
Node_Name	M	M(=)		
Node_index	C	C(=)		
DiagnosticFrame_UDP_Destination_Port	C	C(=)		
Repeat_Time	C	C(=)		
Clear_Duplicate_Detection_State	C	C(=)		
Max_Node_Index	C	C(=)		
Operational_IP_Address	C	C(=)		
Result (+)			S	S(=)
Invoke_Id			M	M(=)
Source_IP_Address				M
Destination_IP_Address			M	M(=)
Destination_Port			M	M(=)

Parameter name	Req	Ind	Rsp	Cnf
Repeat_Time			C	C(=)
Max_Node_index			C	C(=)
Result (-)			S	S(=)
Invoke_Id			M	M(=)
Source_IP_Address				M
Destination_IP_Address			M	M(=)
Destination_Port			M	M(=)
Error_Info			M	M(=)
NOTE For the meaning of Req, Ind, Rsp, Cnf, M, U and S, refer to ISO/IEC 10164-1.				

Argument

The argument conveys the parameters of the service request.

Invoke_Id

This parameter contains a value that is determined by the generator of the request and is matched by the responder.

(Unsigned32)

Source_IP_Address

This parameter is the IP address from which the service request was sent. The responder uses it when returning the response.

(OctetString16)

Source_Port

This parameter is the UDP port from which the service request was sent. The responder uses it when returning the response.

(Unsigned16)

Destination_IP_Address

This parameter is the IP address to which the service request is to be sent. The responder uses it when returning the response.

(OctetString16)

FDA_Address

This parameter contains the address to which the service request is being sent.

(Unsigned32)

Device_Id

This parameter contains a descriptive string of the end node.

(OctetString32)

Node_Name

This parameter contains the value of the end node name. The value is not permitted to be blank.

(OctetString32)

Node_index

This conditional parameter contains the value of the end node's unique device index. Its value is not permitted to be zero.

(Unsigned16)

DiagnosticFrame_UDP_Destination_Port

This conditional parameter contains the value of the UDP port used to receive CRP redundancy messages.

(Unsigned16)

Repeat_Time

This conditional negotiable parameter contains the value of the end node's annunciation message repeat time.

(Unsigned32)

Clear_Duplicate_Detection_State

This conditional parameter causes the duplicate detection state to be set to no duplicates detected if it contains a non-zero value.

(Unsigned8)

Max_Node_Index

This conditional negotiable parameter contains the value of the highest device index used in the CRP network.

(Unsigned16)

Operational_IP_Address

This conditional parameter contains the end node's operational IP address.

(OctetString16)

Result (+)

This parameter indicates that the service request succeeded. The following fields are included in the response. Negotiable parameters may be different than the ones sent by the network manager.

Invoke_Id

Source_IP_Address

Destination_IP_Address

Destination_Port

Repeat_Time

Max_Node_Index

Result (-)

This parameter indicates that the service request failed. The following fields are included in the response.

Invoke_Id

Source_IP_Address

Destination_IP_Address

Destination_Port

Error_Info

This parameter specifies the error condition.

8.9.2.2 Get_Redundancy_Info service

This confirmed service shall be used to retrieve CRP Redundancy attributes using the service parameters shown in Table 12.

Table 12 – CRP Get_Redundancy_Info service

Parameter name	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
Invoke_Id	M	M(=)		
Source_IP Address		M		
Destination_IP_Address	M	M(=)		
Result (+)			S	S(=)
Invoke_Id			M	M(=)
Source_IP_Address				M
Destination_IP_Address			M	M(=)

Parameter name	Req	Ind	Rsp	Cnf
LAN_Redundancy_Attributes_Version			M	M(=)
Number_Of_Network_Adapters			M	M(=)
Max_Message_Number_Difference			M	M(=)
Redundancy_Flags			M	M(=)
Diagnostic_Message_Interval			M	M(=)
Aging_Time			M	M(=)
DiagnosticFrame_Send_Adapter_Address			M	M(=)
DiagnosticFrame_Receive_Adapter_Address			M	M(=)
Result (-)			S	S(=)
Invoke_Id			M	M(=)
Source_IP_Address				M
Destination_IP_Address			M	M(=)
Error_Info			M	M(=)

Argument

The argument conveys the parameters of the service request.

Invoke_Id
Source_IP_Address
Destination_IP_Address

Result(+)

This selection type parameter indicates that the service request succeeded. The following fields are included in the response.

Invoke_Id
Source_IP_Address
Destination_IP_Address
LAN_Redundancy_Attributes_Version

This attribute specifies the version of this object. Each time the value of any of its other attributes changes, the version number is incremented by 1. Version number 0 indicates that this object has not been configured.

(Unsigned32)

Number_Of_Network_Adapters

This attribute specifies the number of adapters on this device. A device may have one or two adapters. They are labelled adapter A and adapter B (adapter B is only used if there are two adapters).

(Unsigned8)

Max_Message_Number_Difference

This attribute defines the maximum acceptable difference between the message number parameters in a pair of diagnostic message service indications received from a single sending device. When the difference exceeds the value of this attribute, a fault in the path from the adapter sending the lower message number is detected.

(Unsigned8)

Redundancy_Flags

This attribute is a bit array that controls how messages are sent and received.

(Unsigned8)

Diagnostic_Message_Interval

This attribute defines the time interval in milliseconds between successive sending of the DiagnosticFrames.

(Unsigned32)

Aging_Time

This attribute defines the time interval in milliseconds used by the LRE to remove silent nodes from its Network_Status_Table.

(Unsigned32)

DiagnosticFrame_Send_Adapter_Address

This attribute defines the send address of the diagnostic frame.

(OctetString16)

DiagnosticFrame_Receive_Adapter_Address

This attribute defines the receive address of the diagnostic frame.

(OctetString16)

Result(-)

This parameter indicates that the service request failed. The following fields are included in the response.

Invoke_Id

Source_IP_Address

Destination_IP_Address

Error_Info

This parameter specifies the error condition.

8.9.2.3 Set_Redundancy_Info service

This confirmed service shall be used to retrieve redundancy attributes. After updating the attributes contained in the request, the responder shall return the values and the updated Redundancy_Attributes_Version number, using the service parameters shown in Table 13.

Table 13 – CRP Set_Redundancy_Info service

Parameter name	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
Invoke_Id	M	M(=)		
Source_IP_Address		M		
Destination_IP_Address	M	M(=)		
Redundancy_Attributes_Version			M	M(=)
Number_Of_Network_Adapters			M	M(=)
Max_Message_Number_Difference			M	M(=)
Redundancy_Flags			M	M(=)
DiagnosticFrame_Interval			M	M(=)
Aging_Time			M	M(=)
DiagnosticFrame_Adapter_Send_Addresses			M	M(=)
DiagnosticFrame_Adapter_Receive_Addresses			M	M(=)
Result (+)			S	S(=)
Invoke_Id			M	M(=)
Source_IP_Address				M
Destination_IP_Address			M	M(=)
LAN_Redundancy_Attributes_Version			M	M(=)
Number_Of_Network_Adapters			M	M(=)
Max_Sequence_Number_Difference			M	M(=)
LAN_Redundancy_Flags			M	M(=)
DiagnosticFrame_Interval			M	M(=)

Parameter name	Req	Ind	Rsp	Cnf
Aging_Time			M	M(=)
DiagnosticFrame_Adapter_Send_Addresses			M	M(=)
DiagnosticFrame_Adapter_Receive_Addresses			M	M(=)
Result (-)			S	S(=)
Invoke_Id			M	M(=)
Source_IP_Address				M
Destination_IP_Address			M	M(=)
Error_Info			M	M(=)
NOTE For the meaning of Req, Ind, Rsp, Cnf, M, U and S, refer to ISO/IEC 10164-1.				

Argument

The argument conveys the parameters of the service request:

Invoke_Id
Source_IP_Address
Destination_IP_Address
Redundancy_Attributes_Version
Number_Of_Network_Adapters
Max_Message_Number_Difference
Redundancy_Flags
DiagnosticFrame_Interval
Aging_Time
DiagnosticFrame_Adapter_Send_Addresses
DiagnosticFrame_Adapter_Receive_Addresses

Result(+)

This selection type parameter indicates that the service request succeeded. The following fields are included in the response:

Invoke_Id
Source_IP_Address
Destination_IP_Address
LAN_Redundancy_Attributes_Version
Number_Of_Network_Adapters
Max_Message_Number_Difference
LAN_Redundancy_Flags
DiagnosticFrame_Interval
Aging_Time
DiagnosticFrame_Adapter_Send_Addresses
DiagnosticFrame_Adapter_Receive_Addresses

Result(-)

This parameter indicates that the service request failed. The following fields are included in the response:

Invoke_Id
Source_IP_Address
Destination_IP_Address
Error_Info

8.9.2.4 Get_Redundancy_Statistics service

This confirmed service shall be used to retrieve statistics attributes using the service parameters shown in Table 14.

Table 14 – CRP Get_Redundancy_Statistics service

Parameter name	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
Invoke_Id	M	M(=)		
Source_IP_Address		M		
Destination_IP_Address	M	M(=)		
Result (+)			S	S(=)
Invoke_Id			M	M(=)
Source_IP_Address				M
Destination_IP_Address			M	M(=)
Number_Of_Diagnostic_Message_Service_Indications_Received			M	M(=)
Number_Of_Diagnostic_Message_Service_Indications_Missed			M	M(=)
Number_Of_Faults_Detected			M	M(=)
List_Of_Crossed_Cable_Status			M	M(=)
Result (-)			S	S(=)
Invoke_Id			M	M(=)
Source_IP_Address				M
Destination_IP_Address			M	M(=)
Error_Info			M	M(=)
NOTE For the meaning of Req, Ind, Rsp, Cnf, M, U and S, refer to ISO/IEC 10164-1.				

Argument

The argument conveys the parameters of the service request:

Invoke_Id
Source_IP_Address
Destination_IP_Address

Result(+)

This selection type parameter indicates that the service request succeeded. The following fields are included in the response.

Invoke_Id
Source_IP_Address
Destination_IP_Address
Number_Of_Diagnostic_Message_Service_Indications_Received
This attribute counts the number of diagnostics messages received from all devices.
(Unsigned32)
Number_Of_Diagnostic_Message_Service_Indications_Missed
This attribute counts the number of diagnostics message number gaps from all devices.
The detection of each missed message number from any device causes this counter to be incremented.
(Unsigned32)

Number_Of_Faults_Detected

This attribute counts the total number of faults detected from missed diagnostics messages from all devices. The detection of a fault from any device causes this counter to be incremented.

(Unsigned32)

List_Of_Crossed_Cable_Status

This attribute contains the list of crossed cable status. Value 0 means that the list is not present.

(Unsigned32)

Result(-)

This parameter indicates that the service request failed. The following fields are included in the response.

Invoke_Id

Source_IP_Address

Destination_IP_Address

Error_Info

9 CRP Management Information Base (MIB)

```
-- *****
IEC-62439-4-MIB DEFINITIONS ::= BEGIN

-- *****
-- Imports
-- *****

IMPORTS

    OBJECT-TYPE, Counter32,
    TimeTicks, Integer32 FROM SNMPv2-SMI
    Boolean          FROM HOST-RESOURCES-MIB
    MacAddress        FROM BRIDGE-MIB
    iso               FROM RFC1155-SMI;

-- *****
-- Root OID
-- *****

iec OBJECT IDENTIFIER ::= { iso 0 }

iec62439-4 MODULE-IDENTITY
    LAST-UPDATED "200811100000Z" -- November 10, 2008
    ORGANIZATION "IEC/SC 65C"
    CONTACT-INFO ""

    DESCRIPTION "This MIB module defines the Network Management interfaces
        for the Redundancy Protocol defined by the IEC 62439 series"

    REVISION "200612160000Z" -- December 16, 2006
    DESCRIPTION "Initial version of the Network Management interface for the
        Crossnetwork Redundancy Protocol"

    REVISION "200811100000Z" -- November 10, 2008
    DESCRIPTION "
        Separation of IEC 62439 into a suite of documents
        This MIB applies to IEC 62439-4, no change in functionality
        "

    ::= { IEC 62439 }

-- *****
-- Redundancy Protocols
-- *****

mrp OBJECT IDENTIFIER ::= { iec62439 1 }
```



```

prp          OBJECT IDENTIFIER ::= { iec62439 2 }
crp          OBJECT IDENTIFIER ::= { iec62439 3 }
brp          OBJECT IDENTIFIER ::= { iec62439 4 }
drp          OBJECT IDENTIFIER ::= { iec62439 5 }

-- *****
-- Objects of the CRP Network Management
-- *****

InvokeID OBJECT-TYPE
    SYNTAX Counter32
    MAX-ACCESS read-write
    STATUS mandatory
    DESCRIPTION
        "Value determined by the requestor matched by the responder"
    ::= { crp 1 }
SourceIPAddress OBJECT-TYPE
    SYNTAX OCTET STRING (SIZE(1..16))
    MAX-ACCESS read-write
    STATUS mandatory
    DESCRIPTION
        "the IP address from which the service request was sent"
    ::= { crp 2 }
SourcePort OBJECT-TYPE
    SYNTAX INTEGER
    MAX-ACCESS read-write
    STATUS mandatory
    DESCRIPTION
        "UDP port from which the service request was sent"
    ::= { crp 3 }
DestinationIPAddress OBJECT-TYPE
    SYNTAX OCTET STRING (SIZE(1..16))
    MAX-ACCESS read-write
    STATUS mandatory
    DESCRIPTION
        "the IP address to which the service request is to be sent"
    ::= { crp 4 }
DeviceID OBJECT-TYPE
    SYNTAX OCTET STRING (SIZE(1..32))
    MAX-ACCESS read-write
    STATUS mandatory
    DESCRIPTION
        "a descriptive string of the end node"
    ::= { crp 5 }
NodeName OBJECT-TYPE
    SYNTAX OCTET STRING (SIZE(1..32))
    MAX-ACCESS read-write
    STATUS mandatory
    DESCRIPTION
        "end node name"
    ::= { crp 6 }
NodeIndex OBJECT-TYPE
    SYNTAX INTEGER
    MAX-ACCESS read-write
    STATUS mandatory
    DESCRIPTION
        "the value of the end node's unique device address"
    ::= { crp 7 }
DiagnosticFrameUDPDestinationPort OBJECT-TYPE
    SYNTAX INTEGER
    MAX-ACCESS read-write
    STATUS mandatory
    DESCRIPTION
        "the value of the UDP port used to receive FRP redundancy messages"
    ::= { crp 8 }
RepeatTime OBJECT-TYPE
    SYNTAX INTEGER
    MAX-ACCESS read-write
    STATUS mandatory
    DESCRIPTION
        "the value of the end node's annunciation message repeat time"
    ::= { crp 9 }
ClearDuplicateDetectionState OBJECT-TYPE
    SYNTAX INTEGER {
        noOp (0),
        clearDuplicateDetectionState (1)
    }
    MAX-ACCESS write-only

```

```

    STATUS mandatory
    DESCRIPTION
        "causes the duplicate detection state to be set to no duplicates detected if it
contains a non-zero value"
    ::= { crp 10 }
MaxNodeIndex OBJECT-TYPE
    SYNTAX INTEGER
    MAX-ACCESS read-write
    STATUS mandatory
    DESCRIPTION
        "the value of the highest device index used in the CRP network"
    ::= { crp 11 }
OperationalIPAddress OBJECT-TYPE
    SYNTAX OCTET STRING (SIZE(1..16))
    MAX-ACCESS read-write
    STATUS mandatory
    DESCRIPTION
        "the end node's operational IP address"
    ::= { crp 12 }

END

```

IECNORM.COM : Click to view the full PDF of IEC 62439-4:2010

Bibliography

IEC 61158 (all parts), *Industrial communication networks – Fieldbus specifications*

IEC 62439-2, *Industrial communication networks – High availability automation networks – Part 2: Media Redundancy Protocol (MRP)* IEC 62439-3, *Industrial communication networks – High availability automation networks – Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)*

IEC 62439-5, *Industrial communication networks – High availability automation networks – Part 5: Beacon Redundancy Protocol (BRP)*

IEC 62439-6, *Industrial communication networks – High availability automation networks – Part 6: Distributed Redundancy Protocol (DRP)*

ISO/IEC 10164-1, *Information technology – Open Systems Interconnection – Systems Management : Object Management Function*

IECNORM.COM : Click to view the full PDF of IEC 62439-4:2010

SOMMAIRE

AVANT-PROPOS	44
INTRODUCTION	46
1 Domaine d'application	47
2 Références normatives	47
3 Termes, définitions, abréviations, acronymes et conventions	47
3.1 Termes et définitions	47
3.2 Abréviations et acronymes	47
3.3 Conventions	48
4 Aperçu CRP	48
5 Nœuds CRP	48
6 Topologie LAN CRP	49
7 Composants-clés CRP	50
7.1 Exécution du protocole général CRP	50
7.1.1 Nœuds doubles (DANC)	50
7.1.2 Nœuds simples	53
7.2 Statistiques CRP	53
7.3 Network_Status_Table CRP	53
7.4 Durée de rétablissement CPR	56
7.4.1 Calcul de la durée de rétablissement	56
7.4.2 Durée maximale de réparation	57
7.5 Messages multicast CRP	57
7.5.1 Envoi	57
7.5.2 Réception	57
7.6 Messages unicast CRP	57
7.6.1 Envoi d'une trame	57
7.6.2 Réception d'une trame	58
7.7 Informations de redondance CRP	58
7.8 Statistiques de redondance CRP	58
8 Protocole CRP	58
8.1 Nœud simple CRP	58
8.2 Nœud double CRP	58
8.3 Installation, configuration et réparation CRP	58
8.4 Attributs du modèle LRE CRP	59
8.4.1 Spécifications des attributs	59
8.4.2 Impact des attributs de configuration des LRE	63
8.5 Codage CRP de DiagnosticFrame	64
8.6 Codage CRP d'AnnunciationFrame	66
8.7 Protocole commun CRP	68
8.7.1 AnnunciationFrames	68
8.7.2 DiagnosticFrames	68
8.7.3 Détection de Node_Index dupliqué	69
8.7.4 Détection de Node_Name dupliqué	69
8.7.5 Détection de défaillances sur la base de l'arrivée de DiagnosticFrames	69
8.7.6 Entrées de la liste de statuts	70
8.7.7 Autre détection de défaillance	70

8.8	Messages opérationnels CRP.....	70
8.8.1	Equilibrage de charge.....	70
8.8.2	Maintenance de LAN et de port	71
8.8.3	Sélection du chemin de transmission.....	71
8.8.4	Sélection de l'adaptateur de réception	72
8.8.5	Crossed_cable_status	72
8.8.6	Paramètres configurés.....	72
8.9	Services CRP	73
8.9.1	Options de configuration et services	73
8.9.2	Spécification du service de redondance LAN	73
9	Base d'information de gestion CRP (MIB).....	81
	Bibliography.....	84
	Figure 1 – Architecture pile CRP.....	48
	Figure 2 – Topographie de réseau LAN simple CRP	49
	Figure 3 – Topologie de réseau LAN double CRP	50
	Figure 4 – Approche de paire de <i>DiagnosticFrame</i> CRP.....	51
	Figure 5 – Système exemple CRP.....	52
	Tableau 1 – Network_Status_Table exemple CRP pour nœud 3	52
	Tableau 2 – CRP Network_Status_Table pour nœuds simples	54
	Tableau 3 – CRP Network_Status_Table pour DANC.....	55
	Tableau 4 – CRP Path_Status_Sets.....	62
	Tableau 5 – Exemple de CRP d'un Path_Status_Set.....	63
	Tableau 6 – Impact des attributs de configuration CRP sur le fonctionnement LAN	63
	Tableau 7 – Format des DiagnosticFrames CRP	65
	Tableau 8 – CRP AnnunciationFrame	66
	Tableau 9 – Gestion des adresses de destination unicast	71
	Tableau 10 – Paramètres de configuration CRP.....	73
	Tableau 11 – Service CRP Set_Assignment_Info.....	74
	Tableau 12 – Service CRP Get_Redundancy_Info	76
	Tableau 13 – Service CRP Set_Redundancy_Info.....	78
	Tableau 14 – Service CRP Get_Redundancy_Statistics	80

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

**RÉSEAUX DE COMMUNICATION INDUSTRIELS –
RÉSEAUX D'AUTOMATISATION À HAUTE DISPONIBILITÉ –****Partie 4: Protocole de redondance inter-réseau (CRP)****AVANT-PROPOS**

- 1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) La CEI elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.

La Norme internationale CEI 62439-4 a été établie par le sous-comité 65C: Réseaux de communication industriels, du comité d'études 65 de la CEI: Mesure, commande et automation dans les processus industriels.

La présente norme annule et remplace la CEI 62439 publiée en 2008. Cette première édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à la CEI 62439 (2008):

- ajout d'une méthode de calcul pour les RSTP (Rapid spanning tree protocol, IEEE 802.1Q),
- ajout de deux nouveaux protocoles de redondance: HSR (High-availability Seamless Redundancy) et DRP (Distributed Redundancy Protocol),
- transfert des anciens Articles 1 à 4 (introduction, définitions, aspects généraux) et des Annexes (taxonomie, calcul de disponibilité) dans la CEI 62439-1, qui sert désormais de base pour les autres documents,

- transfert de l'Article 5 (MRP) dans la CEI 62439-2 avec des modifications éditoriales mineures,
- transfert de l'Article 6 (PRP) dans la CEI 62439-3 avec des modifications éditoriales mineures,
- transfert de l'Article 7 (CRP) dans la CEI 62439-4 avec des modifications éditoriales mineures, et
- transfert de l'Article 8 (BRP) dans la CEI 62439-5 avec des modifications éditoriales mineures,
- ajout d'une méthode de calcul de la durée maximale de rétablissement de RSTP dans une configuration réduite (anneau) dans la CEI 62439-1 comme Article 8,
- ajout de spécifications de protocole HSR (High-availability Seamless Redundancy), qui partage les principes de PRP dans la CEI 62439-3 comme Article 5, et
- introduction du protocole DRP en tant que CEI 62439-6.

La présente version bilingue (2012-12) correspond à la version anglaise monolingue publiée en 2010-02.

Le texte anglais de cette norme est issu des documents 65C/583/FDIS et 65C/589/RVD.

Le rapport de vote 65C/589/RVD donne toute information sur le vote ayant abouti à l'approbation de cette norme.

La version française n'a pas été soumise au vote.

La présente Norme internationale doit être lue conjointement avec la CEI 62439-1:2010, *Réseaux de communication industriels – Réseaux d'automatisation à haute disponibilité – Partie 1: Concepts généraux et méthodes de calcul*.

Une liste de la série CEI 62439 est disponible sur le site web de la CEI, sous le titre général *Réseaux de communication industriels – Réseaux d'automatisation à haute disponibilité*.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Le comité a décidé que le contenu de cet amendement et de la publication de base ne sera pas modifié avant la date de stabilité indiquée sur le site web de la CEI sous "<http://webstore.iec.ch>" dans les données relatives à la publication recherchée. À cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

INTRODUCTION

La CEI 62439 précise des principes importants pour les réseaux à haute disponibilité conformes aux exigences des réseaux d'automatisation industriels.

En l'absence de panne du réseau, les protocoles de la CEI 62439 garantissent une communication des données fiable compatible avec l'ISO/CEI 88023 (IEEE 802.3) et préservent le déterminisme de la communication de données en temps réel. En cas de panne, retrait et insertion d'un composant, ils assurent des temps de rétablissement déterministes.

Ces protocoles possèdent toutes les capacités typiques de communication Ethernet utilisées dans le monde des bureaux, de sorte que le logiciel correspondant reste applicable.

Le marché a besoin de plusieurs solutions de réseau, chacune présentant différentes caractéristiques de performance et capacités fonctionnelles, conformes à diverses exigences d'application. Ces solutions prennent en charge différentes topologies de redondance et mécanismes introduits dans la CEI 62439-1 et précisés dans les autres parties de la CEI 62439. La CEI 62439-1 distingue également les différentes solutions, conseillant ainsi l'utilisateur.

La CEI 62439 suit la structure générale et les termes de la série CEI 61158.

La Commission Électrotechnique Internationale (CEI) attire l'attention sur le fait qu'il est déclaré que la conformité avec les dispositions du présent document peut impliquer l'utilisation d'un brevet concernant un système Ethernet duplex intégral dans lequel chaque dispositif émet de manière périodique un message représentant sa connectivité vis-à-vis des autres dispositifs, leur permettant de choisir un chemin redondant en cas de défaillance, donné en 7.1 et en 7.3.

La CEI ne prend pas position quant à la preuve, la validité et la portée des droits de propriété intellectuelle.

Le détenteur de ces droits a donné l'assurance à la CEI qu'il consentait à négocier les licences correspondantes aux demandeurs du monde entier, soit à titre gratuit soit en des termes et à des conditions raisonnables et non discriminatoires. À ce propos, la déclaration du détenteur des droits de ce brevet est enregistrée à la CEI. Des informations peuvent être obtenues auprès de:

Fieldbus Foundation

9005 Mountain Ridge Drive – Bowie Bldg

Suite 190

Austin, TX 78759

USA

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle autres que ceux identifiés ci-dessus. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété.

L'ISO (www.iso.org/patents) et la CEI (http://www.iec.ch/tctools/patent_decl.htm) tiennent à jour des bases de données en ligne concernant les brevets intéressant leurs normes. Les utilisateurs sont invités à consulter ces bases de données pour connaître les dernières informations à jour concernant les brevets.

RÉSEAUX DE COMMUNICATION INDUSTRIELS – RÉSEAUX D'AUTOMATISATION À HAUTE DISPONIBILITÉ –

Partie 4: Protocole de redondance inter-réseau (CRP)

1 Domaine d'application

La CEI 62439 est applicable aux réseaux d'automatisation à haute disponibilité basés sur la technologie ISO/CEI 8802-3 (IEEE 802.3) (Ethernet).

La présente partie de la CEI 62439 définit un protocole de redondance basé sur la duplication du réseau, le protocole de redondance étant exécuté dans les nœuds terminaux, par opposition à un protocole de redondance intégré aux commutateurs. La décision de commutation est prise individuellement par chaque nœud. La capacité de connexion inter-réseau permet à des nœuds terminaux simples d'être connectés à l'un ou l'autre des deux réseaux.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

CEI 60050-191, *Vocabulaire Electrotechnique International – Chapitre 191: Sureté de fonctionnement et qualité de service*

IEC 62439-1:2010, *Industrial communication networks – High availability automation networks – Part 1: General concepts and calculation methods* (disponible en anglais uniquement)

ISO/IEC 8802-3:2000, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications* (disponible en anglais uniquement)

3 Termes, définitions, abréviations, acronymes et conventions

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans la CEI 60050-191, ainsi que dans la CEI 62439-1, s'appliquent.

3.2 Abréviations et acronymes

Pour les besoins du présent document, les abréviations et acronymes donnés dans la CEI 62439-1 ainsi que les suivants s'appliquent:

DANC Doubly attached node implementing CRP (nœud double avec implémentation CRP)

SANC Single attached node implementing CRP (nœud simple avec implémentation CRP)

3.3 Conventions

Le présent document suit les conventions définies dans la CEI 62439-1.

4 Aperçu CRP

La présente norme internationale précise un protocole de redondance basé sur la duplication du réseau, le protocole de redondance étant exécuté dans les nœuds terminaux contrairement à un protocole de redondance intégré aux commutateurs. Il n'existe pas de "gestionnaire de redondance", chaque nœud fonctionne de manière autonome. La capacité de connexion inter-réseau permet à des nœuds terminaux simples d'être connectés à l'un ou l'autre des deux réseaux.

5 Nœuds CRP

Il existe différentes catégories de nœuds susceptibles d'inter-opérer sur le même réseau:

- les DANC (nœuds doubles) capables d'exécuter le protocole CRP et dotés de deux ports assurant la redondance.
- les SANC (nœuds simples) capables d'exécuter le protocole CRP et dotés d'un seul port.
- les SAN (nœuds simples), tels que les ordinateurs portables usuels ou les serveurs de fichiers non configurés pour le protocole CRP. Bien qu'ils ne soient pas configurés en fonction, les SAN peuvent également accéder aux données de gestion de la redondance, à des fins de surveillance et de gestion du réseau.

Dans les DANC, les deux ports sont désignés port A et port B. Ils sont gérés par l'Entité de redondance de liens (LRE) dont l'implémentation n'est pas prescrite et qui est conceptuellement située dans la pile de communication en dessous de la couche réseau, comme représenté à la Figure 1.

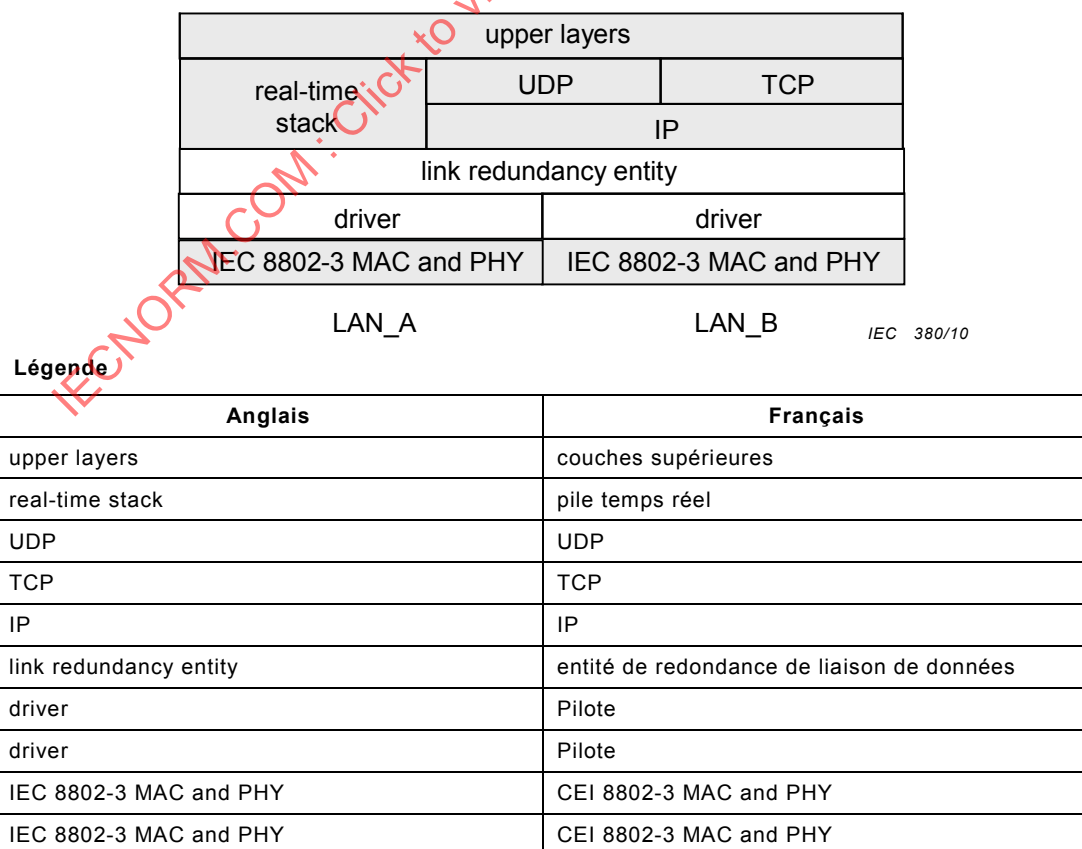


Figure 1 – Architecture pile CRP

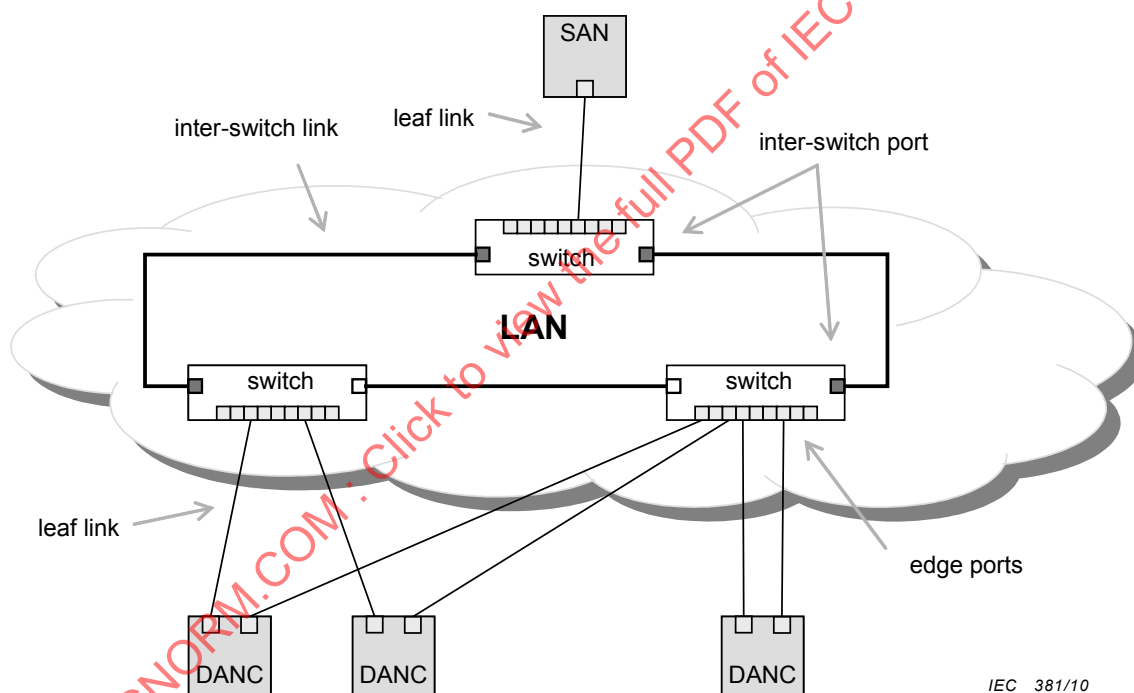
Cet arrangement garantit la transparence au niveau de l'application. La LRE cache la redondance des couches supérieures et gère les ports. Un nœud peut alors fonctionner avec une adresse IP seulement.

6 Topologie LAN CRP

L'implémentation du protocole de redondance dans les DANC autorise diverses topologies, se servant de commutateurs non configurés pour le protocole de redondance et pouvant implémenter un autre protocole de redondance, tel que le RSTP.

Cette norme internationale n'impose pas la topologie, mais permet la configuration du comportement des nœuds, afin d'accommoder les caractéristiques du réseau LAN spécifique utilisé.

Les nœuds peuvent être liés aux mêmes commutateurs ou à des commutateurs différents d'un même LAN, qui peut comprendre des liaisons redondantes ou non, comme représenté à la Figure 2. La connexion des deux liaisons au même commutateur garantit uniquement la résistance aux défaillances de feuilles.



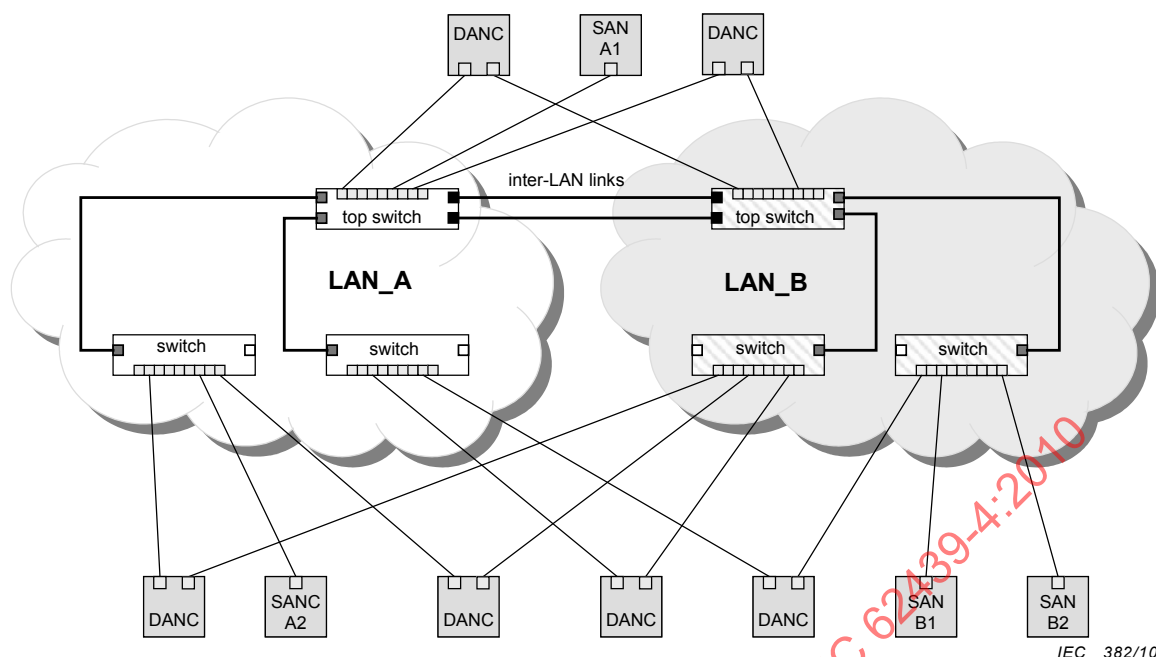
IEC 381/10

Légende

Anglais	Français
liaison inter-commutateur	liaison inter-commutateur
feuille	feuille
commutateur	commutateur
port inter-commutateur	port inter-commutateur
DANC	DANC
ports d'extrémité	ports d'extrémité

Figure 2 – Topographie de réseau LAN simple CRP

Les nœuds peuvent être liés à des réseaux LAN séparés, fondamentalement indépendants en cas de défaillance, mais pouvant être connectés par une liaison inter-LAN, comme représenté à la Figure 3.



IEC 382/10

Légende

Anglais	Français
inter-LAN links	Liaisons inter-LAN
LAN A	LAN A
Switch	commutateur
LAN B	LAN B
DANC	DANC
top Switch	commutateur principal
SAN A1	SAN A1

Figure 3 – Topologie de réseau LAN double CRP

Lorsqu'il n'y a qu'un seul réseau LAN, un nœud est lié à ce LAN par ses deux ports. En cas de configurations à double LAN, le port A est généralement connecté au LAN_A et le port B au LAN_B. La double connexion d'un nœud à la même arborescence de réseau ou la connexion du port A au LAN_B et vice versa peut entraîner une erreur de configuration appelée "câbles croisés".

7 Composants-clés CRP

7.1 Exécution du protocole général CRP

7.1.1 Nœuds doubles (DANC)

Les trames de diagnostic (*DiagnosticFrames*) sont utilisées pour suivre les chemins de communication et évaluer la santé du réseau. Une *DiagnosticFrames* contient un résumé de l'aperçu de la santé et de l'état du réseau livré par le nœud de rapport, y compris son propre port.

Les trames d'annonce sont envoyées pour annoncer l'existence du nœud. Ces trames sont décrites en 8.7.1.

Chaque DANC envoie périodiquement une paire de *DiagnosticFrames*, tous les T_{dmi} , sur ses deux ports, comme représenté à la Figure 4. Chaque DANC recevant un *DiagnosticFrame* sur un port attend l'autre message de la paire sur son autre port (dans un réseau LAN simple, le

nœud reçoit les deux messages sur ses deux ports). Si un nœud ne reçoit pas de message ou s'il ne reçoit pas de second *DiagnosticFrame* sur son autre port, avant de recevoir plusieurs autres *DiagnosticFrames* sur le même port, il enregistre une panne dans la ligne du *Network_Status_Table* du nœud correspondant.

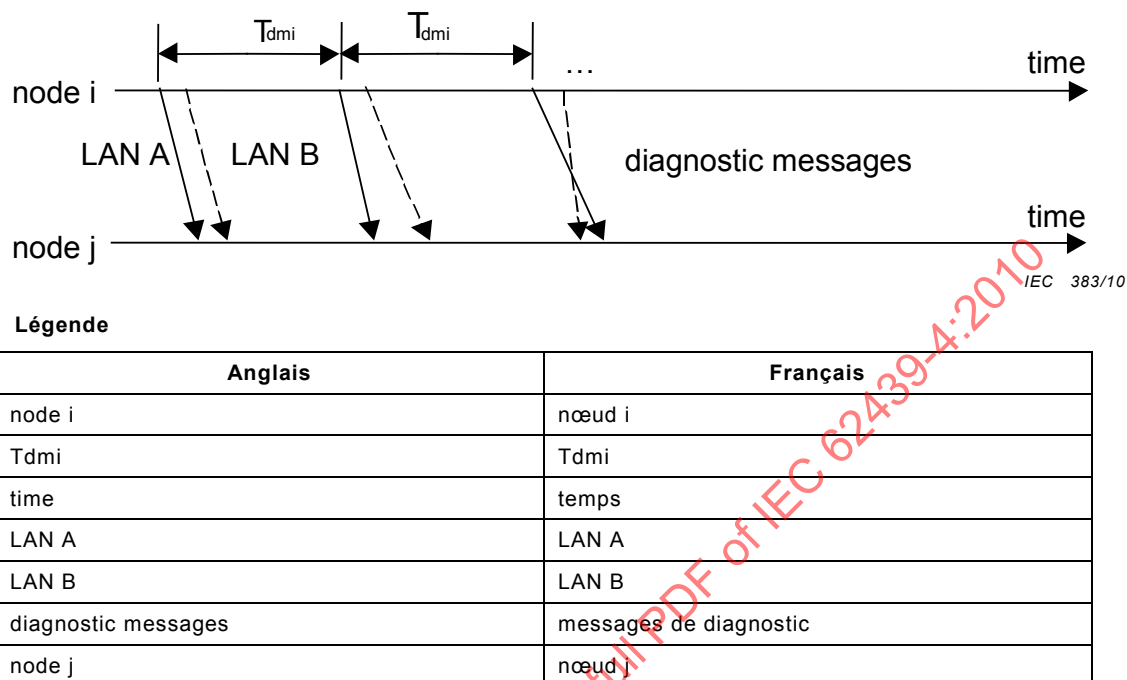


Figure 4 – Approche de paire de *DiagnosticFrame* CRP

En pratique, le nœud récepteur compare le *Sequence_Number* du dernier message reçu sur l'autre port l'ayant juste reçu. Si la différence de *Sequence_Number* est supérieure à la *Max_Sequence_Number_Difference* configurée, une panne est enregistrée.

Sur la base des trames de diagnostic reçues des autres nœuds, chaque nœud peut sélectionner le port qu'il souhaite utiliser pour l'envoi de messages à un nœud particulier, sur une base de nœud par nœud.

EXEMPLE La Figure 5 représente quatre nœuds connectés à deux LAN redondants non connectés entre eux. Les nœuds 3 et 4 présentent des défaillances de liaison. La gestion de la trame de diagnostic du nœud 3 est détaillée.

Chaque nœud émet ses conclusions sur l'état des ports de tous les nœuds qu'il détecte en plus d'autres informations d'état (adresse MAC source, *Node_Index*, etc.).

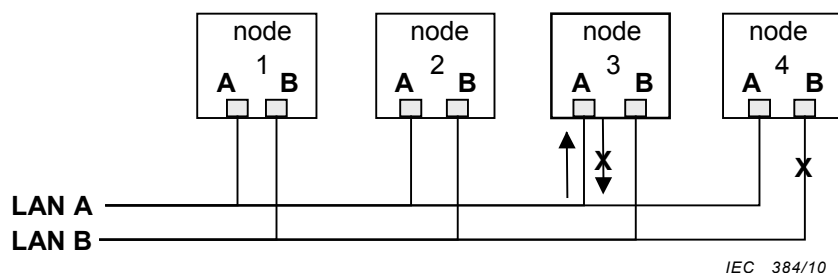
Le nœud 3 garantit le remplissage d'un *Network_Status_Table* par les *DiagnosticFrames* des nœuds 1, 2 et 4, comme indiqué dans le Tableau 1.

La valeur d'état des ports est OK lorsqu'ils sont en bonne condition de fonctionnement et X lorsqu'ils sont dans une condition inconnue ou incorrecte.

Selon les trois premières colonnes du *Network_Status_Table* du Tableau 1, le nœud 3 envoie le *Received_DiagnosticFrame* au port A sous la forme [OK, OK, OK, OK] et au port B sous la forme [OK, OK, OK, X].

De même, le nœud 1 envoie ses conclusions sur les nœuds 2, 3 et 4 sous la forme [OK, OK, X, OK] au port A et [OK, OK, OK, X] au port B. L'état des adaptateurs A et B du nœud 3 est indiqué comme suit dans le Tableau 1.

La rangée du nœud 3 est réglée sur la base de ses propres essais mais dans cet exemple, il n'y a pas d'essai, donc tout semble OK.



Node 3: Interface A partial failure; can receive, but not transmit
Node 4: Interface B complete failure.

Légende

Anglais	Français
node	nœud
LAN A	LAN A
LAN B	LAN B
Node 3: Interface A partial failure; can receive, but not transmit	Nœud 3: Défaillance partielle de l'interface A; peut recevoir, mais pas transmettre
Node 4: Interface B complete failure	Nœud 4: Défaillance complète de l'interface B

Figure 5 – Système exemple CRP

Tableau 1 – Network_Status_Table exemple CRP pour nœud 3

Node_Index Number	Received_DiagnosticFrame		État rapporté extrait du DiagnosticFrame	
	Reçu sur l'adaptateur A	Reçu sur l'adaptateur B	Nœud 3 Reçu sur l'adaptateur A	Nœud 3 Reçu sur l'adaptateur B
	Reçu de l'adaptateur A/B ^a	Reçu de l'adaptateur A ^a /B	Reçu de l'adaptateur A/B ^a	Reçu de l'adaptateur A ^a /B
1	OK/X	X/OK	X/X	X/OK
2	OK/X	X/OK	X/X	X/OK
3 (ce nœud)	OK/X	X/OK	OK/X	X/OK
4	OK/X	X/X	X/X	X/X

^a Les états croisés correspondent à tous les "X" pour un LAN double sans lien inter-LAN. C'est-à-dire que les messages originaires d'un port A ne sont jamais connus sur le port B et vice versa.

Les DiagnosticFrames offrent ainsi:

- l'assurance minimale d'un chemin opérationnel. Pour chaque message reçu, le nœud reçu peut s'assurer que son propre récepteur, l'émetteur du nœud de rapport et le chemin traversant le réseau, fonctionnent tous;
- l'assurance que le chemin inverse fonctionne. Avec chaque message reçu, le nœud reçu peut extraire les conclusions du nœud de rapport sur le nœud récepteur et déterminer ainsi si son propre émetteur, le récepteur du nœud de rapport et le chemin traversant le réseau fonctionnent tous.

Cela permet à l'administrateur du système de construire une large variété des stratégies de couverture, telles que:

- s'assurer que tous les chemins entre les nœuds sont testés ;
- envoyer sur un nœud simple. Ce nœud peut être un "nœud de diagnostic" qui permet uniquement la détection de pannes entre chaque nœud et le nœud de diagnostic.

7.1.2 Nœuds simples

Les nœuds simples (SANC) peuvent également envoyer et recevoir des DiagnosticFrames. S'ils choisissent de les transmettre, les DANC et les SANC détectent leur présence et tentent de s'assurer que les messages les atteignent. Le Network_Status_Table établi par le SANC permet de construire des DiagnosticFrames et, dans un LAN simple, de sélectionner un chemin vers un nœud au port défaillant.

7.2 Statistiques CRP

Il convient de collecter et de présenter les statistiques pour chaque port, par une application de gestion de système. Les exemples de méthodes de présentation sont une interface utilisateur graphique pour le rapport visuel d'erreurs du réseau ou via SNMP.

7.3 Network_Status_Table CRP

Chaque nœud entretient un Network_Status_Table contenant les conclusions du nœud sur le réseau.

Ce tableau est utilisé pour aider à la sélection du/des port(s) à utiliser pour la transmission à une adresse de destination définie et du/des port(s) à utiliser pour la réception de transmissions multicast.

Le Network_Status_Table est constitué à partir des DiagnosticFrames reçus, ainsi que d'autres informations de diagnostic acquises localement et parfois spécifiques au vendeur, par exemple les essais intégrés, les impulsions de contrôle d'intégrité de liaison, etc.

Ce tableau est conceptuel et est décrit pour aider à la compréhension des concepts de ces spécifications. Aucune implémentation spécifique n'est prescrite ou impliquée. Il n'est donc pas visible à la gestion du réseau; cependant les contenus du tableau sont reflétés dans les DiagnosticFrames.

Le Network_Status_Table de chaque nœud enregistre pour chaque nœud, et dans certains cas, pour chaque port de chaque nœud, les informations suivantes:

- a) pour chaque nœud de rapport à distance,
 - identification de nœud à distance (nom, index dans un tableau, etc.);
 - intervalle de message de diagnostic;
 - nombre de ports apparents (1...N);
 - pour chaque port, par ordre nominal (p. ex. port LAN_A avant port LAN_B) l'adresse MAC du port à distance.
- b) pour chaque paire de ports locaux et à distance (p. ex. A/B, B/A, A/A ou B/B)
 - heure de réception du dernier message;
 - numéro de séquence du dernier message reçu;
 - réception de DiagnosticFrame à partir du port à distance dans un certain délai;
 - état de liaison du port à distance à partir du dernier DiagnosticFrame reçu.
- c) pour l'évaluation de la connectivité à distance
 - statut supposé d'un ensemble de ports (fonctionnement correct, interconnecté, ...);
 - couplage de port préféré.

EXEMPLE Le Tableau 2 représente un Network_Status_Table pour SANC et le Tableau 3 un Network_Status_Table pour DANC.

Tableau 2 – CRP Network_Status_Table pour nœuds simples

Informations du nœud de rapport			Messages reçus ici envoyés par l'adaptateur A du nœud de rapport				Messages reçus ici envoyés par l'adaptateur B du nœud de rapport			
Node_Index et Node_Nom	Nombre d'adaptateurs	Intervalle (ms)	Time	Sequence – nombre du dernier message reçu	Diagnostic Frame reçu	Etat rapporté extrait du DiagnosticFrame pour AA	Time	Sequence – nombre du dernier message reçu	Diagnostic cFrame reçu	Etat rapporté extrait du DiagnosticFrame pour BA
1 FD001	1	2 000	Time	Numéro	OK	OK				
2 FD002	1	2 000	Time	Numéro	OK	OK				
3 LD001	1	1 000					Time	Numéro	OK	OK
4										
5 LD003	1	5 000	Time	Numéro	OK	OK				
6	2	5 000	Time	Numéro	OK	OK	Time	Numéro	OK	OK
7	1	5 000	Time	Numéro	OK	OK				

Tableau 3 – CRP Network_Status_Table pour DANC

Informations du nœud de rapport				Messages reçus ici sur l'adaptateur A				B ^a		Evaluation pour le nœud de rapport	
Node_Index et Node_Name	Adresses des adapta- teurs A, B	Nombre d'adap- tateurs	Inter- valle (ms)	A ^b	Envoyés par l'adaptateur B du nœud de rapport			A ^c	B ^d	Crossed_ cable_status	Adaptateur de transmission et adaptateur de réception sélectionnés
				Time	Sequence- Number du dernier message reçu	Diagnos- tic Frame reçu	Etat rapporté extrait du Diagnostic Frame pour BA				
1 FD001	addr1.A, addr1.B	2	2 000	...	Time	Numéro	OK	OK	...	OK	BB
2 FD002	addr2.A, addr2.B	2	2 000	...	Time	Numéro	OK	OK	...	OK	AA
3 LD001	addr3.A, addr3.B	2	1 000	...	Time	Numéro	OK	OK	...	OK	AA
4											
5 LD003	addr5.A, addr5.B	2	5 000	...	Time	Numéro	OK	OK	...	OK	AA
6	addr6.A, addr6.B	2	5 000	...	Time	Numéro	OK	OK	...	OK	BB
7	addr7.A	1	5 000	OK	N/A	N/A	N/A	N/A	NA	OK	AA

a Messages reçus ici sur l'adaptateur B.

b Envoyés par l'adaptateur A du nœud de rapport.

c Envoyés par l'adaptateur A du nœud de rapport.

d Envoyés par l'adaptateur B du nœud de rapport.

7.4 Durée de rétablissement CPR

7.4.1 Calcul de la durée de rétablissement

Le temps de rétablissement maximal d'une panne est:

$$t_{\text{rec}} = (1 + \text{Max_Sequence_Number_Difference}) \times t_{\text{dmi}} + t_{\text{path}} + t_{\text{proc}}$$

où

t_{rec} est la durée de rétablissement;

t_{dmi} est l'intervalle de temps entre les trames de diagnostic;

t_{path} est la latence de la livraison des trames du réseau; et

t_{proc} est le temps de traitement de l'entité de redondance réceptrice du réseau LAN.

La valeur de t_{path} est déterminée par la durée nécessaire à un paquet pour traverser le réseau. Dans un réseau commuté, la durée de transition maximale à travers un commutateur à base de FIFO dépend du nombre de ports du commutateur. Il peut être nécessaire d'utiliser QoS pour respecter ce délai. L'arrivée du paquet d'intérêt après tous les autres paquets destinés à l'interface de destination d'intérêt occasionne l'écoulement du délai maximal. Dans ce cas, le délai est:

$$t_{\text{sw}} = N_{\text{ports}} \times t_{\text{rate}} \times S_{\text{pak}} \times 8$$

où

t_{sw} est le délai dans un commutateur simple;

N_{ports} est le nombre de ports de commutation d'un commutateur simple;

t_{rate} est 1/débit de données; et

S_{pak} est la taille de paquet max. en octets.

EXEMPLE Ce qui suit constitue des exemples de durées de rétablissement pour diverses vitesses de nœuds terminaux.

La durée de traitement est dominée par le temps de réponse d'interruption du nœud terminal. Pour cet exemple, la durée d'interruption est fixée à 15 μs .

Avec: $t_{\text{dmi}} = 400 \text{ ms}$, $t_{\text{proc}} = 15 \mu\text{s}$, $\text{Max_Sequence_Number_Difference} = 1$, $N_{\text{ports}} = 24$ et $S_{\text{pak}} = 1\,522$ octets dans tous les cas.

Pour tous les nœuds terminaux d'une bande passante de 10 Mbit/s:

$$t_{\text{sw}} = 24 \times 10^{-7} \times 1\,522 \times 8 = 0,029 \text{ s}$$

Dans un réseau LAN simple redondant comprenant 6 commutateurs à 24 ports chacun, en supposant que le paquet de diagnostic traverse tous les commutateurs, le t_{path} total est $6 \times t_{\text{sw}} = 0,174 \text{ s}$.

Ainsi,

$$t_{\text{rec}} = 2 \times 0,40 + 0,174 + 0,000\,015 \text{ s}$$

Pour cet exemple, le temps de traitement maximal est négligeable, ainsi:

$$t_{\text{rec}} = 0,974 \text{ s}$$

Pour tous les nœuds terminaux d'une bande passante de 100 Mbit/s, l'équation est directement redimensionnée ainsi

$$t_{\text{sw}} = 24 \times 10^{-8} \times 1\,522 \times 8 = 0,002\,9 \text{ s and for 6 paths} = 0,014\,6 \text{ s}$$

Ainsi

$$t_{\text{rec}} = 2 \times 0,40 + 0,017\,4 + 0,000\,015$$

$$t_{\text{rec}} = 0,817\,4\,\text{s}$$

7.4.2 Durée maximale de réparation

Dans le cas de pannes telles que la rupture d'un câble, il n'y a pas de durée de réparation. Cependant, dans une topologie de commutation à interface multiple, la réparation d'une interface défectueuse nécessite le remplacement de tout le commutateur. Dans ce cas, la mise hors tension du commutateur pour son remplacement entraîne des interruptions de réseau supplémentaires dans les nœuds dont les chemins passent par ce commutateur. Au pire, la durée de réparation est alors identique à la durée de rétablissement d'une panne décrite en 7.4.1.

7.5 Messages multicast CRP

7.5.1 Envoi

Les messages multicast sont toujours envoyés à partir des deux ports (s'ils sont tous les deux opérationnels). Ils transportent comme adresse MAC source l'adresse du port via lequel ils sont envoyés.

Cela s'applique plus particulièrement aux DiagnosticFrames et AnnunciationFrames

7.5.2 Réception

Sur certaines topologies de réseau, un message multicast opérationnel simple peut être reçu sur chacun des ports d'un nœud. Si un nœud comporte deux ports, le nœud peut être configuré pour l'utilisation du Network_Status_Table afin de sélectionner un port de réception pour les messages opérationnels multicast et réduire ainsi sa charge de traitement d'interruptions et de messages. Il faut toujours détecter et supprimer les doublons.

7.6 Messages unicast CRP

7.6.1 Envoi d'une trame

Chaque trame unicast envoyée par un nœud participant à la redondance CRP est envoyée à partir d'un port seulement.

Lorsque la LRE reçoit une trame à partir de la pile IP (ou d'une autre couche supérieure), elle examine la trame, identifie l'adresse MAC de destination et contrôle cette adresse dans le Network_Status_Table.

Si le chemin A-A vers la destination est OK dans le tableau, la LRE envoie la trame au port A, qui insère son adresse comme adresse MAC source.

Si le chemin A-A est NOT OK dans le tableau, mais que le chemin A-B est OK, la LRE remplace l'adresse MAC B du nœud de destination dans la trame et envoie la trame au port A, qui insère son adresse comme adresse MAC source.

Si les chemins A-A et A-B sont tous les deux NOT OK, mais que le chemin B-A est OK, la LRE envoie la trame au port B, qui insère son adresse comme adresse MAC source.

Si les chemins A-A, A-B et B-A sont NOT OK, la LRE remplace l'adresse MAC B du nœud de destination dans la trame et envoie la trame au port B, qui insère son adresse comme adresse MAC source.

Si le message est à diffusion générale ou multicast, la LRE envoie la trame vers A lorsque A fonctionne et à B lorsque A ne fonctionne pas.

7.6.2 Réception d'une trame

Lorsque la LRE reçoit une trame de la couche physique via le port B, elle remplace l'adresse de destination MAC B en MAC A, avant de retransmettre la trame à la pile. Certaines piles IP sont sensibles à la bonne association IP/MAC. L'adresse IP n'est pas manipulée / remplacée de quelque manière que ce soit lors de la transmission ou de la réception.

7.7 Informations de redondance CRP

Chaque nœud est configuré par un mécanisme définissable par l'utilisateur. La configuration détermine les détails de la manière dont chaque nœud transmet des DiagnosticFrames et de la manière dont ils utilisent le Network_Status_Table pour sélectionner les ports de transmission et de réception. Ces informations peuvent être obtenues auprès d'un autre nœud en écoutant les AnnunciationFrames.

7.8 Statistiques de redondance CRP

Chaque nœud (même ceux qui ne sont pas activés CRP), peut collecter et afficher la santé des nœuds du réseau en souscrivant à l'adresse multicast utilisée pour les DiagnosticFrames. L'application peut ensuite générer un Network_Status_Table et l'utiliser de quelque manière que ce soit.

8 Protocole CRP

8.1 Nœud simple CRP

Les SANC doivent posséder un port et participer au protocole de redondance CRP.

8.2 Nœud double CRP

Les DANC doivent posséder deux ports et participer au protocole de redondance CRP.

8.3 Installation, configuration et réparation CRP

Les DANC doivent être connectés à un réseau LAN redondant simple à feuilles redondantes ou à un réseau LAN redondant sans feuilles redondantes, comme décrit dans l'Article 6.

NOTE 1 La première connexion offre quatre chemins possibles aux autres nœuds doubles connectés, alors que la dernière en offre seulement deux.

Afin d'obtenir une redondance de commutation et de feuille, chaque port d'un DANC doit être connecté à un commutateur différent.

Les SANC et SAN peuvent être connectés à n'importe quel LAN, mais il est préférable que tous les SANC et les SAN soient connectés au même réseau LAN.

Le Node_Index et le Node_Name affectés doivent être uniques sur le réseau.

Le Node_Index max. est 2 048; la valeur 0 ne doit pas être utilisée pour le Node_Index.

Le nombre max. de nœuds est 2 047.

NOTE 2 Ce nombre est limité par la longueur de la liste de statuts disponible dans le paquet de diagnostic.

Le nombre maximal de couches de commutation de réseau d'un réseau LAN redondant simple à feuilles redondantes doit être 3.

NOTE 3 Cette limite maintient un diamètre d'arborescence de 7 sauts pour les réseaux dans lesquels l'arborescence est utilisée pour empêcher la création de boucles.

8.4 Attributs du modèle LRE CRP

8.4.1 Spécifications des attributs

8.4.1.1 Protocol_Version

Cet attribut configuré précise le protocole CRP utilisé. Il s'agit d'un Unsigned8 d'une valeur de 0x01.

Les paquets aux numéros de version supérieurs doivent être rejetés par les versions inférieures. Les nouvelles versions doivent retourner à l'état du mode de compatibilité lorsque des paquets de versions plus anciens sont reçus.

8.4.1.2 Number_of_ports

Cet attribut configuré précise le nombre de ports du nœud, prévus pour assurer sa redondance (Unsigned8 = 1 ou 2).

8.4.1.3 Max_Sequence_Number_Difference

Cet attribut configuré précise la différence max. acceptable entre les paramètres de Sequence_Number dans une paire de DiagnosticFrames reçus à partir d'un nœud émetteur particulier. Unsigned8 doit être supérieur ou égal à 1.

NOTE Cet attribut affecte la vitesse et la précision de l'approche à double message. La valeur du nombre Max_Sequence_Number_Difference est 1 au minimum pour garantir que les pannes ne soient pas détectées par l'incrément normal du Sequence_Number. Un nombre au minimum égal à deux garantit qu'un seul message perdu n'entraîne pas la détection de pannes. Des nombres supérieurs assurent la tolérance de perte de plusieurs messages successifs mais ralentissent la vitesse à laquelle l'algorithme détecte les pannes réelles, agissant comme un compromis entre la tolérance transitoire et la vitesse de détection.

8.4.1.4 Redundancy_Flags

Cet attribut configuré précise cinq drapeaux qui ne sont pas transmis, indiquant un ou plusieurs des éléments suivants:

- a) SingleMulticastMessageTransmissionEnabled. Cet élément définit la politique de transmission de tous les services ayant des adresses de destination multicast, sauf du DiagnosticFrame.
 - False Transmet sur les deux ports
 - True Transmet sur un port
- b) CrossedCableDetectionEnabled.
 - False Ne détecte pas les câbles croisés
 - True Détecte les câbles croisés
- c) SinglePortMulticastMessageReceptionEnabled. Cet élément définit la politique de réception de toutes les trames multicast, sauf les DiagnosticFrame_Addresses des ports A et B.
 - False Réception des adresses multicast sur les deux ports
 - True Réception des adresses multicast sur un port sauf en cas de détection de panne
- d) DiagnosisUsingOwnMessagesEnabled.
 - False N'utilise pas ses propres DiagnosticFrames pour le diagnostic
 - True Utilise ses propres DiagnosticFrames pour le diagnostic
- e) LoadBalancingEnabled.
 - False Pas d'équilibrage de charge
 - True Équilibrage de charge

8.4.1.5 DiagnosticFrame_Interval

Cet attribut configuré précise l'intervalle de temps en millisecondes entre l'envoi successif des DiagnosticFrames en tant que Unsigned32.

NOTE Ce paramètre est configuré individuellement pour chaque dispositif terminal. Cela permet un ajustement précis des intervalles afin d'assurer la détection rapide des dispositifs terminaux critiques, tout en réduisant le trafic d'autres dispositifs terminaux.

8.4.1.6 Ageing time

Cet attribut configuré précise l'intervalle de temps en millisecondes, nécessaire à la LRE pour éliminer les nœuds silencieux de son Network_Status_Table.

NOTE 1 La configuration garantit que la valeur de cet attribut est supérieure à la valeur de l'attribut Max_Sequence_Number_Difference, multipliée par la valeur maximale de l'attribut DiagnosticFrame_Interval, indiquée dans les DiagnosticFrames reçus.

NOTE 2 De courts temps de vieillissement (minutes) signifient que les DANC apparaissent et disparaissent si le courant est coupé pendant un court instant. Des temps de vieillissement plus longs (jours) signifient que les DANC éliminés continuent d'apparaître dans les Network_Status_Tables.

8.4.1.7 DiagnosticFrame_Address

Cet attribut configuré précise l'adresse IP à 32 bits des DiagnosticFrames. L'adresse peut être une adresse IP à diffusion générale ou multicast.

L'adresse 224.0.0.105 a été enregistrée dans cet objectif.

8.4.1.8 DiagnosticFrame_UDP_source_port

Cet attribut configuré précise le port source UDP à 16 bits utilisé pour les DiagnosticFrames.

Il ne faut pas utiliser le même numéro de port que pour les AnnunciationFrames.

8.4.1.9 DiagnosticFrame_UDP_destination_port

Cet attribut configuré précise le port de destination UDP à 16 bits utilisé pour les DiagnosticFrames.

Il ne faut pas utiliser le même numéro de port que pour les AnnunciationFrames.

8.4.1.10 Annunciation_UPD_port

Cet attribut fixe précise le port source et le port de destination UDP à 16 bits utilisé pour les AnnunciationFrames comme un Unsigned16 d'une valeur de 1 098.

8.4.1.11 Node_Index

Cet attribut configuré précise le Node_Index à 16 bits de ce nœud.

NOTE Chaque nœud se trouvant dans le champ de la DiagnosticFrame_Address possède un Node_Index unique.

8.4.1.12 Max_Node_Index

Cet attribut configuré précise le Node_Index max. attendu.

NOTE Ce nombre est utilisé pour déterminer la longueur de la liste de statuts de l'adaptateur et de la liste des câbles croisés dans le DiagnosticFrame, ainsi que la longueur du Network_Status_Table de chaque dispositif terminal du réseau. La valeur de ce paramètre affecte la taille des DiagnosticFrames; c'est pourquoi, un très grand nombre influence négativement la performance.

Il est recommandé de régler le Max_Node_Index sur la même valeur pour tous les dispositifs du réseau.

8.4.1.13 Node_Name

Cet attribut configuré est une VisibleString de 32 octets précisant un Node_Name unique pour chaque nœud se trouvant dans le champ de la DiagnosticFrame_Address. Les octets non utilisés de ce champ doivent être transmis sous forme de caractères d'espacement ASCII.

8.4.1.14 Annunciation_Interval

Cet attribut configuré précise l'intervalle de temps auquel les AnnunciationFrames sont envoyées.

8.4.1.15 Operational_IP_Address

Cet attribut configuré précise l'adresse IP utilisée pour la communication de l'application.

8.4.1.16 Duplicate_Detection_State

Cet attribut dynamique indique la possible détection d'adresses multiples.

Il doit être réinitialisé à 0 partout lors de la configuration ou du démarrage et réglé pour la détection de situations de réseaux conflictuelles.

Il s'agit d'un jeu de bits, codé comme suit:

0	1	2	3	4	5	6	7
RES						DND	DID

Bit 0 — 5: Réservés

définis à 0

Bit 1: DND

1: nom dupliqué détecté,

Bit 0: DID

1: index de nœud dupliqué détecté,

8.4.1.17 LRE state

Cet attribut dynamique précise l'état de la LRE sous la forme d'un octet.

0	1	2	3	4	5	6	7
CONF						SYN	

Bit 0 — 6: CONF

0 = réservé

1 = aucun nom configuré

2 = opérationnel

3 – 127 = réservés

Bit 7: SYN

0 = Non synchronisé avec le serveur temporel

1 = Synchronisé avec le serveur temporel

L'état de la LRE doit être réinitialisé à "0" partout lors de la configuration ou du démarrage.

8.4.1.18 Sequence_Number

Cet attribut dynamique est un nombre entier croissant de 32 bits commençant à 0 pour le premier DiagnosticFrame envoyé après le démarrage et augmentant de 1 en 1, avant de revenir à 0.

8.4.1.19 Path_Status

Cet attribut dynamique résume les conclusions du nœud sur ses chemins. Il est constitué de quatre Path_Status réglés, comme indiqué dans le Tableau 4.

Tableau 4 – CRP Path_Status_Sets

	Nœud à distance d'envoi	Nœud de réception
Path_Status_A_to_A	A	A
Path_Status_B_to_A	B	A
Path_Status_A_to_B	A	B
Path_Status_B_to_B	B	B

Chaque jeu de Path_Status est constitué d'une séquence de bits alignée de 32 bits, chaque bit représentant un nœud, utilisant le Node_Index comme décalage et indiquant le statut du chemin de transmission à partir du nœud de rapport jusqu'à ce nœud.

Les valeurs suivantes sont utilisées pour chaque bit:

- 0 = DiagnosticFrames reçues correctement
- 1 = DiagnosticFrames non reçues

EXEMPLE Le Tableau 5 présente un jeu de Path_Status pour le nœud au Node_Index 4. Ce nœud (4) indique qu'il voit:

Nœud 1: a reçu les messages "A" via son LAN_A et les messages "B" via son LAN_B.

Nœud 2: n'a pas reçu de message sur une période supérieure à l'Aging_Time.

Nœud 3: a reçu les messages "A" uniquement via son LAN_A (il peut s'agir d'un SAN).

Nœud 4: a reçu ses propres messages via leur port d'envoi.

Nœud 5: a reçu les messages "A" via son LAN_A et les messages "B" via son LAN_A – erreur de configuration possible.

Nœud 6: a reçu les messages "A" via son LAN_B et les messages "B" via son LAN_A – erreur de croisement de câbles possible.

Tableau 5 – Exemple de CRP d'un Path_Status_Set

	0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
Path_Status_A_to_A																
	0	1	0	1	1	1	0	0	0	0	0	0	0	0	0	0
	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Path_Status_B_to_A																
	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Path_Status_A_to_B																
	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Path_Status_B_to_B																
	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0
	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

8.4.1.20 Configuration_Version

Cet attribut précise la version de cet objet comme Unsigned16. Chaque fois que la valeur de l'un de ses autres attributs change lors de la configuration, le numéro de version doit être incrémenté de 1. Le numéro de version 0 indique que cet objet n'a pas été configuré. Cette valeur doit être sautée à chaque nouveau cycle de configuration.

8.4.2 Impact des attributs de configuration des LRE

L'impact des attributs configurés des LRE est résumé dans le Tableau 6.

Tableau 6 – Impact des attributs de configuration CRP sur le fonctionnement LAN

Paramètre de configuration	LAN double	LAN simple
Node_Index	Identique pour les deux, voir 8.4.1.11	
Max_Node_Index	Identique pour les deux, voir 8.4.1.12	
Max_Sequence_Number_Difference	Identique pour les deux, voir 8.4.1.3	
DiagnosticFrame_UDP_destination_port	Identique pour les deux, voir 8.4.1.9	
Redundancy_Flags	Ce paramètre est constitué des cinq drapeaux suivants	
SingleMulticastMessageTransmissionEnabled	Généralement réglé sur False, permettant aux messages multicast d'être envoyés sur les deux LAN, si les conditions d'erreur et la présence de SANC le garantit. Cependant, lorsque le chargement du nœud de réception est critique, il peut être réglé sur True	Généralement réglé sur True, permettant aux messages multicast d'être propagés aux deux adaptateurs d'autres nœuds. L'envoi sur les deux adaptateurs augmente le trafic sur le LAN et les nœuds récepteurs
CrossedCableDetectionEnabled	Généralement réglé sur True. Il permet la détection de câbles croisés	Généralement réglé sur False. Les câbles croisés ne sont pas problématiques dans un LAN simple

Paramètre de configuration	LAN double	LAN simple
SingleMulticastMessageReceptionEnabled	Généralement réglé sur False, permettant la réception de multicasts sur l'un ou l'autre des adaptateurs. Dans la mesure où chaque nœud multicast peut choisir sur quel adaptateur émettre, l'écoute des deux adaptateurs est essentielle pour les entendre	Généralement réglé sur False, permettant aux messages multicast d'exploitation d'être propagés aux deux adaptateurs d'autres nœuds. L'écoute des deux adaptateurs augmente le trafic sur le nœud récepteur
DiagnosisUsingOwnMessagesEnabled	Généralement réglé sur False, empêchant les DiagnosticFrames envoyés à un adaptateur d'être entendus sur l'autre adaptateur	Généralement réglé sur True, autorisant les DiagnosticFrames envoyés à partir d'un adaptateur à être reçus sur l'autre. Cette méthode de diagnostic améliore la détection des pannes, tout en augmentant la charge du processeur
LoadBalancingEnabled	Peut être réglé sur False temporairement pour faciliter la maintenance	Généralement réglé sur False. L'équilibrage de charge n'est pas applicable aux réseaux LAN simples
DiagnosticFrame_Interval	Identique pour les deux, voir 8.4.1.5	
Aging_Time	Identique pour les deux, voir 8.4.1.6	
Adresse d'envoi de l'adaptateur de DiagnosticFrame A	L'adresse à laquelle les DiagnosticFrames sont envoyées sur les adaptateurs A et B. Généralement, la même adresse est utilisée pour les deux adaptateurs	Les adresses auxquelles les DiagnosticFrames sont envoyées sur les adaptateurs A et B. La même adresse peut être utilisée pour maximiser la capacité de détection et de rétablissement en cas de pannes. Cela augmentera la charge du processeur. Différentes adresses permettent une réduction du trafic considéré par le nœud récepteur
Adresse d'envoi de l'adaptateur de DiagnosticFrame B		
Adresse de réception de l'adaptateur de DiagnosticFrame A	L'adresse sur laquelle les DiagnosticFrames sont reçues sur les adaptateurs A et B. Généralement, la même adresse est utilisée pour les deux adaptateurs	Les adresses sur lesquelles les DiagnosticFrames sont reçues sur les adaptateurs A et B. La même adresse peut être utilisée pour maximiser la capacité de détection et de rétablissement en cas de pannes. Cela augmentera la charge du processeur

8.5 Codage CRP de DiagnosticFrame

Le contenu d'un DiagnosticFrame doit être décrit dans le Tableau 7.

Tableau 7 – Format des DiagnosticFrames CRP

Nom de paramètre	Décalage	Type de données	Taille	Description
En-tête Ethernet DLL				
Préambule	0		8	Alternance de 1 et de 0
Adresse de destination	8		6	Adresse MAC à diffusion générale, multicast
Adresse source	14		6	Adresse MAC source unicast de l'adaptateur utilisé pour l'envoi du message
Type	20		2	0x800 pour datagrammes IP
En-tête IP				
Version IP	22		4	Version IP (champ à 4 bits) = 4
Longueur de l'en-tête IP				La longueur de l'en-tête Internet (champ à 4 bits) est la longueur de l'en-tête Internet en mots de 32 bits = 6
Type de service IP				Type de service (champ à 8 bits) – régler tous les champs = 0 Bits 0-2: précedence. Bit 3: 0 = délai normal, 1 = faible délai. Bits 4: 0 = débit normal, 1 = débit élevé. Bits 5: 0 = fiabilité normale, 1 = fiabilité élevée. Bit 6-7: réservé pour un usage ultérieur.
Longueur totale IP				Longueur du champ IP (champ à 16 bits) en octets, y compris en-tête IP et données = 346
Identifiant IP	26		4	Identifiant pour paquets fragmentés. Réglage = 0
Drapeaux IP				Drapeaux (champ à 3 bits) Bit 0: réservé, doit avoir pour valeur "zéro" Bit 1: ne pas fragmenter = 1 Bit 2: 0 = dernier fragment
Décalage de fragment IP				Position dans le datagramme original. Premier fragment = 0
Durée de vie IP	30	Unsigned8	4	Défini sur 1
Protocole IP		Unsigned8		Datagramme utilisateur = 17 (décimal)
Somme de contrôle de l'en-tête IP				16 bits. Le champ de la somme de contrôle est le complément à un sur 16 bits de la somme du complément à un de tous les termes de 16 bits de l'en-tête. Pour les besoins de calcul de la somme de contrôle, la valeur du champ de la somme de contrôle est zéro
Adresse IP source	34		4	Source_IP_Address.
Adresse IP de destination	38		4	DiagnosticFrame_Address configurée, voir 8.4.1.7
Options IP	42		1	
IP pad	43		3	En-tête Pad sur une frontière de 32 bits. Réglage Pad = 0
En-tête UDP				
Port source UDP	46		2	Voir 8.4.1.8
Port de destination UDP	48		2	Voir 8.4.1.9
Longueur UDP	50		2	Longueur du champ UDP
Somme de contrôle UDP	52		2	La somme de contrôle est le complément à un sur 16 bits de la somme du complément à un d'un pseudo en-tête d'informations de l'en-tête IP, de l'en-tête UDP et des données
En-tête CRP				
CRP Protocol_Version	54	Unsigned8	1	Voir 8.4.1.1
réservé	58	Unsigned24	3	Défini sur 0x801001
Adresse auxiliaire CRP	58	Unsigned32	4	Non utilisé – défini sur 0
Longueur de message CRP	62	Unsigned32	4	Précise le nombre d'octets contenus dans le message entier, démarre immédiatement après l'en-tête UDP, jusqu'à la fin du message
Corps CRP				
CRP Node_Index	66	Unsigned16	2	Voir 8.4.1.10
CRP Number_of_ports	68	Unsigned8	1	Voir 8.4.1.2
Adaptateur de transmission	69	Unsigned8	1	Port utilisé pour transmettre ce DiagnosticFrame. 0 = adaptateur A 1 = adaptateur B
CRP	70	Unsigned 32	4	Voir 8.4.1.5

Nom de paramètre	Décalage	Type de données	Taille	Description
DiagnosticFrame_Interval				
CRP Node_Name	74	VisibleString	32	Voir 8.4.1.13
Réservé	106	Unsigned8	1	Réservé, défini à zéro
CRP Duplicate_Detection_State	107	Unsigned8	1	Voir 8.4.1.16
Number_Of_Adapter_Statuses	108	Unsigned16	2	Nombre d'entrées Unsigned32 dans le Path_Status.
Path_Status_A_to_A	110	liste de Unsigned32	Voir ^a	Voir Tableau 4
Path_Status_B_to_A	Voir a)	liste de Unsigned32	Voir ^a	Voir Tableau 4
Path_Status_A_to_B	Voir a)	liste de Unsigned32	Voir ^a	Voir Tableau 4
Path_Status_B_to_B	Voir a)	liste de Unsigned32	Voir ^a	Voir Tableau 4
Sequence_Number	Voir a)	Unsigned32	4	Voir 8.4.1.18
Extension en option	Voir a)	OctetString	8	Réservé
Queue de bande Ethernet DLL				
FCS	Voir a)		4	Séquence de contrôle de trame basée CRC
^a La taille et le décalage du champ dépendent du nombre de statuts d'adaptateur, la taille de chaque champ Path_Status est 4 x le nombre de statuts d'adaptateur, le décalage est incrémenté par la taille du champ précédent.				

8.6 Codage CRP d'AnnunciationFrame

Le format d'un AnnunciationFrame doit être présenté dans le Tableau 8.

Tableau 8 – CRP AnnunciationFrame

Nom de paramètre	Décalage	Type de données	Longueur en octets	Description
Préambule	0		8	Alternance de 1 et de 0
Destination_Addresses	8		6	Adresse MAC à diffusion générale, multicast
Source_Address	14		6	Adresse MAC source unicast de l'adaptateur utilisé pour l'envoi du message
EtherType	20		2	0x800 pour datagrammes IP
En-tête IP				
Version IP	0		4	Version IP (champ à 4 bits) = 4
Longueur de l'en-tête IP				La longueur de l'en-tête Internet (champ à 4 bits) est la longueur de l'en-tête Internet en mots de 32 bits = 6
Service IP				Service (champ à 8 bits) – régler tous les champs = 0 Bits 0-2: précedence. Bit 3: 0 = délai normal, 1 = faible délai. Bits 4: 0 = débit normal, 1 = débit élevé. Bits 5: 0 = fiabilité normale, 1 = fiabilité élevée. Bit 6-7: réservé pour un usage ultérieur.
Longueur totale IP				Longueur du champ IP (16 bits) en octets, y compris en-tête IP et données
Identifiant IP	4		4	Identifiant pour paquets fragmentés. Réglage = 0

Nom de paramètre	Décalage	Type de données	Longueur en octets	Description
Drapeaux IP				Drapeaux (champ à 3 bits) Bit 0: réservé, défini sur 0 Bit 1: ne pas fragmenter = 1 Bit 2: 0 = dernier fragment
Décalage de fragment IP				Position dans le datagramme original. Premier fragment = 0
Durée de vie IP	8		4	8 bits. Défini sur 1
Protocole IP				8 bits. Datagramme utilisateur = 17 (décimal)
Somme de contrôle de l'en-tête IP				16 bits. Le champ de la somme de contrôle est le complément à un sur 16 bits de la somme du complément à un de tous les termes de 16 bits de l'en-tête. Pour les besoins de calcul de la somme de contrôle, la valeur du champ de la somme de contrôle est zéro.
Adresse IP source	12		4	Adresse IP source de ce nœud
Adresse IP de destination	16		4	voir 8.4.1.7.
Options IP	20		1	Champ d'option IP
IP pad	21		3	En-tête Pad sur une frontière de 32 bits. Réglage Pad = 0
En-tête UDP				
Port source UDP	0		2	Port d'annonce, voir 8.4.1.8
Port de destination UDP	2		2	Port d'annonce voir 8.4.1.9
Longueur UDP	4		2	Longueur du champ UDP
Somme de contrôle UDP	6		2	La somme de contrôle est le complément à un sur 16 bits de la somme du complément à un d'un pseudo en-tête d'informations de l'en-tête IP, de l'en-tête UDP et des données
Corps				
CRP LRE_State	0	Unsigned8	1	
CRP Reserved0	1	Unsigned8	1	Réservé
CRP Reserved1	2	Unsigned8	1	Réservé
CRP Duplicate_Detection_State	3	Unsigned8	1	voir 8.4.1.16
CRP Node_Index	4	Unsigned16	2	voir 8.4.1.11
CRP Max_Node_Index	6	Unsigned16	2	voir 8.4.1.12
CRP Operational_IP_Addresses	8	OctetString	16	voir 8.4.1.15
CRP ReservedString	24	VisibleString	32	Réservé
CRP Node_Name	56	VisibleString	32	voir 8.4.1.13.
CRP Annunciation_Interval	88	Unsigned32	4	voir 8.4.1.14
CRP DiagnosticFrame_UDP_Port	92	Unsigned16	2	voir 8.4.1.8 et 8.4.1.9
CRP Reserved	94	Unsigned16	2	Réservé, défini sur 0.

Nom de paramètre	Décalage	Type de données	Longueur en octets	Description
CRP Configuration_Version	96	Unsigned32	4	Voir 8.4.1.1
CRP User_Option	100	Unsigned32	4	Réservé
CRP Number_Of_Entries	104	Unsigned32	4	indique le nombre d'entrées définies par l'utilisateur
Entrées CRP	108	Unsigned32	4 x nombre d'entrées	Réservé pour les entrées définies par l'utilisateur
Queue de bande Ethernet DLL				
FCS	0		4	Séquence de contrôle de trame basée CRC

8.7 Protocole commun CRP

8.7.1 AnnunciationFrames

8.7.1.1 Envoi

Un nœud doit envoyer un AnnunciationFrame au format indiqué dans le Tableau 8:

- après le premier démarrage ou un redémarrage à chaud;
- après la configuration des paramètres de nœud;
- périodiquement, à un taux déterminé par l'Annunciation_Interval.

Un SANC doit envoyer l'AnnunciationFrame via son port A.

Un DANC doit envoyer l'AnnunciationFrame via ses ports A et B.

8.7.1.2 Réception

Le nœud récepteur doit inclure le nœud envoyant l'AnnunciationFrame au Network_Status_Table.

8.7.2 DiagnosticFrames

8.7.2.1 Envoi

Les nœuds doivent transmettre les DiagnosticFrames au format spécifié dans le Tableau 7:

- au démarrage ou redémarrage à chaud, si le nœud est configuré ;
- après une configuration réussie du nœud;
- autrement, à un taux spécifié par l'attribut DiagnosticFrame_Interval (8.4.1.5);
- aussi longtemps que le nœud est opérationnel.

Un SANC doit envoyer un DiagnosticFrame via son port A, avec:

- la valeur du champ du nombre de ports réglée sur 1;
- le Sequence_Number incrémenté de 1 pour chaque message successif envoyé;
- l'adaptateur émetteur réglé sur "1" (LAN_A).

Un DANC doit envoyer une paire de DiagnosticFrames via ses ports A et B, avec:

- la valeur du champ du nombre de ports réglée sur 2;
- le Sequence_Number incrémenté de 1 pour chaque envoi successif d'une paire et des champs de Sequence_Numbers dans les deux messages d'une paire;
- le réglage des adresses MAC associées;