

High availability automation networks

ICS 25.040.40; 35.040; 35.110

National foreword

This British Standard is the UK implementation of EN 62439:2008. It is identical to IEC 62439:2008.

The UK participation in its preparation was entrusted to Technical Committee AMT/7, Industrial communications: process measurement and control, including fieldbus.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 September 2008

© BSI 2008

ISBN 978 0 580 62071 3

Amendments/corrigenda issued since publication

Date	Comments

**High availability automation networks
(IEC 62439:2008)**

Réseaux d'automatismes
à haute disponibilité
(CEI 62439:2008)

Hochverfügbare
Automatisierungsnetze
(IEC 62439:2008)

This European Standard was approved by CENELEC on 2008-06-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Central Secretariat: rue de Stassart 35, B - 1050 Brussels

Foreword

The text of document 65C/495/FDIS, future edition 1 of IEC 62439, prepared by SC 65C, Industrial networks, of IEC TC 65, Industrial-process measurement, control and automation, was submitted to the IEC-CENELEC parallel vote and was approved by CENELEC as EN 62439 on 2008-06-01.

The following dates were fixed:

- latest date by which the EN has to be implemented
at national level by publication of an identical
national standard or by endorsement (dop) 2009-03-01
- latest date by which the national standards conflicting
with the EN have to be withdrawn (dow) 2011-06-01

The International Electrotechnical Commission (IEC) and CENELEC draw attention to the fact that it is claimed that compliance with this document may involve the use of the following patents:

- Clause 5 (MRP) may involve Patent WO 99/046908 A1 “Local network, especially Ethernet network, with redundancy properties and redundancy manager”, owned by Siemens AG A&D, Gleiwitzerstr. 555, Nürnberg 90475 Germany and Hirschmann Automation and Control GmbH, Stuttgarter Strasse 45-51, Neckartenzlingen 72654, Germany;
- Clause 6 (PRP) may involve Patent WO06053459 “Reception of redundant and non-redundant frames”, owned by ABB Switzerland Ltd, Corporate Research, Segelhofstr 1K, 5405 Baden, Switzerland;
- Clause 7 (CRP) may involve Patent U.S. 6,826,590 „Block Oriented Control System on High Speed Ethernet“, owned by the Fieldbus Foundation, 9005 Mountain Ridge Drive – Bowie Bldg, Suite190, Austin, TX 78759, USA;
- Clause 8 (BRP) may involve Patent Application Serial No. US 11/520,192, "Multiple fault-tolerant Ethernet redundancy", owned by Rockwell Automation Technologies, Inc., 1 Allen-Bradley Drive, Mayfield Heights, Ohio, USA.

The IEC and CENELEC take 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 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 the IEC.

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 and CENELEC shall not be held responsible for identifying any or all such patent rights.

Annex ZA has been added by CENELEC.

Endorsement notice

The text of the International Standard IEC 62439:2008 was approved by CENELEC as a European Standard without any modification.

CONTENTS

INTRODUCTION.....	9
1 Scope.....	10
2 Normative references	10
3 Terms, definitions, abbreviated terms, acronyms, and conventions.....	11
3.1 Terms and definitions	11
3.2 Abbreviated terms and acronyms	18
3.3 Conventions	20
3.3.1 General conventions.....	20
3.3.2 Conventions for state machine definitions.....	20
3.3.3 Conventions for PDU specification.....	20
3.4 Reserved network addresses	20
4 Concepts for high availability automation networks.....	21
4.1 Characteristics of application of automation networks.....	21
4.1.1 Resilience in case of failure.....	21
4.1.2 Classes of network redundancy	22
4.1.3 Redundancy maintenance	22
4.1.4 Comparison and indicators	22
4.2 Generic network system	24
4.2.1 Network elements.....	24
4.2.2 Topologies.....	25
4.2.3 Redundancy handling	31
4.2.4 Network recovery time	31
4.2.5 Diagnosis coverage	31
4.2.6 Failures	31
4.3 Safety	33
4.4 Security.....	33
4.5 Conformance.....	33
4.5.1 Conformance to redundancy protocols.....	33
4.5.2 Conformance tests	33
5 MRP – Media Redundancy Protocol based on a ring topology	36
5.1 MRP Overview	36
5.2 MRP Media redundancy behaviour	37
5.2.1 Ring ports.....	37
5.2.2 Media Redundancy Manager (MRM).....	38
5.2.3 Media Redundancy Client (MRC).....	39
5.2.4 Redundancy domain	39
5.2.5 Usage with diagnosis and alarms.....	39
5.2.6 Ring diagnosis.....	40
5.2.7 Multiple MRM in a single ring.....	40
5.2.8 BLOCKED not supported (option)	40
5.3 MRP Class specification	41
5.3.1 General	41
5.3.2 Template	41
5.3.3 Attributes.....	41
5.4 MRP Service specification	44

5.4.1	Start MRM	44
5.4.2	Stop MRM	45
5.4.3	State Change	46
5.4.4	Start MRC	47
5.4.5	Stop MRC	48
5.4.6	Read MRM	49
5.4.7	Read MRC	51
5.5	MRP Protocol specification	52
5.5.1	PDU description	52
5.5.2	Protocol machines	58
5.6	MRP Installation, configuration and repair	78
5.6.1	Ring port parameters	78
5.6.2	Ring topology parameters	79
5.6.3	MRM and MRC parameters	79
5.6.4	Configuration	80
6	PRP – Parallel Redundancy Protocol	80
6.1	PRP Principle of operation	80
6.1.1	Single points of failure	82
6.1.2	Node structure	82
6.1.3	Compatibility between singly and doubly attached nodes	83
6.1.4	Network management	83
6.1.5	Transition to non-redundant networks	83
6.1.6	Duplicate handling	84
6.1.7	Configuration check	89
6.1.8	Network supervision	89
6.1.9	Redundancy management interface	89
6.2	PRP protocol specifications	90
6.2.1	Installation, configuration and repair guidelines	90
6.2.2	MAC addresses	90
6.2.3	Multicast MAC addresses	90
6.2.4	IP addresses	90
6.2.5	Nodes	91
6.2.6	Duplicate accept mode	91
6.2.7	Duplicate discard mode	91
6.3	PRP service specification	97
6.3.1	Arguments	97
6.3.2	NodesTable	98
6.3.3	PRP Write	99
6.3.4	PRP Read	100
6.4	PRP Management Information Base	101
6.5	PRP Protocol Implementation Conformance Statement (PICS)	102
7	CRP – Cross-network Redundancy Protocol	102
7.1	CRP Overview	102
7.2	CRP Nodes	102
7.3	CRP LAN topology	102
7.4	CRP Key components	104
7.4.1	CRP General protocol operation	104
7.4.2	CRP Statistics	105
7.4.3	CRP Network_Status_Table	106

7.4.4	CRP Recovery time	109
7.4.5	CRP Multicast messages	110
7.4.6	CRP Unicast messages	110
7.4.7	CRP Redundancy information	111
7.4.8	CRP Redundancy statistics	111
7.5	CRP Protocol	111
7.5.1	CRP Singly attached node	111
7.5.2	CRP Doubly attached node	111
7.5.3	CRP Installation, configuration and repair	111
7.5.4	CRP LRE model attributes	111
7.5.5	CRP Encoding of the DiagnosticFrame	117
7.5.6	CRP Encoding of the AnnunciationFrame	118
7.5.7	CRP Common protocol	120
7.5.8	CRP Operational messages	122
7.5.9	CRP services	125
8	BRP – Beacon redundancy protocol	132
8.1	BRP Overview	132
8.2	BRP Principle of operation	132
8.2.1	General	132
8.2.2	Network topology	132
8.2.3	Network components	134
8.2.4	Rapid reconfiguration of network traffic	135
8.3	BRP stack and fault detection features	135
8.4	BRP Protocol specification	137
8.4.1	MAC addresses	137
8.4.2	EtherType	137
8.4.3	Fault detection mechanisms	137
8.4.4	End node state diagram	137
8.4.5	Beacon end node state diagram	144
8.5	BRP Message structure	151
8.5.1	General	151
8.5.2	IEEE 802.3 tagged frame header	151
8.5.3	Beacon message	151
8.5.4	Learning_Update message	152
8.5.5	Failure_Notify message	152
8.5.6	Path_Check_Request message	152
8.5.7	Path_Check_Response message	153
8.6	BRP Fault recovery time	153
8.7	BRP Service definition	154
8.7.1	Supported services	154
8.7.2	Common service parameters	154
8.7.3	Set node parameters service	154
8.7.4	Get node parameters service	156
8.7.5	Add node receive parameters service	158
8.7.6	Remove node receive parameters service	159
8.7.7	Get node status service	160
Annex A (informative)	Classification of networks	162
Annex B (informative)	Availability calculations	164
Annex C (normative)	Network management information base	173

Annex D (informative) PRP algorithm as pseudo-code	196
Annex ZA (normative) Normative references to international publications with their corresponding European publications	200
Bibliography.....	199
Figure 1 – General network elements (tree topology)	24
Figure 2 – Example of tree topology.....	26
Figure 3 – Example of linear topology	27
Figure 4 – Example of ring topology	27
Figure 5 – Example of a partially meshed topology	28
Figure 6 – Example of fully meshed topology	29
Figure 7 – Single LAN structure without redundant leaf links.....	29
Figure 8 – Single LAN structure with redundant leaf links.....	30
Figure 9 – Redundant LAN structure without redundant leaf links	30
Figure 10 – Redundant LAN structure with redundant leaf links	30
Figure 11 – Conformance test overview	34
Figure 12 – MRP Stack	37
Figure 13 – MRP Ring topology with one manager and clients	38
Figure 14 – MRP MRM in an open ring	38
Figure 15 – MRP Ring with more than one MRM.....	40
Figure 16 – MRP Protocol machine for MRM.....	59
Figure 17 – MRP Protocol machine for MRC.....	69
Figure 18 – PRP General redundant network example	80
Figure 19 – PRP Redundant network example as two LANs (bus topology).....	81
Figure 20 – PRP Redundant ring example with SANs and DANPs.	81
Figure 21 – PRP Single Ring with DANPs in SRP mode.....	82
Figure 22 – PRP Two DANPs communicating	82
Figure 23 – PRP Redundancy Box, transition from single to double LAN.	84
Figure 24 – PRP Frame extended by an RCT.....	85
Figure 25 – PRP Tagged frame extended by an RCT	86
Figure 26 – PRP Constructed, padded frame closed by an RCT.....	86
Figure 27 – PRP Drop window on LAN_A.....	87
Figure 28 – PRP Drop window reduction after a discard.....	88
Figure 29 – PRP Frame from LAN_B was not discarded.	88
Figure 30 – PRP Synchronized LANs.....	88
Figure 31 – CRP Stack architecture	102
Figure 32 – CRP Single LAN topography	103
Figure 33 – CRP Double LAN topology	103
Figure 34 – CRP DiagnosticFrame pair approach.....	104
Figure 35 – CRP Example system.....	105
Figure 36 – BRP Star network example.....	132
Figure 37 – BRP Linear network example	133
Figure 38 – BRP Ring network example	134
Figure 39 – BRP Stack architecture	135
Figure 40 – BRP State diagram of end node	138

Figure 41 – BRP State diagram for beacon end node.....	145
Figure B.1 – General symmetrical fault model.....	165
Figure B.2 – Simplified fault model	166
Figure B.3 – Asymmetric fault model.....	167
Figure B.4 – Network with no redundancy	168
Figure B.5 – Network with no single point of failure.....	169
Figure B.6 – Network with resiliency to second failure.....	171
Table 1 – Examples of application grace time	21
Table 2 – Examples of redundancy protocols	23
Table 3 – MRP Start MRM	44
Table 4 – MRP Stop MRM.....	46
Table 5 – MRP Change State.....	46
Table 6 – MRP Start MRC.....	47
Table 7 – MRP Stop MRC	48
Table 8 – MRP Read MRM	49
Table 9 – MRP Read MRC.....	51
Table 10 – MRP IEEE 802.3 DLPDU syntax.....	53
Table 11 – MRP OUI.....	53
Table 12 – MRP MulticastMACAddress	54
Table 13 – MRP TagControlInformation.Priority field.....	54
Table 14 – MRP LT field	54
Table 15 – MRP APDU syntax	55
Table 16 – MRP Substitutions.....	55
Table 17 – MRP_TLVHeader.Type.....	55
Table 18 – MRP_Version	56
Table 19 – MRP_Prio.....	56
Table 20 – MRP_PortRole	56
Table 21 – MRP_RingState.....	57
Table 22 – MRP_Interval	57
Table 23 – MRP_Transition.....	57
Table 24 – MRP_TimeStamp	57
Table 25 – MRP_Blocked.....	58
Table 26 – MRP_DomainUUID.....	58
Table 27 – MRP Local variables of MRM protocol machine	60
Table 28 – MRM State machine	61
Table 29 – MRP Local variables of MRC protocol machine	70
Table 30 – MRC State machine	70
Table 31 – MRP Functions.....	75
Table 32 – MRP FDB Clear Timer.....	78
Table 33 – MRP Topology Change Timer.....	78
Table 34 – MRP Network/Connection parameters	79
Table 35 – MRP MRM parameters	79

Table 36 – MRP MRC parameters.....	79
Table 37 – PRP_Supervision frame with VLAN tagging.....	95
Table 38 – PRP Constants.....	97
Table 39 – PRP Arguments.....	98
Table 40 – PRP Arguments.....	99
Table 41 – PRP Write	100
Table 42 – PRP Read	101
Table 43 – CRP Example Network_Status_Table for node 3	105
Table 44 – CRP Network_Status_Table for singly connected nodes.....	107
Table 45 – CRP Network_Status_Table for DANC	108
Table 46 – CRP Path_Status_Sets	115
Table 47 – CRP Example of a Path_Status_Set.....	115
Table 48 – CRP Configuration attributes impact on LAN operation.....	116
Table 49 – CRP DiagnosticFrame format	117
Table 50 – CRP AnnunciationFrame	118
Table 51 – CRP Unicast destination address handling	123
Table 52 – CRP Configuration Parameters.....	124
Table 53 – CRP Set assignment info service parameters	125
Table 54 – CRP Get redundancy info service.....	127
Table 55 – CRP Put redundancy info service	129
Table 56 – CRP Get statistics service	130
Table 57 – BRP End node flags	139
Table 58 – BRP End node state transition table	140
Table 59 – BRP Beacon end node flags.....	146
Table 60 – BRP Beacon end node state transition table.....	147
Table 61 – BRP Common Header with IEEE 802.3 tagged frame format	151
Table 62 – BRP Beacon message format.....	152
Table 63 – BRP Learning_Update message format	152
Table 64 – BRP Failure_Notify message format	152
Table 65 – BRP Path_Check_Request message format	152
Table 66 – BRP Path_Check_Response message format	153
Table 67 – BRP Set Node Parameters service parameters.....	155
Table 68 – BRP Get Node Parameters service parameters	156
Table 69 – BRP Add Node Receive Parameters service parameters	158
Table 70 – BRP Remove Node Receive Parameters service parameters.....	159
Table 71 – BRP Get Node Status service parameters	160
Table A.1 – Code assignment for the <TYPE> field.....	162
Table A.2 – Code assignment for the <PLCYleaf> field	162
Table A.3 – Code assignment for the <TPLGY> field	162
Table A.4 – Code assignment for the <ITYPE> field.....	163

INTRODUCTION

This International Standard specifies relevant principles for high availability networks that meet the requirements for industrial automation networks.

In the fault-free state of the network, this International Standard provides ISO/IEC 8802-3 compatible, reliable data communication, and preserves determinism of real-time data communication. In cases of fault, removal, and insertion of a component, it provides deterministic recovery times.

The typical Ethernet communication capabilities as used in the office world are fully retained, 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 Clause 4 and specified in the clauses following it. Clause 4 also distinguishes between the different solutions, giving guidance to the user.

This International Standard follows the general structure and terms of IEC 61158.

HIGH AVAILABILITY AUTOMATION NETWORKS

1 Scope

This International Standard is applicable to high-availability automation networks based on the ISO/IEC 8802-3 (Ethernet) technology.

This International Standard specifies

- a classification scheme for network characteristics (see Annex A);
- a methodology for estimating network availability (see Annex B);
- a set of communication protocols that realize high availability automation networks via the use of redundancy and that can be used in a variety of applications (see Clauses 5, 6, 7, 8).

2 Normative references

The following referenced documents are indispensable for the application of this International Standard. 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 (IEV) – Chapter 191: Dependability and quality of service*

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

IEC 61784-1, *Industrial communication networks – Profiles – Part 1: Fieldbus profiles*

IEC 61784-2, *Industrial communications networks – Profiles – Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3*

IEC 61918, *Industrial communications networks – Installation of communication networks in industrial premises*

IEEE 802, *IEEE standard for local and metropolitan area networks: Overview and Architecture*

IEEE 802a, *IEEE standard for local and metropolitan area networks: Overview and Architecture*

Amendment 1: *Ethertypes for Prototype and Vendor-Specific Protocol Development*

IEEE 802.1D, *IEEE standard for local and metropolitan area networks: Media Access Control (MAC) bridges*

IEEE 802.1Q, *IEEE standards for local and metropolitan area networks: Virtual bridged local area networks*

IEEE 802.3:2005, *Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*

IEEE 1588, *IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*

DARPA Internet Program Protocol Specification, *Internet Protocol, RFC 791*

3 Terms, definitions, abbreviated terms, 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 the following, apply.

3.1.1

aggregated link

set of inter-switch links configured to work as one inter-switch link

[IEEE 802.3:2005, Clause 43]

3.1.2

aggregated ports

set of inter-switch ports configured to work as one inter-switch port

[IEEE 802.3:2005, Clause 43]

3.1.3

availability (performance)

ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided.

NOTE 1 This ability depends on the combined aspects of the reliability performance, the maintainability performance, and the maintenance support performance.

NOTE 2 Required external resources, other than maintenance resources, do not affect the availability performance of the item.

[IEV 191-02-05]

3.1.4

channel

layer 2 connection between two end nodes which consists of one or more paths (for redundancy) between end nodes

3.1.5

common mode failure

failure that affects all redundant elements for a given function at the same time

3.1.6

complete failure

failure which results in the complete inability of an item to perform all required functions

[IEV 191-04-20]

3.1.7

connection

logical relationship between two nodes

3.1.8

coverage

probability that a failure is discovered within a time short enough for redundancy to handle it, also expressing the percentage of failures caught up by redundancy versus total number of failures

3.1.9**degradation failure**

failure which is both a gradual failure and a partial failure

[IEV 191-04-22]

3.1.10**dependability**

collective term used to describe the availability performance and its influencing factors: reliability performance, maintainability performance and maintenance support performance

NOTE Dependability is used only for general descriptions in non-quantitative terms.

[IEV 191-02-03]

3.1.11**device**

physical entity connected to the network composed of communication element and possibly other functional elements

[IEC 61158-2, 3.1.12, modified]

NOTE Devices are for instance nodes, routers and switches in this International Standard, an end node and a switch can be combined in one device.

3.1.12**doubly attached node**

node that has two ports for the purpose of redundant operation

3.1.13**edge port**

port of a switch connected to a leaf link

3.1.14**end node**

node which is not able to forward application data to other nodes.

NOTE For the purpose of this standard, further specification is given in 4.2.1.2.

3.1.15**error**

discrepancy between a computed, observed or measured value or condition and the specified or theoretically correct value or condition

NOTE 1 An error can be caused by a faulty item, for example, a computing error made by faulty computer equipment.

NOTE 2 The French term "erreur" may also designate a mistake (see IEV 191-05-25).

[IEV 191-05-24, modified]

3.1.16**extended frame**

frame that has been extended by a Redundancy Control Trailer

3.1.17**failure**

termination of the ability of an item to perform a required function

NOTE 1 After failure the item has a fault.

NOTE 2 "Failure" is an event, as distinguished from "fault", which is a state.

NOTE 3 This concept as defined does not apply to items consisting of software only.

[IEV 191-04-01]

3.1.18

fault

state of an item characterized by its inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources

[IEV 191-05-01]

NOTE A fault is often the result of a failure of the item itself, but may exist without prior failure.

3.1.19

fault recovery time

time from the fault event, to the time when the network regains its required communication function in the presence of the fault

NOTE After fault recovery, the network is operating in a degraded mode using some of the redundancy elements, so it has reduced fault resilience, and may not be able to recover from a second fault.

3.1.20

frame

unit of data transmission on an ISO/IEC 8802-3 MAC (Media Access Control) that conveys a protocol data unit (PDU) between MAC service users

[IEEE 802.1Q, modified]

3.1.21

higher-layer entity

entity in a Media Access Control (MAC) Bridge that manages the logical topology of the LAN (spanning tree protocol entity, GARP entity, bridge management, etc.)

[IEEE 802.1D, 7.12.7]

3.1.22

instantaneous failure rate

limit, if it exists, of the quotient of the conditional probability that the instant of a failure of a non-repaired item falls within a given time interval ($t, t + \Delta t$) and the duration of this time interval, Δt , when Δt tends to zero, given that the item has not failed up to the beginning of the time interval

[IEV 191-12-02]

NOTE The failure rate is the reciprocal number of the MTTF when the failure rate is constant over the lifetime of one item.

3.1.23

inter-switch link

link between two switches

3.1.24

inter-switch port

port of a switch connected to another switch via an inter-switch link

3.1.25

LAN

part of the network consisting of hubs, switches and inter-switch links, characterized by a common link layer protocol and link address space

NOTE 1 An LAN excludes the end nodes and the leaf links.

NOTE 2 In the context of redundancy, a network may consist of several LANs operated in redundancy.

3.1.26

leaf link

link between an end node and the LAN

NOTE For the purpose of this standard, further specification is given in 4.2.1.3.

3.1.27

linear topology

topology where the switches are connected in series, with two switches each connected to only one other switch and all other switches each connected to two other switches (that is, connected in the shape of a line)

NOTE 1 This topology corresponds to that of an open ring.

NOTE 2 This configuration is sometimes named “daisy chain”. This International Standard does not use the term “daisy chain” because of possible confusion with the term “daisy chain” used elsewhere for busses. From the wiring point of view they require two different implementations.

[IEC 61918, 3.1.39, with modified notes]

3.1.28

link

physical, point-to-point, generally duplex connection between two adjacent nodes

[ISO/IEC 11801, modified]

NOTE “Link” is different from “bus”, which is a broadcast physical medium.

3.1.29

link redundancy entity

entity at layer 2 that hides port redundancy from the upper layers, by forwarding to the upper layers the frames received from the active redundant ports as if they came from a single port, and by forwarding to the active redundant ports a frame coming from the upper layers

3.1.30

link service data unit

data transported within a protocol layer on behalf of the upper layer

NOTE The link service data unit in an Ethernet frame is the content of the frame located between the length/type field and the frame check sequence.

3.1.31

mean failure rate

mean of the instantaneous failure rate over a given time interval $\lambda(t_1, t_2)$.

[IEV 191-12-03]

NOTE This standard uses “failure rate” for the meaning of “mean failure rate” defined by IEV 191-12-03.

3.1.32

mean operating time between failures

expectation of the operating time between failures

[IEV 191-12-09]

3.1.33

mean time to failure (MTTF)

expectation of the time to failure

[IEV 191-12-07]

3.1.34

mean time to recovery (MTTR)

expectation of the time to recovery

[IEV 191-13-08]

3.1.35

mesh topology

topology where each node is connected with three or more inter-switch links

3.1.36

message

ordered series of octets intended to convey information

NOTE Normally used to convey information between peers at the application layer.

[IEC 61784-2, 3.1.14]

3.1.37

network

communication system consisting of end nodes, leaf links and LAN(s)

NOTE A network may have more than one LAN for the purpose of redundancy.

3.1.38

node

network entity connected to one or more links

NOTE Nodes may be either a switch or an end node or both.

[IEC 61784-2, 3.1.16, modified]

3.1.39

partial failure

failure which results in the inability of an item to perform some, but not all, required functions

3.1.40

path

set of links and switches joined in series

NOTE There may be two or more paths between two switches to provide redundancy.

3.1.41

plant

system that depends on the availability of the automation network to operate

EXAMPLE Plants can be power plants, printing machines, manufacturing systems, substations, vehicles.

3.1.42

port

connection point of a node to the network

[ISO/IEC 15802-3]

NOTE 1 This definition is different from a TCP port or a UDP port, which this standard qualifies explicitly, if necessary.

NOTE 2 A port includes layer 1 and 2 implementation.

3.1.43**recovery**

event when the network regains the ability to perform its required communication function after a disruption

NOTE Examples of disruptions could be a fault or removal and reinsertion of a component.

3.1.44**recovery time**

time period between disruption and recovery

3.1.45**redundancy**

existence in an item of two or more means of performing a required function

[IEV 191-15-01]

NOTE In this standard, the existence of more than one path (consisting of links and switches) between end nodes.

3.1.46**reinstatement recovery time**

time to reinstate the original, or pre-fault, network configuration, including original operating and management states in each device

3.1.47**reliability**

ability of an item to perform a required function under given conditions for a given time interval

[IEV 191-02-06]

NOTE 1 It is generally assumed that the item is in a state to perform this required function at the beginning of the time interval.

NOTE 2 The term “reliability” is also used as a measure of reliability performance (see IEV 191-12-01).

3.1.48**repair**

action taken for the re-establishment of the specified condition

3.1.49**repair recovery time**

delay between the start of the repair action and the completion of repair of the faulty element such that the network has regained both its required communication function and its required fault resilience

NOTE 1 This time includes any network down time caused by the repair process, for example a network outage to replace a switch with several good ports and one faulty port.

NOTE 2 This time does not include re-instatement time to return the network from its backup mode of operation to the original mode of operation.

3.1.50**ring link**

link that connects two switches of a ring

3.1.51**ring port**

port of a switch to which a ring link is attached

3.1.52

ring topology

topology in which each node is connected in series to two other nodes

NOTE 1 Nodes are connected to one another in the logical shape of a circle.

NOTE 2 Frames are passed sequentially between active nodes, each node being able to examine or modify the frame before forwarding it.

[IEC 61918, 3.1.57, modified]

3.1.53

robustness

behaviour of the network in face of failures

3.1.54

route

layer 3 communication path between two nodes

3.1.55

single failure criterion

capacity of a system that includes redundant components to maintain its full functionality upon one failure of any of its components, prior to maintenance or automatic recovery

3.1.56

single point of failure

single failure point

component whose failure would result in failure of the system and is not compensated for by redundancy or alternative operational procedure

NOTE A single point of failure or single failure point causes a common mode failure. It may be caused by a design error in the redundant elements or by an external cause that affects all redundant elements in the same way, for example, extreme temperature.

3.1.57

singly attached node

node that has only one port to a LAN

3.1.58

stand-by redundancy

redundancy wherein a part of the means for performing a required function is intended to operate, while the remaining part(s) of the means are inoperative until needed

[IEV 19-5-03]

NOTE This is also known as dynamic redundancy.

3.1.59

star topology

topology in which all devices are connected to a central node

[IEC 61918, 3.1.63, modified]

3.1.60

switch

switch node

MAC bridge as defined in IEEE 802.1D

NOTE The term “switch” is used as a synonym for the term “switch node”.

3.1.61**systematic failure**

failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

NOTE 1 Corrective maintenance without modification usually eliminates the failure cause.

NOTE 2 A systematic failure can be induced by simulating the failure cause.

[IEV 191-04-19]

3.1.62**topology**

pattern of the relative positions and interconnections of the individual nodes of the network

[IEC 61918, 3.1.67, modified]

NOTE Additional aspects such as the delay, attenuation and physical media classes of the paths connecting network nodes are sometimes also considered to be properties of the topology.

3.1.63**tree topology**

topology in which any two nodes have only one path between them and at least one switch is attached to more than two inter-switch links

3.1.64**trunk portion**

part of a switched LAN that carries traffic for several end nodes

3.1.65**unavailability**

state of an item of being unable to perform its required function

[IEV 603-05-05]

NOTE Unavailability is expressed as the fraction of expected operating life that an item is not available, for example given in minutes per year.

3.1.66**upper layer entity**

parts of the protocol stack immediately above the redundancy handling layer

[IEV 603-05-05]

3.1.67**worst case recovery time**

maximum expected recovery time amongst all faults and for all allowed configurations

NOTE This delay is important for a network designer to indicate which aspects of the network need special treatment to minimize communication disruption.

3.2 Abbreviated terms and acronyms

AL	Application Layer
ARP	Address Resolution Protocol
ASE	Application Service Element
BPDU	Bridge management Protocol Data Unit, according to IEEE 802.1D

BRP	Beacon Redundancy Protocol, according to Clause 8.
CRP	Cross-network Redundancy Protocol, according to Clause 7
DAN	Doubly attached node
DANB	Double attached node implementing BRP, according to Clause 8
DANC	Doubly attached node implementing CRP, according to Clause 7
DANP	Double attached node implementing PRP, according to Clause 6
DLPPDU	Data Link Protocol Data Unit
DLSPDU	Data Link Service Data Unit
FCS	Frame Check Sequence, IEEE 802.3 cyclic redundancy check
FDB	Filtering Data Base
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
LLDP	Link Layer Discovery Protocol, see IEEE 802.1AB:2005
LRE	Link Redundancy Entity
LSB	Least Significant Bit
LSPDU	Link Service Data Unit
MAC	Media Access Control
MIB	Management Information Base
MRC	Media Redundancy Client, see Clause 5
MRM	Media Redundancy Manager, see Clause 5
MRP	Media Redundancy Protocol, see Clause 5
MTBF	Mean Time Between Failure
MTTF	Mean Time To Failure
MTTFN	Mean Time To Failure of Network
MTTFS	Mean Time To Failure of System
MTTR	Mean Time To Repair
MTTRP	Mean Time To Repair Plant
OUI	Organizational Unique Identifier
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
PRP	Parallel Redundancy Protocol, see Clause 6
PTP	Precision Time Protocol, see IEEE 1588

QAN	Quadruply Attached Node
RCT	Redundancy Control Trailer, see Clause 6
RSTP	Rapid Spanning Tree Protocol, see IEEE 802.1D:2004
SAN	Singly Attached Node
SANC	Singly Attached Node implementing CRP, see Clause 7
SNMP	Simple Network Management Protocol
SRP	Serial Redundancy Protocol, see Clause 6
VDAN	Virtual Doubly Attached Node, see Clause 6
VLAN	Virtual LAN, see IEEE 802.1Q

3.3 Conventions

3.3.1 General conventions

The protocols specified in this standard follow the structure defined in IEC 61158-1.

General guidelines are specified in IEC 61158-6-10, 3.6.

3.3.2 Conventions for state machine definitions

This standard follows the conventions used in IEC 61158-6-10, 3.7. The following is a summary.

- Each state is described by one table, with a separate row for each transition that may cause a state change.
- Transitions are defined as events that may carry arguments and be subject to conditions.
- The action field expresses the action that take place in case the event is fired.
- For space reasons, the event and the actions are in the same cell.
- The right column indicates the next state that is entered after the action is finished.

3.3.3 Conventions for PDU specification

PDUs are described according to specification DARPA RFC 791, Appendix B.

In particular:

- bits, octets and arrays are numbered starting with 0;
- the Network Byte Ordering (big-endian, most significant octet first) convention is observed.

IEC 61158-6-10 distinguishes bit identification from the bit offset.

EXAMPLE In a bit string of 8 bits, the rightmost bit (LSB) is labelled bit 0, but it has bit offset 7 within the bit string octet.

When specifying data objects rather than PDUs, the bit identification according to IEC 61158-6 is used. Consequently, bits of a bit string are specified in ascending bit identification, although they are transmitted in the opposite order.

3.4 Reserved network addresses

The following is a summary of the network addresses reserved for the purpose of this standard, whilst the prescribed values are specified in the respective clauses.

For the purpose of this standard, the OUI 01-15-4E has been reserved by IEEE. All bands within this OUI are reserved for this standard. The following bands are assigned:

- MRP (see Clause 5) uses 01-15-4E, band 00-00-xx.
- PRP (see Clause 6) uses 01-15-4E, band 00-01-xx.
- CRP (see Clause 7) uses an IP multicast MAC address.
- BRP (see Clause 8) uses 01-15-4E, band 00-02-xx.

For the purpose of this standard, the following Ethertypes (see IEEE 802a) have been reserved by IEEE:

- MRP (see Clause 5) uses 0x88E3.
- PRP (see Clause 6) uses 0x88FB.
- CRP (see Clause 7) uses 0x0800 (IP) with UDP port 3622.
- BRP (see Clause 8) uses 0x80E1.

4 Concepts for high availability automation networks

4.1 Characteristics of application of automation networks

4.1.1 Resilience in case of failure

Plants rely on the correct function of the automation system. Plants tolerate a degradation of the automation system for only a short time, called the grace time. The network recovery time should be shorter than the grace time since the application typically needs to perform additional tasks (related to protocol and data handling, waiting for the next scheduled communication cycle, etc.) before the plant is back to the fully operational state. Applications can be distinguished by their grace time, as Table 1 shows.

Table 1 – Examples of application grace time

Applications	Typical grace time
Uncritical Automation, for example, enterprise systems	20 s
Automation management, for example, manufacturing, discrete automation	2 s
General automation, for example, process automation, power plants	0,2 s
Time-critical automation, for example, synchronized drives	0,020 s

Some plants have stricter requirements when they are required to operate continuously, having no idle period during which the plant may be maintained or reconfigured. In this case, the grace time holds for the stricter requirement, for instance, dictated by the hot-swapping of parts of the equipment.

Automation systems may contain redundancy to cope with failures. Methods differ on how to handle redundancy, but their key performance factor is the recovery time, i.e., the time needed to restore operation after occurrence of a disruption. If the recovery time exceeds the grace time of the plant, protection mechanisms initiate a (safe) shutdown, which may cause significant loss of production and plant operational availability.

A key characteristic of recovery is its determinism, i.e., the guarantee that the recovery time remains below a certain value as long as the basic assumptions (single failure at a time, no common mode of failure, less than maximum system extension) are met.

Whenever operation depends on the correct function of the automation network, it may become necessary to increase the availability of the network.

Raising availability by increasing reliability of the elements or improving maintenance is outside the scope of this standard. This standard considers only protocols that introduce redundancy and automatically reconfigure redundant network elements in case of failure.

4.1.2 Classes of network redundancy

4.1.2.1 General

This standard considers two classes of network redundancy:

- redundancy managed within the network;
- redundancy managed in the end nodes.

NOTE This standard does not consider redundancy of the end nodes themselves, i.e., the use of redundant end nodes, since this is highly application specific.

4.1.2.2 Redundancy managed within the network

Redundancy within a network has been applied to wide area networks and to legacy field busses.

Layer 3 routers (not considered in this standard) calculate alternate routes upon link failures. The corresponding protocols are well proven as part of the IP suite, but the recovery time is in the order of dozen of seconds, if not minutes, depending on the topology. Such recovery times are only tolerated by the most benign applications.

Automation networks usually operate within one single Local Area Network (LAN), i.e., messages for operation are threaded through layer 1 repeaters or layer 2 switches, but do not cross routers. Messages to and from the outside world over routers or firewalls do exist, but are considered to be uncritical.

Classically, redundancy within a LAN is handled by protocols that react to loss of links and switches by reconfiguring the LAN, using redundant links and switches, such as the Rapid Spanning Tree Protocol (RSTP) according to IEEE 802.1D.

Improved Layer 2 redundancy protocols build on similar principles as RSTP, but provide a faster recovery by exploiting the assumption that the automation network has a ring topology. End nodes are unmodified automation nodes.

4.1.2.3 Redundancy managed in the end nodes

Further improvements in recovery time require managing of redundancy in the end nodes, by equipping the end nodes with several, redundant communication links. In general, doubly attached end nodes provide sufficient redundancy. In this type of redundancy, no assumption about the switches within the LAN is made.

For time-critical applications such as synchronized drives, the parallel operation of disjoint networks provides a seamless recovery, but requires complete duplication of the network. Some critical plants also require doubly attached nodes in order to cope with a failure of a leaf link, even if they do not require a very short recovery time.

4.1.3 Redundancy maintenance

Redundancy can be affected by latent faults, which can be detected by testing. The testing interval allows availability to be estimated. All protocols provide the means to test the redundant or spare components and report detected failures to the network management.

4.1.4 Comparison and indicators

The protocols specified in this standard offer

- a maximum, deterministic and guaranteed recovery time (that may depend on the topology);
- transparency of the actual communication towards the application under all circumstances; and
- for doubly attached nodes, interoperability with singly attached devices (off-the-shelf, IT equipment).

Table 2 compares some characteristics of some redundancy protocols, ordered by recovery time.

Table 2 – Examples of redundancy protocols

Protocol	Solution	Frame loss	Redundancy protocol	End node attachment	Network topology	Recovery time fault or repair
IP	IP routing	Yes	Within the network	Single	Single meshed	>30 s typical not deterministic
STP	IEEE 802.1D:1998	Yes	Within the network	Single	Single meshed	>20 s typical not deterministic
RSTP	IEEE 802.1D:2004	Yes	Within the network	Single	Single meshed	>2 s typical not deterministic
CRP	IEC 62439, Clause 7	Yes	In the end nodes	Single and double	Connected, doubly meshed	1 s worst case for 512 end nodes
MRP	IEC 62439, Clause 5	Yes	Within the network	Single	Ring	200 ms worst case for 50 switches
BRP	IEC 62439, Clause 8	Yes	In the end nodes	Double	Connected, doubly meshed	4,8 ms worst case for 500 end nodes
PRP	IEC 62439, Clause 6	No	In the end nodes	Double	Independent double meshed	0 s

NOTE For the redundancy protocols specified in this standard, the recovery times in Table 2 are guaranteed when using the specified settings and parameters. Faster recovery times may be achieved using different settings and parameters under the user's responsibility.

The indicators for the different solutions include, when applicable,

- fault recovery time;
- repair recovery time;
- reinstatement recovery time;
- worst-case recovery time;
- impact on normal operation.

The fault cases include

- failure of the current active network manager (if it exists) followed by repair and reinstatement;
- failure of the current source of network time (if it exists), followed by repair and reinstatement.

Subclause 4.2 generalizes the above considerations and introduces a classification scheme.

4.2 Generic network system

4.2.1 Network elements

4.2.1.1 General

The generic network is modelled with the functional elements listed below and represented in Figure 1.

- End nodes
- Leaf links
- Switches (with edge ports and inter-switch ports)
- Inter-switch links
- Switching end nodes

The LAN consists of all network components, except the end nodes and leaf links.

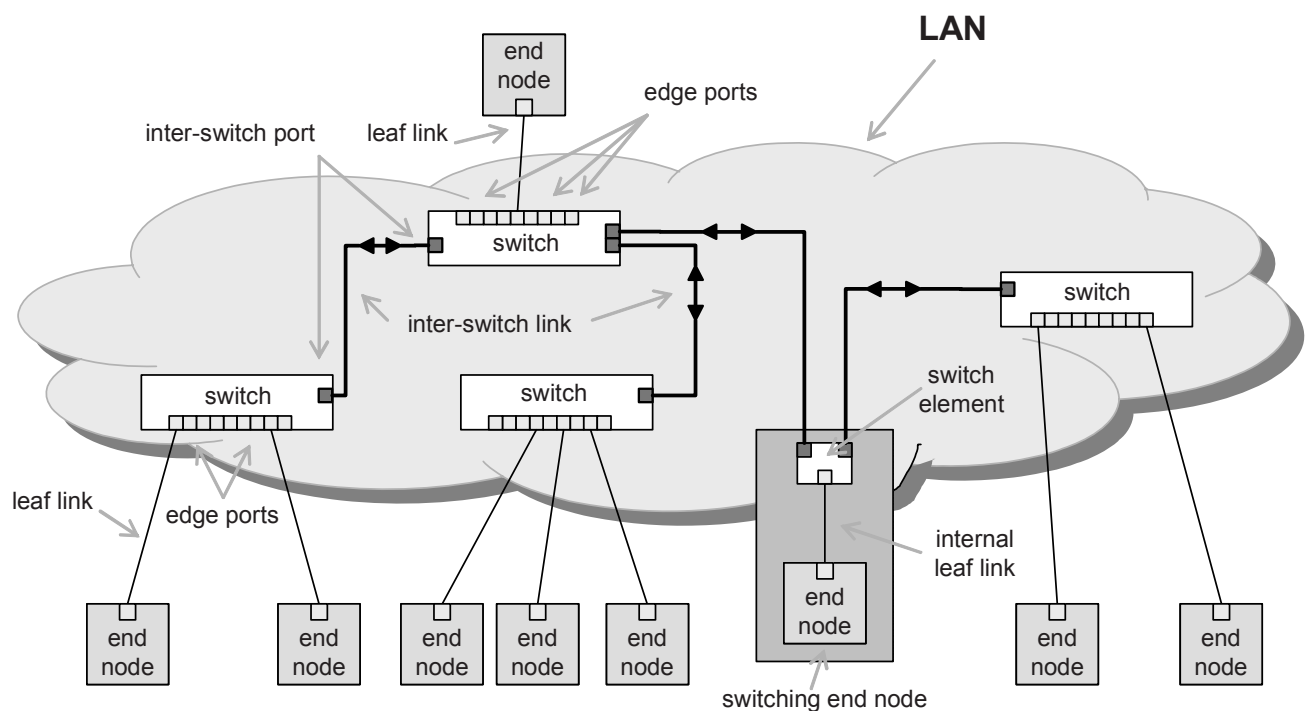


Figure 1 – General network elements (tree topology)

NOTE Edge ports are shaded in light grey, inter-switch ports are shaded in dark grey, inter-switch links are drawn with a thick line, leaf links drawn with a thin line.

4.2.1.2 End node

An end node requires one connection port to the LAN for its normal operation.

The connection port of an end node is connected to an edge port of a switch in a LAN by a leaf link.

4.2.1.3 Leaf link

A leaf link connects an end node with a LAN.

This connection may be internal to a device, in the case where the device combines the end node and switch or LRE functionality (switching end node in Figure 1).

4.2.1.4 Inter-switch link

An inter-switch link connects the switches within a LAN.

There may be several inter-switch links between two switches to increase availability.

4.2.1.5 Switches

Switches are layer 2 connecting elements as defined in IEEE 802.1D.

NOTE Bridges according to IEEE 802.1D are called switches in this standard.

Switches are connected to each other by inter-switch links.

A switch is connected to a leaf link through an edge port.

4.2.1.6 Switching end node

A switch element may be implemented within the same piece of physical equipment as the end node. Although this makes the end node appear to be a doubly attached node, internally the operating principle is different, since there is no need for a link redundancy entity (LRE) because the switch element plays this role.

4.2.1.7 End nodes with multiple attachments

End nodes may have more than one connection port for redundancy. Connection ports of an end node may be connected to the same LAN or may be connected to different LANs.

End nodes with more than one attachment require an LRE in their communication stack to hide redundancy from the application (see Figure 22 or Figure 31 or Figure 39).

An end node connected to one or two LANs of the same network through two leaf links is a doubly attached node (DAN).

An end node connected to one or more LANs of the same network through four leaf links is a quadruply attached node (QAN).

NOTE End nodes using different communication ports for independent networks are not considered here, the considerations apply to each network separately.

4.2.2 Topologies

4.2.2.1 General

Redundancy within the network considers the presence of more network elements (switches, links) than necessary for operation, in order to prevent loss of communication caused by a failure. To this effect, there is more than one physical path between any two end nodes.

IEC 61918 specifies various kinds of basic physical topologies, some of which are used by this standard to define different topologies.

- a) Topologies without redundancy
 - Tree topology (Figure 2)
 - Linear topology (Figure 3)
- b) Topologies with redundant links
 - Ring topology (Figure 4)
 - Partial meshed topology (Figure 5)

– Fully meshed topology (Figure 6)

There are four top level structures.

- Single LAN without redundant leaf links (see 4.2.2.4.1)
- Single LAN with redundant leaf links (see 4.2.2.4.2)
- Redundant LANs without redundant leaf links (see 4.2.2.4.3)
- Redundant LANs with redundant leaf links (see 4.2.2.4.4)

When redundancy is handled in the LAN, end nodes can be singly attached. In the case of switch or leaf link failure, such end nodes may lose communication.

4.2.2.2 Topologies without redundancy

4.2.2.2.1 Tree topology

In a tree topology, at least one switch has more than two inter-switch links and there is only one path between any two devices. Figure 2 shows an example of tree topology.

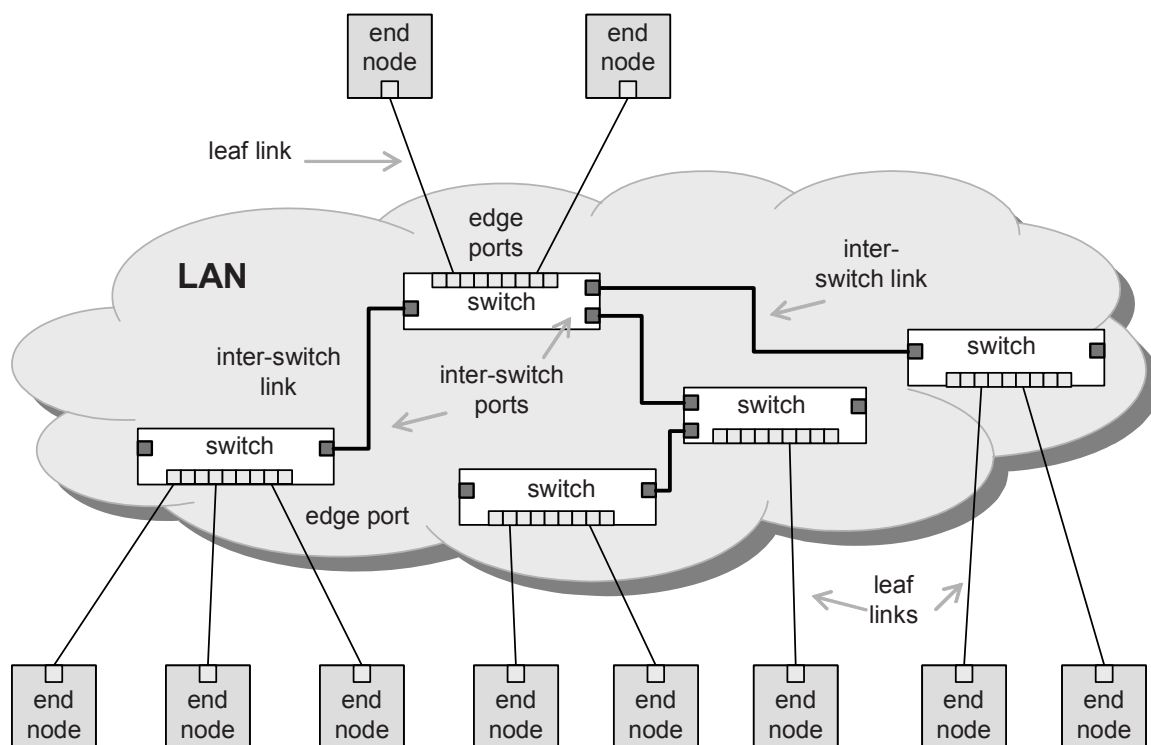


Figure 2 – Example of tree topology

4.2.2.2.2 Linear topology

In a linear topology, all switches are connected to each other in line and no node has more than two inter-switch links but the two nodes located at the end of the line have only one inter-switch link. Figure 3 shows an example of linear topology.

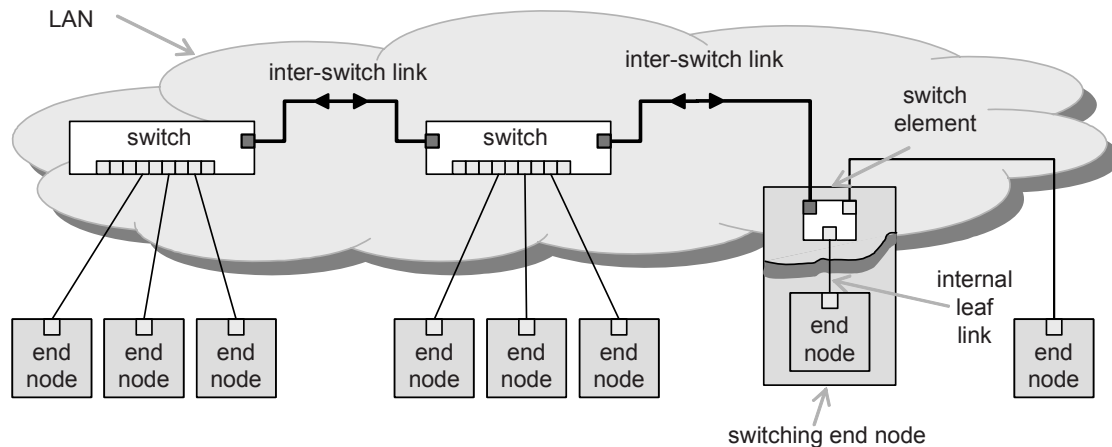


Figure 3 – Example of linear topology

NOTE A node may be a switching end node, as shown in the second rightmost end node of Figure 3.

4.2.2.3 Topologies with redundant links

4.2.2.3.1 Ring topology

NOTE This topology applies to MRP redundancy (see Clause 5).

In a ring topology, every switch has two inter-switch links and any two end nodes have two paths between them when all components are operational. Figure 4 shows an example for the ring topology.

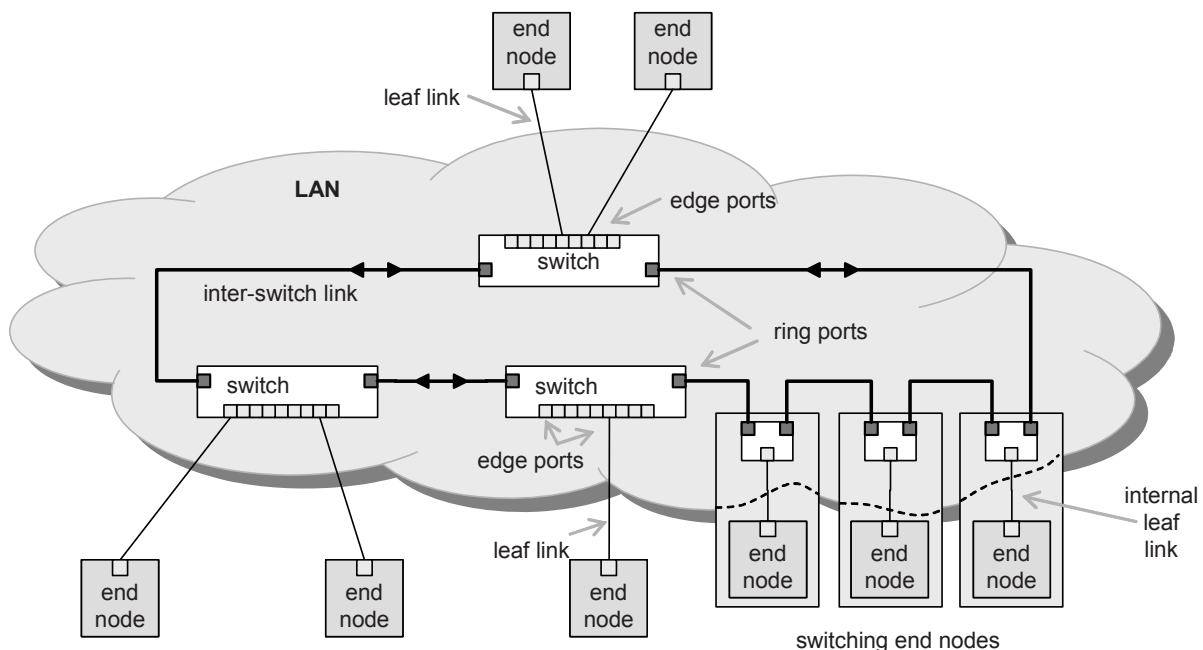


Figure 4 – Example of ring topology

A ring topology introduces a loop in the LAN that could lead to flooding by permanently circulating frames. Protocols such as the rapid spanning tree protocol (RSTP) and the media redundancy protocol (MRP) ensure that the switches maintain a logical linear topology during initialization, operation and reconfiguration.

If a switch or an inter-switch link fails, the switch is excluded from the ring, and a new logical linear topology is established. However, end nodes connected to a failed switch lose connectivity.

4.2.2.3.2 Partially meshed topology

In a partially meshed topology, at least one switch has more than two inter-switch links and there exist more than one path between some devices. Figure 5 shows an example of a meshed topology.

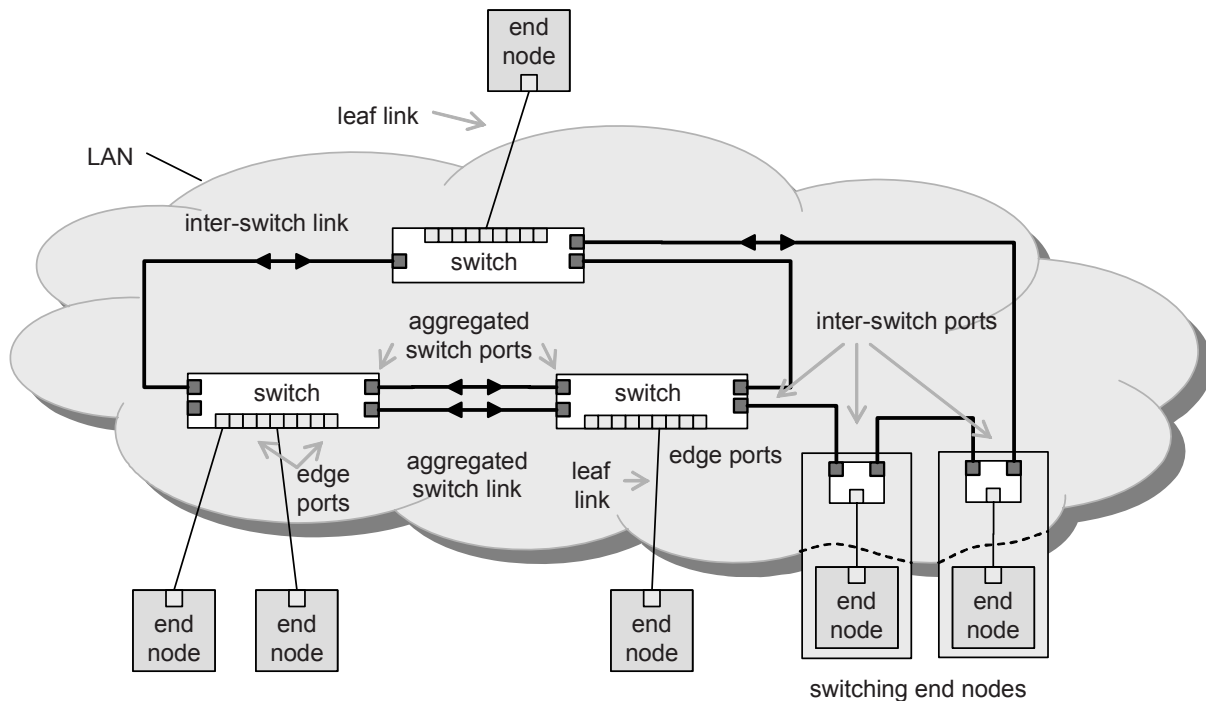


Figure 5 – Example of a partially meshed topology

4.2.2.3.3 Fully meshed topology

In a fully meshed topology, every switch has more than two inter-switch links.

In a fully meshed topology, the failure of any inter-switch link and of any switch can be tolerated. However, end nodes connected to a failed switch lose connectivity. Figure 6 shows an example of a fully meshed topology.

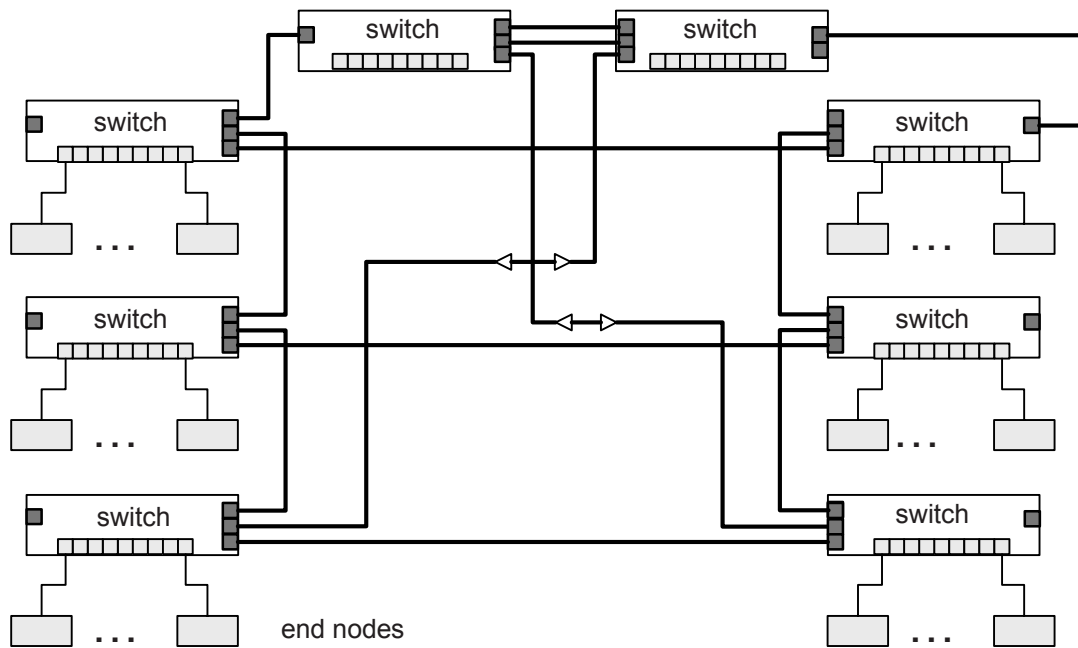


Figure 6 – Example of fully meshed topology

4.2.2.4 Top level structures of networks

4.2.2.4.1 Single LAN without redundant leaf links

This topology has only one path between any two nodes (see Figure 7).

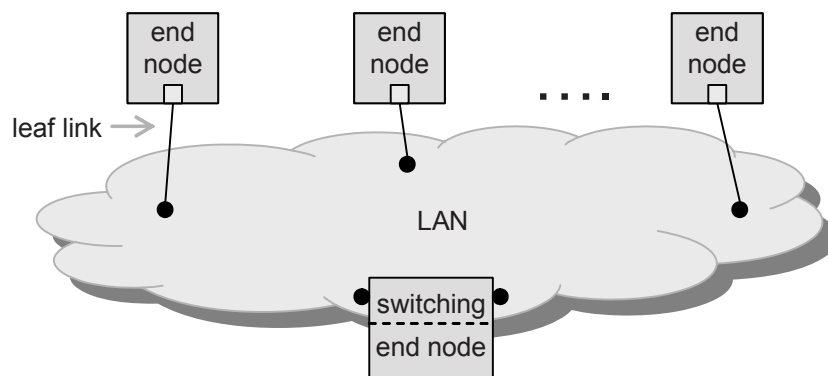


Figure 7 – Single LAN structure without redundant leaf links

Examples of this topology are the tree and linear topologies (see Figure 2 and Figure 3).

4.2.2.4.2 Single LAN with redundant leaves

NOTE This topology applies to SRP (see Clause 6).

DANs are connected to the same LAN through leaf links. Each edge port may belong to the same switch or to different switches. Figure 8 gives an example.

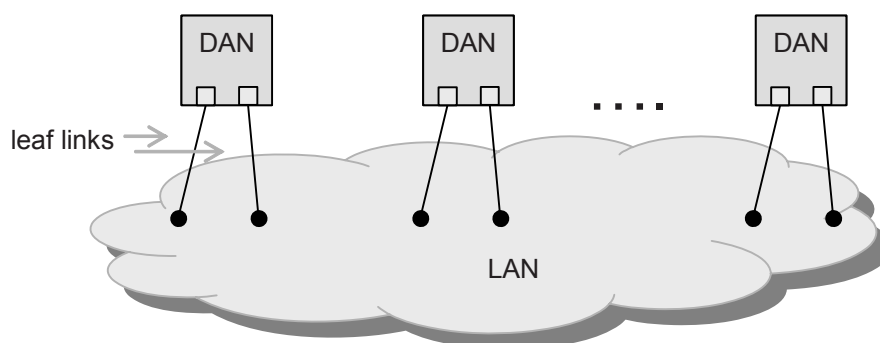


Figure 8 – Single LAN structure with redundant leaf links

4.2.2.4.3 Network without redundant leaves

NOTE This topology applies to PRP (see Clause 6), CRP (see Clause 7) and BRP (see Clause 8).

In this type of topology, paths do not overlap. Redundant leaf links are connected to different LANs. An example is shown in Figure 9.

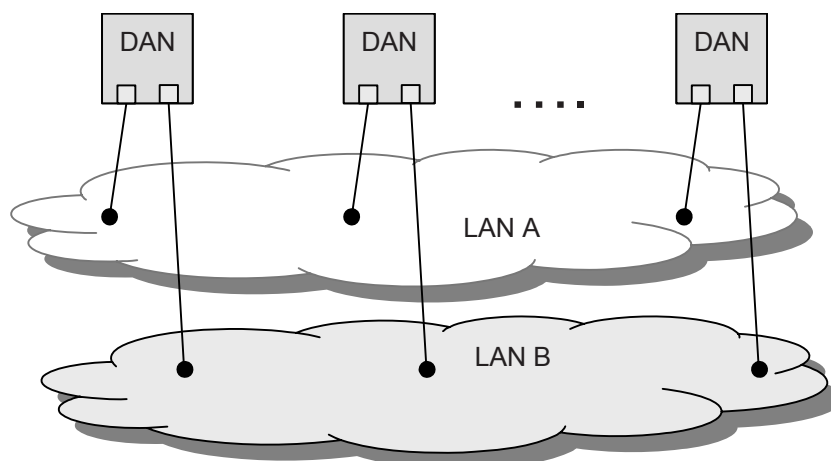


Figure 9 – Redundant LAN structure without redundant leaf links

4.2.2.4.4 Network with redundant leaf links

Redundant leaf links are connected both to the same LAN and different LANs. Nodes are quadruply attached nodes (QANs). An example is shown in Figure 10.

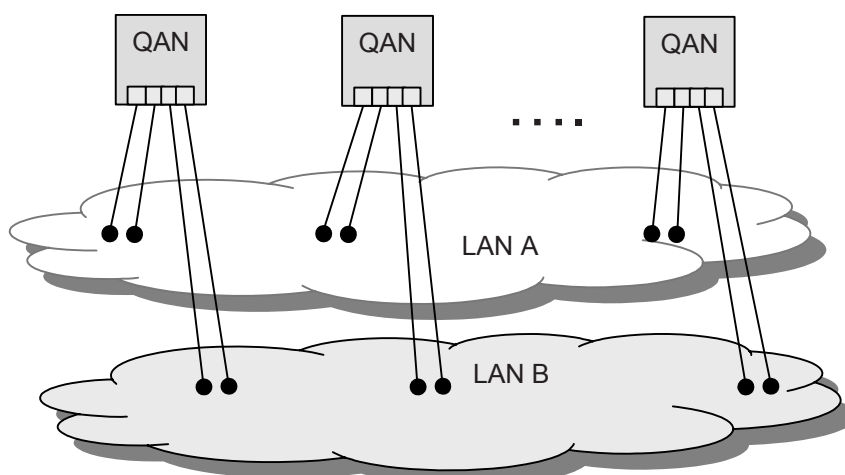


Figure 10 – Redundant LAN structure with redundant leaf links

4.2.3 Redundancy handling

4.2.3.1 Backup mode

In the backup mode, only one of the redundant paths is selected as on-service while the other paths are in stand-by.

If the on-service path becomes unavailable, another path backs it up.

During the elapsed time from the loss of the on-service path to the beginning of operation of the backup path, messages can be lost, therefore the channel is considered in disconnected state.

NOTE IEV calls this kind of redundancy “stand-by” or “passive” redundancy. The term “dynamic redundancy” is also used.

4.2.3.2 Alternate (active) mode

In the alternate mode, redundant paths are used alternately, at random or according to regular patterns, and messages are transmitted via one of the redundant paths.

If it is detected that one of the redundant paths is in disconnected state, that path stops being used while other paths continue being used alternatively.

This mode allows checking the availability of the components continuously and therefore increases coverage.

4.2.3.3 Parallel (active) operation

In the parallel operation, messages are transmitted via all available redundant paths.

The receiving end node selects one of the received messages.

NOTE The term “static redundancy” or “work-by” is also used.

4.2.4 Network recovery time

Network recovery time is called recovery time in this standard because this standard deals only with networks. The definition in 3.1.44 applies.

4.2.5 Diagnosis coverage

Faults are detected through error-detection mechanisms that detect only a percentage of the faults. The coverage is the probability that diagnosis mechanisms detect an error within a time that allows recovery before other mechanisms take action to protect the plant or before the plant suffers damage.

4.2.6 Failures

4.2.6.1 Kinds of failure

There are three kinds of failure:

- transient failure;
- component failure; and
- systematic failure.

They affect the following elements:

- end nodes;

- leaf links;
- switches;
- inter-switch links.

4.2.6.2 Transient failures

A transient failure such as EM interferences causes transient errors, which leave the hardware essentially intact but disrupt the function. In this case, the failed part can be automatically reintegrated after automatic testing. Such mechanisms are partially implemented in the redundancy protocols specified in this standard.

NOTE EM interferences can become systematic failures.

4.2.6.3 Component failure

A component failure may be partial or complete. Only complete failures of components (not intermittent, not spurious) are considered in this standard.

4.2.6.4 Systematic failure

A systematic failure affects several redundant components at the same time; it is therefore a single point of failure. Configuration errors also belong to this category. The redundancy protocols specified in this standard do not consider systematic failures but allow detecting some.

NOTE Diversity of the design is possibly able to reduce impact of systematic failure.

4.2.6.5 End node failure

End node failure is outside the scope of this standard.

4.2.6.6 Leaf link failure

Leaf link failure is caused by

- failure of the connection port of end node;
- failure of the leaf link cable; or
- failure of the edge port.

4.2.6.7 Switch failure

A switch consists of a core switch functionality (for instance, processor, power supply) and a number of ports.

For calculation purposes, a switch failure considers only the failure of the core switch function.

Failure of an edge port of the switch is considered as a leaf link failure.

Failure of an inter-switch port of the switch is considered as an inter-switch link failure.

4.2.6.8 Inter-switch link failure

Inter-switch link failure is caused by

- failure of either inter-switch port; or
- failure of the inter-switch link cable.

4.3 Safety

This standard does not consider safety aspects such as integrity.

NOTE Even though safety is not directly addressed, high reliability is a desirable feature in a safety system.

4.4 Security

This standard does not consider security (for example privacy, authentication) issues.

4.5 Conformance

4.5.1 Conformance to redundancy protocols

A statement of compliance with a clause of this standard shall be stated as:

- compliance to IEC 62439, Clause 5 (MRP); or
- compliance to IEC 62439, Clause 6 (PRP); or
- compliance to IEC 62439, Clause 7 (CRP); or
- compliance to IEC 62439, Clause 8 (BRP).

A conformance statement shall be supported with appropriate documentation as defined in 4.5.2. The supported protocols and options shall be specified as PICS, in the format PICS_62439-X_supported options.

Example PICS_62439-5_BlockingSupported.

4.5.2 Conformance tests

4.5.2.1 Concept

The concept of this conformance test is to verify the capabilities of a device under test (DUT) against a consistent set of indicators under simulated worst-case conditions. The conformance test shall assert the interoperability of devices which claim compliance with the same protocol.

This standard contains specifications that are to be observed by the following different actors:

- the device builder, who designs and tests a compliant interface;
- the network manager, who defines the topology;
- the user of the network, who respects the operational limitations.

A device sold as being fully compliant with this standard could underperform if the network configuration rules are not observed when it is used.

Figure 11 gives an overview of the conformance test related to this standard.

NOTE Conformance test implementation and conformance test execution are not defined in this standard.

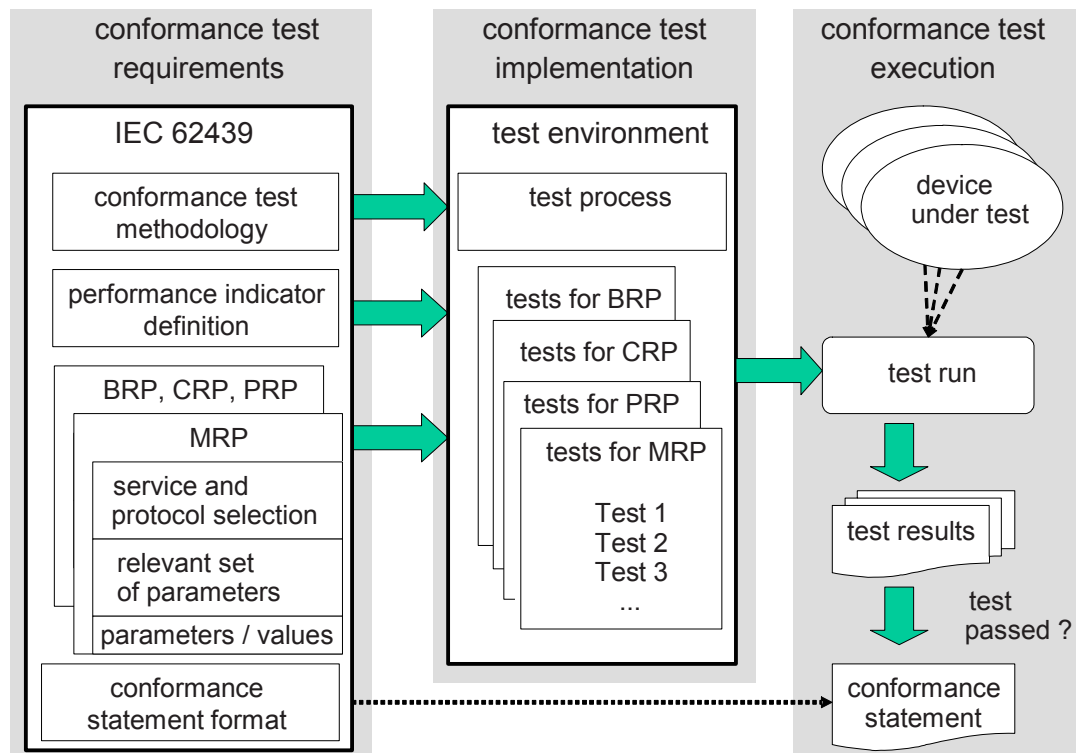


Figure 11 – Conformance test overview

4.5.2.2 Methodology

Test cases shall be developed in a way that tests are repeatable. Test results shall be documented and shall be used as the basis for the conformance statement.

Conformance tests of a device shall include, as appropriate, the verification of

- correctness of the specified functionality;
- network-related indicator values;
- device-related indicator values.

The performance indicator values of the protocol and of the device under test shall be used.

NOTE 1 A description of a conformance testing process is given in ISO/IEC 14496-4.

NOTE 2 It is assumed that the quality of the test cases guarantees the interoperability of a tested device. If any irregularities are reported, the test cases will be adapted accordingly.

4.5.2.3 Test conditions and test cases

Test conditions and test cases shall be defined and documented based on a specific redundancy protocol. This shall include the following indicators, when applicable:

- number of nodes;
- network topology;
- number of switches between nodes;
- type of traffic.

For each measured indicator, test condition and test case documents shall be prepared and shall describe

- test purpose;

- test set-up;
- test procedure;
- criteria for compliance.

Test set-up describes the equipment set-up necessary to perform the test including measurement equipment, DUT, auxiliary equipment, interconnection diagram, and test environmental conditions.

Parts of the test environment may be emulated or simulated. The effects of the emulation or simulation shall be documented.

The test procedure describes how the test should be performed, which also includes a description of a specific set of indicators required to perform this test. The criteria for compliance define test results accepted as compliance with this test.

4.5.2.4 Test procedure and measuring

The measured indicators shall include, when applicable,

- redundancy recovery time;
- impact of redundancy overhead on normal operation.

The test procedure shall be based on the principles of 4.5.2.3.

The sequence of measuring actions to complete a test run shall be provided.

The number of independent runs of the test shall be provided.

The method to compute the result of the test from the independent runs shall be provided if applicable.

4.5.2.5 Test report

The test report shall contain sufficient information so that the test can be repeated.

The test report shall contain at least

- a) the reference to the conformance test methodology according to 4.5.2.2;
- b) the reference to the performance indicator definitions;
- c) the reference to the used redundancy protocol according to this standard,
- d) a description of the conformance test environment including network emulators, measurement equipment and the person or organization responsible for the test execution, and the date of testing;
- e) a description of the DUT, its manufacturer, and hardware and software revision;
- f) the number and type of devices connected to the network together with the topology;
- g) a reference to the test case specifications;
- h) the measured values;
- i) a statement regarding compliance with the redundancy protocol.

5 MRP – Media Redundancy Protocol based on a ring topology

5.1 MRP Overview

The Media Redundancy Protocol (MRP) specifies a recovery protocol based on a ring topology.

MRP is designed to react deterministically on a single failure of an inter-switch link or switch in the network.

MRP is based on functions of ISO/IEC 8802-3 (IEEE 802.3) and IEEE 802.1D including the filtering data base (FDB) and is located between the data link layer and application layer (see Figure 12).

NOTE Layering is assumed to be according to IEC 61158-1.

A compliant network shall have a ring topology with multiple nodes.

One of the nodes has the role of a media redundancy manager (MRM). The function of the MRM is to observe and to control the ring topology in order to react on network faults. The MRM does this by sending frames on one ring port over the ring and receiving them from the ring over its other ring port, and vice versa in the other direction.

The other nodes in the ring have the role of media redundancy clients (MRC). An MRC reacts on received reconfiguration frames from the MRM and can detect and signal link changes on its ring ports.

A compliant node shall have the ability to perform as one of the following:

- media redundancy manager (MRM);
- media redundancy client (MRC); or
- both MRM and MRC (but both roles shall not be active at the same time).

Each MRP-compliant node requires a switch element with two ring ports connected to the ring.

NOTE Additional ring ports may be used to connect to another ring.

Each node in the ring is able to detect the failure or recovery of an inter-switch link or the failure or recovery of a neighbouring node (see 5.2.1).

The MRP consists of a service and a protocol entity, see stack model in Figure 12.

The service entity specifies, in an abstract way, the externally visible service provided by the data link layer in terms of

- primitive actions and events of the service;
- parameters associated with each primitive action and event, and the form which they take; and
- interrelationship between these actions and events, and their valid sequences.

MRP defines the services provided to

- the application layer at the boundary between the application layer and the data link layer; and
- the MRP management at the boundary between the data link layer and the MRP management.

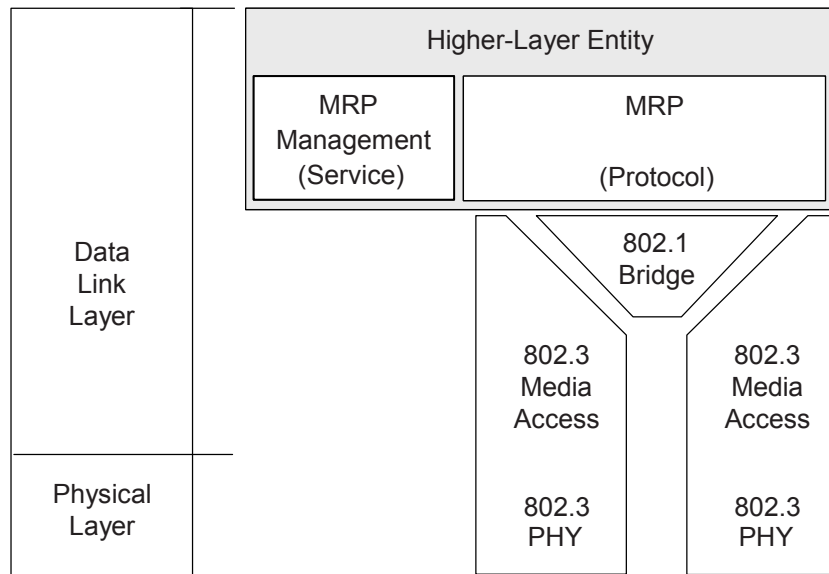


Figure 12 – MRP stack

5.2 MRP Media redundancy behaviour

5.2.1 Ring ports

The MRM and the MRC shall have two ring ports.

The MRM and MRC shall be able to detect the failure or recovery of a link on a ring port with mechanisms based on IEEE 802.3.

The MRM and MRC shall not forward MRP_Test frames, MRP_TopologyChange frames, and MRP_LinkChange frames to non-ring ports.

A ring port shall take one of the following port states:

- **DISABLED:**
All frames shall be dropped.
- **BLOCKED:**
All frames shall be dropped except:
 - MRP_TopologyChange frames and MRP_Test frames from the MRM.
 - MRP_LinkChange frames from an MRC.
 - frames from other protocols that are defined in IEEE 802.1D, Tables 7-10 to pass ports that are in BLOCKED state (for example, LLDP, PTP).
 - frames with a destination address equal to a group address configured in the Permanent Database (see IEEE 802.1D, 7.12.6) marked to pass ports that are in BLOCKED state.
- **FORWARDING:**
All frames shall be passed through according to the forwarding behaviour of IEEE 802.1D.

NOTE 1 Designers should be aware that switches in a ring should not block additional services which are supported by the switches.

NOTE 2 IEEE 802.1D calls the port state corresponding to BLOCKED as BLOCKING.

5.2.2 Media Redundancy Manager (MRM)

The first ring port of the MRM shall be connected to a ring port of an MRC. The other ring port of that MRC shall be connected to a ring port of another MRC or to the second ring port of the MRM, thereby forming a ring topology as shown in Figure 13.

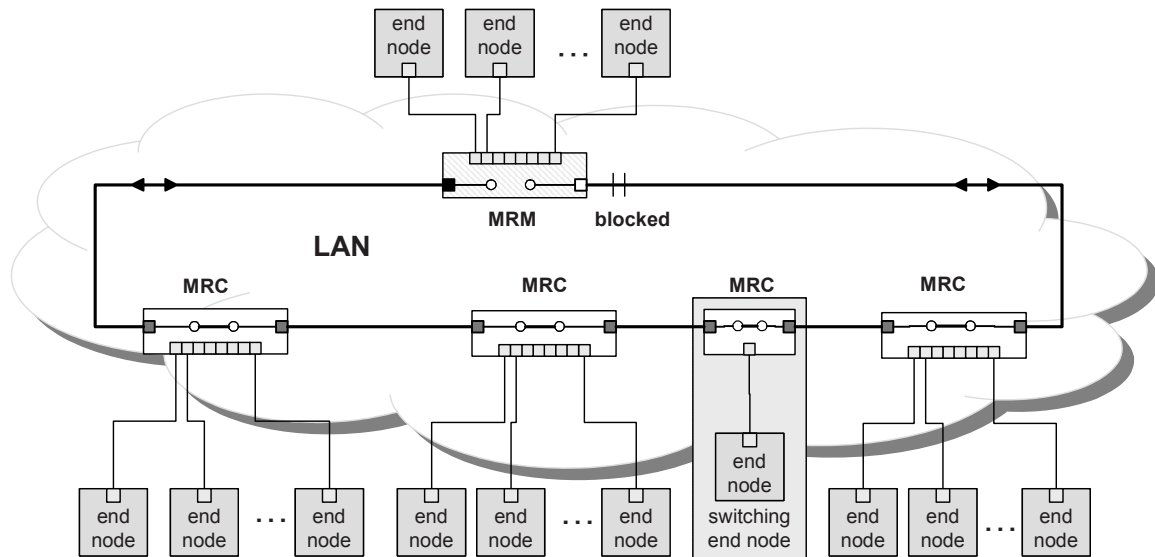


Figure 13 – MRP ring topology with one manager and clients

The MRM shall control the ring state by

- sending MRP_Test frames at a configured time period in both directions of the ring;
- setting one ring port in FORWARDING state and the other ring port in BLOCKED state if it receives its own MRP_Test frames (this means that the ring is closed, see Figure 13);
- setting both ring ports in FORWARDING state if it does not receive its own MRP_Test frames within a configured time according to MRP_TSTdefaultT, MRP_TSTshortT and MRP_TSTNRmax in Table 35 (this means that the ring is open, see Figure 14).

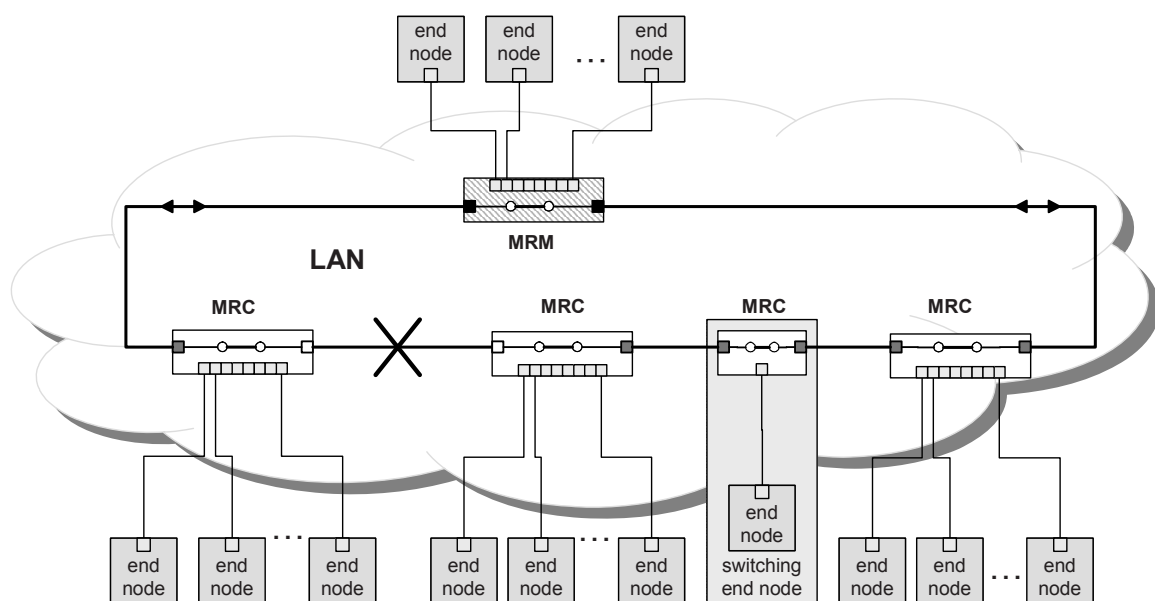


Figure 14 – MRP MRM in an open ring

The following mechanism supports synchronization between MRM and MRC in ring topology changes.

The MRM shall indicate changes in the ring state to the MRCs by means of MRP_TopologyChange frames.

The MRM shall not forward MRP specific frames (MRP_Test frames, MRP_TopologyChange frames, MRP_LinkChange frames) between its ring ports.

If the MRM receives an MRP_LinkUp or MRP_LinkDown frame, then the MRM shall reduce its test monitoring time according to Table 35 to accelerate the detection of the open ring. When the open ring is detected then the MRM shall send the MRP_TopologyChange frames through both its ring ports.

Optionally, the MRM shall send the MRP_TopologyChange frames through its ring ports. This option is selected by setting the parameter REACT_ON_LINK_CHANGE; see Table 28.

The MRM shall send to the MRCs an MRP_TopologyChange frame with the delay, after which the ring topology change will be performed. The parameter carrying this delay is called MRP_Interval. When this time has expired, all MRCs shall clear their filtering database (FDB).

Each MRC shall send the configured delay in MRP_Interval to the MRM in the MRP_LinkUp and MRP_LinkDown frames to tell the MRM after which time the MRC will change its port state from BLOCKED to FORWARDING (MRP_LinkUp frame) or to DISABLED (MRP_LinkDown frame).

Measures shall be included to prevent the MRM from remaining stuck in the closed state in case of node failure.

5.2.3 Media Redundancy Client (MRC)

Each MRC shall forward MRP_Test frames received on one ring port to the other ring port and vice versa.

If the MRC detects a failure or recovery of a ring port link, the MRC may optionally notify the change by sending MRP_LinkChange frames through both of its ring ports. Each MRC shall forward MRP_LinkChange frames received on one ring port to the other ring port and vice versa.

Each MRC shall forward MRP_TopologyChange frames received on one ring port to the other ring port and vice versa. Each MRC shall process these frames. It shall clear its FDB if requested by an MRP_TopologyChange frame in a given time interval (see Table 35, MRP_TOPchgT).

5.2.4 Redundancy domain

The redundancy domain represents a ring. By default, all MRM and MRCs belong to the default domain. A unique domain ID can be allocated as a key attribute, especially if an MRM or an MRC is member of multiple rings. A node shall assign exactly two unique ring ports per redundancy domain.

NOTE 1 A device may have other ports than the two assigned to MRP. These other ports are not influenced by MRP.

NOTE 2 MRP ports should behave as if RSTP is disabled.

5.2.5 Usage with diagnosis and alarms

If the attribute Check Media Redundancy has the value TRUE, media redundancy events shall cause diagnosis events and alarm notifications.

5.2.6 Ring diagnosis

In a redundancy domain the following diagnosis events handling shall be implemented by each MRM.

- If a device is configured as MRM, but not operating in the manager role, it shall signal a “MANAGER_ROLE_FAIL” diagnosis event and suspend reporting of all other media redundancy diagnosis events while not in the manager role.
- If a device is operating in manager role and this device detects another active MRM, it shall signal the “MULTIPLE MANAGERS” event. This event can occur concurrently with the ring state event “RING_OPEN”.
- If a device is operating in manager role and detects an open ring, it shall signal the “RING_OPEN” event.

These events shall be signalled by using the State Change service see 5.4.3.

NOTE The presence of MRP_Test frames enables the checking of the existence of an MRM.

5.2.7 Multiple MRM in a single ring

There shall be only one active MRM in the ring even if several nodes have this ability.

NOTE Multiple active MRMs cause the ring to divide itself into several segments.

As an option, in case of more than one node having the ability to become an MRM in the ring, an enhanced protocol not specified in this standard may be used to decide which of these nodes shall become the MRM, while the other nodes take over the MRC role as shown in Figure 15. To this effect the nodes with the MRM ability have different priorities that shall be conveyed in the MRP_Prio field of the MRP_Test frame.

If an optional protocol for multiple MRM in a single ring is used then all MRM in the ring shall support the same protocol. The vendor shall specify the supported protocols.

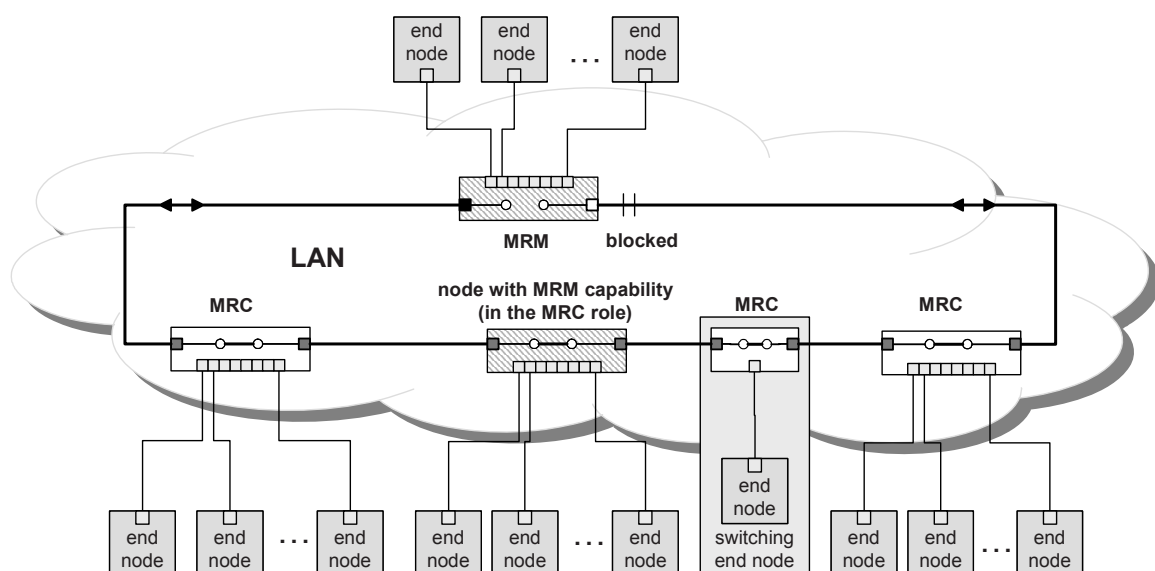


Figure 15 – MRP ring with more than one MRM

5.2.8 BLOCKED not supported (option)

If an MRC is not able to support the BLOCKED port state at its ring ports, the MRC shall report it in the corresponding parameter of the MRP_LinkChange frames.

If an MRC does not support the BLOCKED state in a ring, then a MRM shall support additional functionalities (see Table 28, MRP_BLOCKED_SUPPORTED).

5.3 MRP Class specification

5.3.1 General

The MRP Application Service Element (ASE) defines one object type.

5.3.2 Template

An MRP object is described by the following template:

ASE:		Media redundancy ASE	
CLASS:		Media redundancy	
CLASS ID:		not used	
PARENT CLASS:		IEEE 802.3, IEEE 802.1D	
ATTRIBUTES:			
1.	(m)	Key Attribute:	Domain ID
2.	(m)	Attribute:	Domain Name
3.	(m)	Attribute:	Ring Port 1 ID
4.	(m)	Attribute:	Ring Port 2 ID
5.	(o)	Attribute:	VLAN ID
6.	(m)	Attribute:	Expected Role (MANAGER, CLIENT)
7.	(c)	Constraint:	Expected Role = MANAGER
7.1	(m)	Attribute:	Manager Priority
7.2	(m)	Attribute:	Topology Change Interval
7.3	(m)	Attribute:	Topology Change Repeat Count
7.4	(m)	Attribute:	Short Test Interval
7.5	(m)	Attribute:	Default Test Interval
7.6	(m)	Attribute:	Test Monitoring Count
7.7	(m)	Attribute:	Non-blocking MRC supported (TRUE, FALSE)
7.8	(c)	Constraint:	Non-blocking MRC supported = TRUE
7.8.1	(m)	Attribute:	Test Monitoring Extended Count
7.9	(o)	Attribute:	React on link change (TRUE, FALSE)
7.10	(m)	Attribute:	Check Media Redundancy (TRUE, FALSE)
7.10.1	(c)	Constraint:	Check Media Redundancy = TRUE
7.10.1.1	(m)	Attribute:	Real Role State
7.10.1.2	(m)	Attribute:	Real Ring State
7.10.1.3	(o)	Attribute:	Ring Port 1 Port State
7.10.1.4	(o)	Attribute:	Ring Port 2 Port State
8.	(c)	Constraint:	Expected Role = CLIENT
8.1	(m)	Attribute:	Link Down Interval
8.2	(m)	Attribute:	Link Up Interval
8.3	(m)	Attribute:	Link Change Count
8.4	(o)	Attribute:	Ring Port 1 Port State
8.5	(o)	Attribute:	Ring Port 2 Port State
8.6	(m)	Attribute:	BLOCKED state supported (TRUE, FALSE)
SERVICES:			
1	(m)	OpsService:	Start MRM
2	(m)	OpsService:	Stop MRM
3	(o)	OpsService:	State Change
4	(m)	OpsService:	Start MRC
5	(m)	OpsService:	Stop MRC
6	(o)	OpsService:	Read MRM
7	(o)	OpsService:	Read MRC

5.3.3 Attributes

Domain ID

This key attribute defines the redundancy domain representing the ring the MRP object belongs to. It is set to default domain ID or provided as unique ID by engineering.

Attribute Type: UUID

Domain Name

This attribute defines the redundancy domain representing the ring the Media redundancy object belongs to. It is set to default domain name or provided as unique ID by engineering.

Attribute Type: VisibleString[240]

Ring Port 1 ID

This attribute specifies one port of a switch which is assigned as ring port 1 in the redundancy domain referenced by the value of the attribute Domain ID.

Attribute Type: Unsigned16

Ring Port 2 ID

This attribute specifies another port of a switch different from Ring Port 1 ID which is assigned as ring port 2 in the redundancy domain referenced by the value of the attribute Domain ID.

Attribute Type: Unsigned16

VLAN ID

This optional attribute may be used by the MRP object and specifies its VLAN identifier in the redundancy domain.

Attribute Type: Unsigned16

Expected Role

This attribute specifies the role of the MRP object in the redundancy domain.

Attribute Type: Unsigned16

Allowed Values: MANAGER, CLIENT

Manager Priority

This attribute shall contain the priority of the MRM. A lower value indicates a higher priority, 0x0000 (highest priority) to 0xF000 (lowest priority) in increments of 0x1000.

Attribute Type: Unsigned16

Topology Change Interval

This attribute specifies the interval for sending MRP_TopologyChange frames.

Attribute Type: Unsigned16

Topology Change Repeat Count

This attribute specifies the interval count which controls repeated transmissions of MRP_TopologyChange frames.

Attribute Type: Unsigned16

Short Test Interval

This attribute specifies the short interval for sending MRP_Test frames on ring ports after link changes in the ring.

Attribute Type: Unsigned16

Default Test Interval

This attribute specifies the default interval for sending MRP_Test frames on ring ports.

Attribute Type: Unsigned16

Test Monitoring Count

This attribute specifies the interval count for monitoring the reception of MRP_Test frames.

Attribute Type: Unsigned16

Non-blocking MRC supported

This attribute specifies the ability of the MRM to support MRCs without BLOCKED port state support in the ring.

Attribute Type: Boolean

Test Monitoring Extended Count

This attribute specifies the extended interval count for monitoring the reception of MRP_Test frames.

Attribute Type: Unsigned16

React on link change

This optional attribute specifies whether the MRM reacts on MRP_LinkChange frames or not.

Attribute Type: Boolean

Check Media Redundancy

This attribute specifies whether monitoring of MRM state is enabled (TRUE) or disabled (FALSE) in the redundancy domain.

Attribute Type: Boolean

Real Role State

This attribute specifies the actual role of the MRP object in the redundancy domain.

Attribute Type: Unsigned16

Allowed Values: MANAGER, CLIENT, UNDEFINED

Real Ring State

This attribute specifies the actual ring state of the MRP object in the redundancy domain. The Ring State shall have one of the following values:

OPEN: Ring is open due to link or MRC failure in ring.

CLOSED: Ring is closed (normal operation, no error).

UNDEFINED: Shall be set if the attribute Real Role State contains the value CLIENT (i.e. MRP object was reconfigured to client role).

Attribute Type: Unsigned16

Allowed Values: OPEN, CLOSED, UNDEFINED

Ring Port 1 Port State

This optional attribute specifies the actual port state of Ring Port 1. The Ring Port 1 state shall be specified according to Ring port states in 5.2.1.

Attribute Type: Unsigned16

Allowed values: DISABLED, BLOCKED, FORWARDING

Ring Port 2 Port State

This optional attribute specifies the actual port state of Ring Port 2. The Ring Port 2 state shall be specified according to Ring port states in 5.2.1.

Attribute Type: Unsigned16

Allowed values: DISABLED, BLOCKED, FORWARDING

Link Down Interval

This attribute specifies the interval for sending MRP_LinkDown frames on ring ports.

Attribute Type: Unsigned16

Link Up Interval

This attribute specifies the interval for sending MRP_LinkUp frames on ring ports.

Attribute Type: Unsigned16

Link Change Count

This attribute specifies the MRP_LinkChange frame count which controls repeated transmission of MRP_LinkChange frames.

Attribute Type: Unsigned16

BLOCKED state supported

This attribute specifies whether the MRC supports BLOCKED state at its ring ports or not.

Attribute Type: Boolean

5.4 MRP Service specification

5.4.1 Start MRM

The Start MRM service creates a local instance of the MRM protocol machine.

Table 3 shows the parameters of the service.

Table 3 – MRP Start MRM

Parameter name	Req	Cnf
Argument	M	
Domain ID	M	
Ring Port 1 ID	M	
Ring Port 2 ID	M	
VLAN ID	U	
Manager Priority	U	
Topology Change Interval	U	
Topology Change Repeat Count	U	
Short Test Interval	U	
Default Test Interval	U	
Test Monitoring Count	U	
Non-blocking MRC supported	U	
Test Monitoring Extended Count	U	
React on link change	U	
Check Media Redundancy	U	
Result(+)		S
Domain ID		M
Result(-)		S
Domain ID		M
Error Code		M

Argument

The argument shall convey the service specific parameters of the service request.

Domain ID

This is the key attribute to identify the instance of the protocol machine.

Ring Port 1 ID

This parameter contains the ID of the port which serves as first ring port.

Ring Port 2 ID

This parameter contains the ID of the port which serves as second ring port.

VLAN ID

This optional parameter contains the value for the VLAN identifier.

Manager Priority

This parameter contains the value for the manager priority.

Topology Change Interval

This parameter contains the value of the interval for sending MRP_TopologyChange frames.

Topology Change Repeat Count

This parameter contains the value of the interval count which controls repeated transmissions of MRP_TopologyChange frames.

Short Test Interval

This parameter contains the value of the short interval for sending MRP_Test frames on ring ports after link changes in the ring.

Default Test Interval

This parameter contains the value of the default interval for sending MRP_Test frames on ring ports.

Test Monitoring Count

This parameter contains the value of the interval count for monitoring the reception of MRP_Test frames.

Non-blocking MRC supported

This parameter specifies the ability of the MRM to support MRCs without BLOCKED port state support in the ring.

Test Monitoring Extended Count

This optional parameter contains the value of the extended interval count for monitoring the reception of MRP_Test frames.

React on link change

This optional parameter specifies whether the MRM reacts on MRP_LinkChange frames or not.

Check Media Redundancy

This parameter selects whether monitoring of MRM state is enabled or disabled.

Result(+)

This parameter indicates that the service request succeeded.

Domain ID

This is the key attribute to identify the instance of the protocol machine.

Result(-)

This parameter indicates that the service request failed.

Domain ID

This is the key attribute to identify the instance of the protocol machine.

Error Code

The parameter Result contains the error code of the specific error.

Type: Unsigned16

Allowed Values: DOMAIN_ID_MISMATCH, ROLE_NOT_SUPPORTED, INVALID_RINGPORT

5.4.2 Stop MRM

This service shall be used to stop the MRM protocol machine. Ring port states and switch functionality remain.

Table 4 shows the parameters of the service.

Table 4 – MRP Stop MRM

Parameter name	Req	Cnf
Argument	M	
Domain ID	M	
Result(+)		S
Domain ID		M
Result(-)		S
Domain ID		M
Error Code		M

Argument

The argument shall convey the service specific parameters of the service request.

Domain ID

This is the key attribute to identify the instance of the protocol machine.

Result(+)

This parameter indicates that the service request succeeded.

Domain ID

This is the key attribute to identify the instance of the protocol machine.

Result(-)

This parameter indicates that the service request failed.

Domain ID

This is the key attribute to identify the instance of the protocol machine.

Error Code

The parameter Result contains the error code of the specific error.

Type: Unsigned16

Allowed Values: DOMAIN_ID_MISMATCH

5.4.3 State Change

This service shall be used to indicate a change of the MRP domain state.

Table 5 shows the parameters of the service.

Table 5 – MRP Change State

Parameter name	Ind
Argument	M
Domain ID	M
Error Type List	M

Argument

The argument shall convey the service specific parameters of the service request.

Domain ID

This is the key attribute to identify the instance of the protocol machine.

Error Type List

This attribute consists of the following elements:

Error Type

This attribute identifies a media redundancy error.

Attribute Type: Unsigned16

Allowed Values: MANAGER_ROLE_FAIL, RING_OPEN, MULTIPLE_MANAGERS

Appear

This attribute identifies whether the error appears or disappears.

Attribute Type: Boolean

Allowed Values: TRUE, FALSE

5.4.4 Start MRC

The Start MRC service creates an instance of the MRC protocol machine.

Table 6 shows the parameters of the service.

Table 6 – MRP Start MRC

Parameter name	Req	Cnf
Argument	M	
Domain ID	M	
Ring Port 1 ID	M	
Ring Port 2 ID	M	
VLAN ID	U	
Link Down Interval	U	
Link Up Interval	U	
Link Change Count	U	
BLOCKED state supported	U	
Result(+)		S
Domain ID		M
Result(-)		S
Domain ID		M
Error Code		M

Argument

The argument shall convey the service specific parameters of the service request.

Domain ID

This is the key attribute to identify the instance of the protocol machine.

Ring Port 1 ID

This parameter contains the ID of the port which serves as first ring port.

Ring Port 2 ID

This parameter contains the ID of the port which serves as second ring port.

VLAN ID

This optional parameter contains the value for the VLAN identifier.

Link Down Interval

This parameter contains the value of the interval for sending MRP_LinkDown frames on ring ports.

Link Up Interval

This parameter contains the value of the interval for sending MRP_LinkUp frames on ring ports.

Link Change Count

This parameter contains the value of the MRP_LinkChange frame count which controls repeated transmissions of MRP_LinkUp or MRP_LinkDown frames.

BLOCKED state supported

This parameter specifies whether the MRC supports BLOCKED state at its ring ports or not.

Result(+)

This parameter indicates that the service request succeeded.

Domain ID

This is the key attribute to identify the instance of the protocol machine.

Result(-)

This parameter indicates that the service request failed.

Domain ID

This is the key attribute to identify the instance of the protocol machine.

Error Code

The parameter result contains the error code of the specific error.

Type: Unsigned16

Allowed Values: DOMAIN_ID_MISMATCH, ROLE_NOT_SUPPORTED, INVALID_RINGPORT

5.4.5 Stop MRC

This service shall be used to stop the MRC protocol machine. Ring port states and switch functionality remain. Table 7 shows the parameters of the service.

Table 7 – MRP Stop MRC

Parameter name	Req	Cnf
Argument	M	
Domain ID	M	
Result(+)		S
Domain ID		M
Result(-)		S
Domain ID		M
Error Code		M

Argument

The argument shall convey the service specific parameters of the service request.

Domain ID

This is the key attribute to identify the instance of the protocol machine.

Result(+)

This parameter indicates that the service request succeeded.

Domain ID

This is the key attribute to identify the instance of the protocol machine.