IEC 62439-5

Edition 1.0 2010-02

INTERNATIONAL STANDARD

colour inside

Industrial communication networks – High availability automation networks – Part 5: Beacon Redundancy Protocol (BRP)

IEC 62439-5:2010(E)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: 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.

- Catalogue of IEC publications: www.iec.ch/searchpub
The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub
Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv
If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC 62439-5

Edition 1.0 2010-02

INTERNATIONAL STANDARD

colour inside

Industrial communication networks – High availability automation networks – Part 5: Beacon Redundancy Protocol (BRP)

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE X

ICS 25.040, 35.040

ISBN 2-8318-1081-5

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

INDUSTRIAL COMMUNICATION NETWORKS – HIGH AVAILABILITY AUTOMATION NETWORKS –

Part 5: Beacon Redundancy Protocol (BRP)

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 62439-5 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.

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.

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.

A bilingual version of this standard may be issued at a later date.

IMPORTANT – The "colour inside" logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this publication using a colour printer.

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 fault-tolerant Ethernet provided through the use of special interfaces providing duplicate ports that may be alternatively enabled with the same network address. Switching between the ports corrects for single faults in a two-way redundant system. This is given in Clauses 5 and 6.

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:

Rockwell Automation Technologies

1 Allen-Bradley Drive

Mayfield Heights

Ohio

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 5: Beacon Redundancy Protocol (BRP)

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. Fast error detection is provided by two beacon nodes, the switchover decision is taken in every 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/TR 8802-1, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 1: Overview of Local Area Network Standards* (IEEE 802.1)

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*

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

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

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:

BRP Beacon Redundancy Protocol

DANB Double attached node implementing BRP

3.3 Conventions

This part of the IEC 62439 series follows the conventions defined in IEC 62439-1.

4 BRP overview

This clause specifies a protocol for an Ethernet network tolerant to all single point failures. This protocol is called Beacon Redundancy Protocol or BRP. A network based on the BRP is called a BRP network. The BRP network is based on switched ISO/IEC 8802-3 (IEEE 802.3) (Ethernet) and ISO/IEC/TR 8802-1 (IEEE 802.1) technologies and redundant infrastructure. In this network, the decision to switch between infrastructures is made individually in each end node.

5 BRP principle of operation

5.1 General

Subclauses 5.2 to 5.4 are an explanation of overall actions performed by the BRP state machine. If a difference in the interpretation occurs between these subclauses and the state machines in 7, then the state machines take precedence.

5.2 Network topology

The BRP network topology can be described as two interconnected top switches, each heading an underlying topology of star, line, or ring. Beacon end nodes shall be connected to the top switches. Examples of star, linear and ring BRP networks are shown in Figure 1, Figure 2 and Figure 3 respectively.

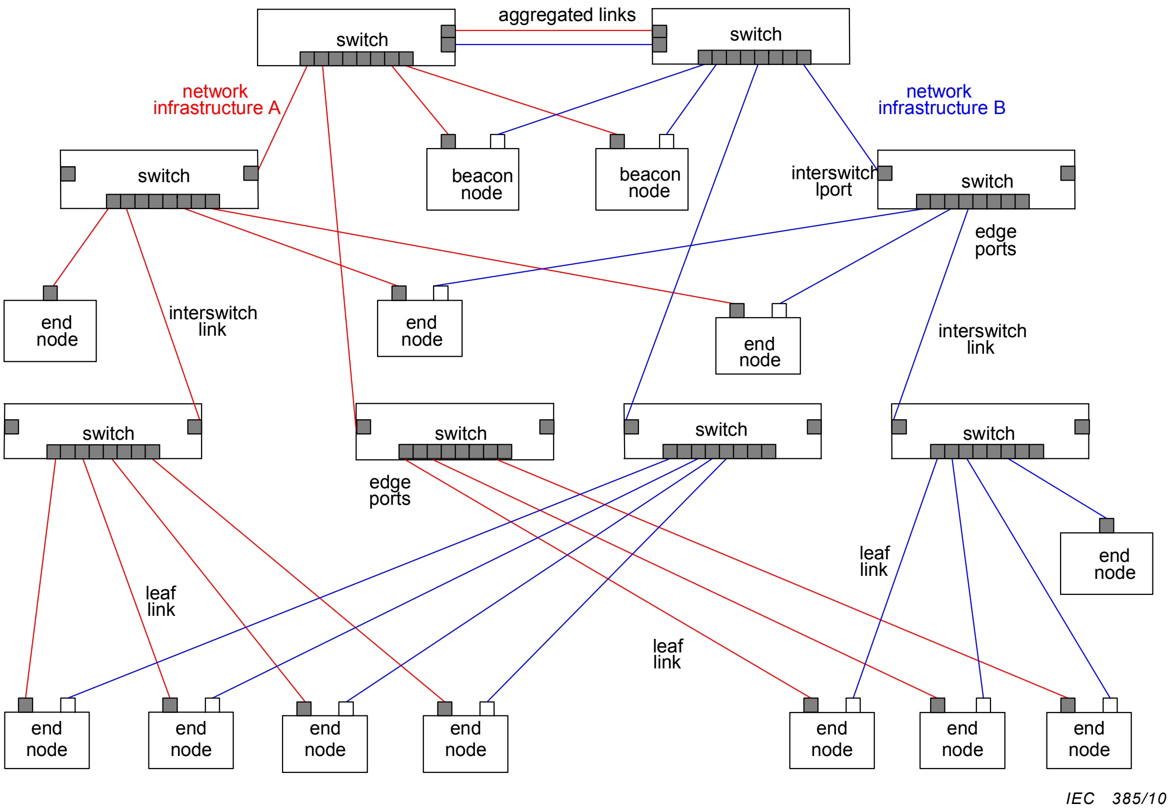

Figure 1 – BRP star network example

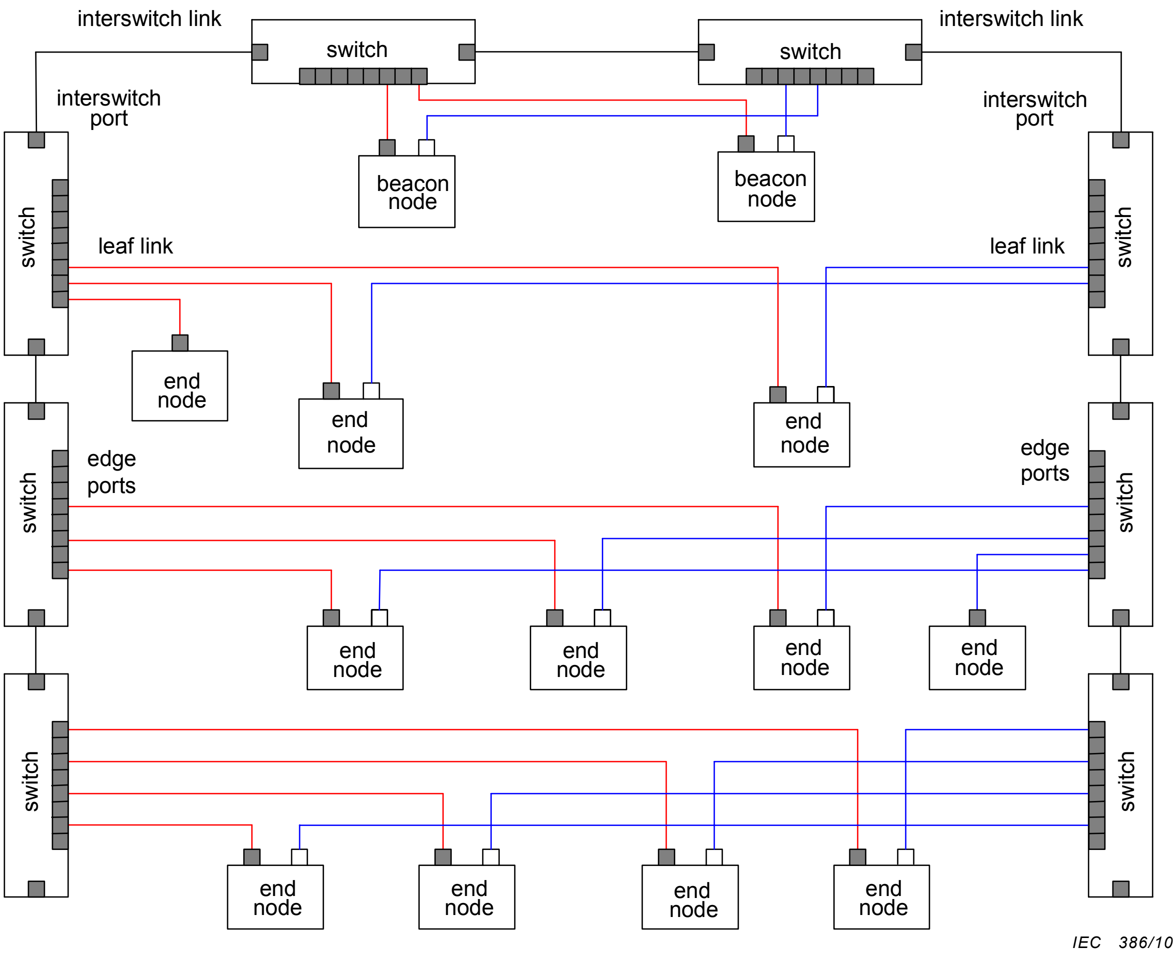

Figure 2 – BRP linear network example

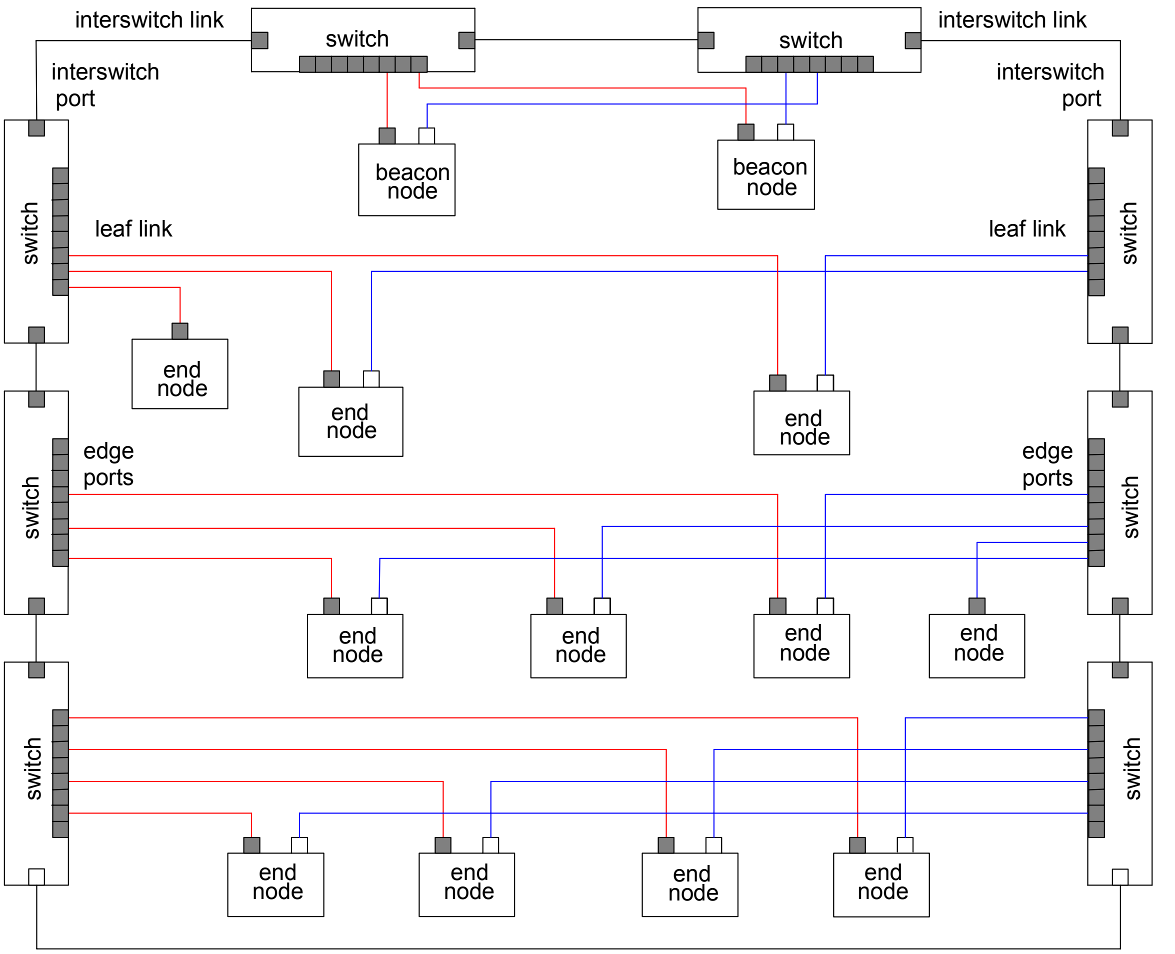

Figure 3 – BRP ring network example

5.3 Network components

The BRP network is built from layer 2 switches compliant with IEEE 802.1D and ISO/IEC 8802-3 (IEEE 802.3). No support of the BRP protocol in switches is required.

Figure 1 shows an example of a BRP star network in the 2-way redundancy mode. It uses two sets of network infrastructure A and B (shown in two different colours). The number of levels of switches and number of switches on each level are dependent only on application requirements. Even with three levels of hierarchy it is possible to construct very large networks. For example, a BRP star network built from switches with eight regular ports and one uplink port can contain 500 nodes maximum. Two switches at the top level shall be connected to each other with one or more links providing sufficient bandwidth. With link aggregation capability, traffic is shared among bundle of links and failure of one link does not bring the network down. With such an arrangement infrastructures A and B form a single network.

Two types of end nodes can be connected to the BRP network: doubly attached and singly attached. A doubly attached end node can function as a BRP end node or a BRP beacon end node. A BRP beacon end node is a special case of a doubly attached end node that is connected directly to the top switches. Though doubly attached BRP end nodes have two network ports they use only one MAC address.

At any given point in time a BRP end node actively communicates through only one of its ports, while blocking all transmit and receive traffic on its other port, with the exception of received beacon messages and Failure_Notify messages. Fault tolerance is achieved in a distributed fashion by BRP end nodes switching between their ports from inactive to active mode and vice versa.

As shown in Figure 1, Figure 2 and Figure 3, two beacon end nodes shall be connected to top level switches. Beacon end nodes multi/broadcast a short beacon message on the network periodically. Similarly to BRP end nodes, beacon end node at any given point in time actively communicates through only one of its ports, while blocking all traffic on its other port, with the exception of received Failure_Notify messages. Fault tolerance is achieved by beacon end nodes switching between their ports from inactive to active mode and vice versa.

Singly attached end nodes may also be connected to BRP network but they do not support the BRP protocol. A singly attached node can communicate with doubly attached nodes as well as other singly attached nodes on the network.

Since switches are IEEE 802.1D compliant, they support the RSTP protocol. This eliminates loop formation in BRP ring networks like in the one shown in Figure 3.

5.4 Rapid reconfiguration of network traffic

For fast reconfiguration, multicast control features in the switches shall be disabled. The multicast traffic is therefore treated as the broadcast traffic.

Unicast packets are affected by switches learning and filtering features. After end node port reconfiguration, switches have invalid knowledge. A switch implementing learning shall update its database when a packet with a learned MAC address in the source field is received on a different port from the learned port stored in the database.

When a BRP end node switches to the inactive port, its first action is to send a short multicast message, called Learning_Update message, through its newly enabled port. As this message propagates through the network, switches update their MAC address database resulting in rapid reconfiguration of the unicast traffic. This message is of no interest to other end nodes in the network and is dropped by them.

6 BRP stack and fault detection features

Figure 4 shows the BRP stack architecture. It is applicable to both BRP and beacon end nodes.

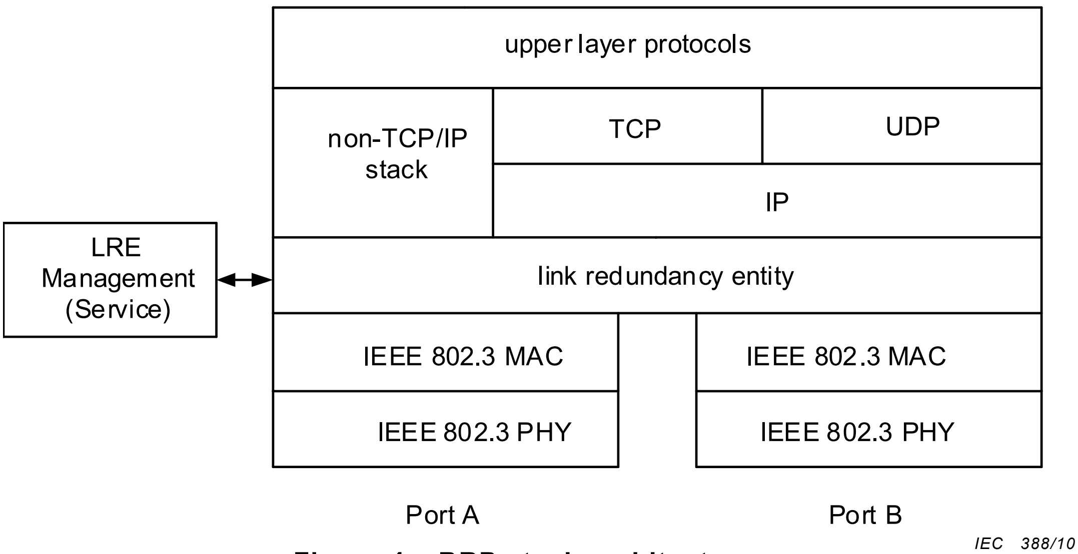

Figure 4 – BRP stack architecture

The BRP stack contains two identical ISO/IEC 8802-3 (IEEE 802.3) ports, identified here as ports A and B, connected to the network. These ports interface with the MAC sub-layer compliant with ISO/IEC 8802-3 (IEEE 802.3). Though there are two physical ports, a BRP end node uses only a single MAC address.

The link redundancy entity continuously monitors the status of leaf links between both ports and corresponding ports on the switches. When a failure of the leaf link between the end node active port and the corresponding port on the switch is detected, the link redundancy entity shall reconfigure end node ports, provided the inactive port was not in the fault mode as well. After reconfiguration, all traffic flows through the newly activated port. Some messages may be lost during the failure detection and reconfiguration process, and their recovery is supported by upper layer protocols which also deal with messages lost due to other network errors.

The link redundancy entity also monitors arrival of beacon messages on both ports. When a beacon message fails to arrive at the active port for a configured timeout period, the port is declared to be in the fault mode, and the link redundancy entity shall reconfigure end node ports, provided the other port was not in the fault mode as well. After reconfiguration all traffic starts flowing through newly activated port. Failure of beacon messages to arrive at inactive ports shall also be detected.

If one of the top switches fails, then all BRP nodes connected directly to it, or to network infrastructure below it, switch to the other network infrastructure. If, for example, the top switch of the LAN A fails, then all BRP nodes connected to LAN A switch over to LAN B.

If the fault occurred on a beacon end node, the network continues to operate without any problems, since the other beacon end node is active. The rate of beacon message arrival decreases from approximately two messages per beacon timer interval to one.

It is possible for transmit path failures to occur in the opposite direction to the flow of beacon messages. If such a fault manifests itself in the physical layer, it is detected by end nodes or switches adjacent to the faulty link. This results in a BRP end node reconfiguring its ports immediately or results in traffic being blocked on the affected link. The latter event leads to loss of beacon messages at the downstream end nodes, so they reconfigure themselves at expiry of the beacon timeout.

In a case when such failures are not detectable in the physical layer, the following mechanism is employed by the BRP link redundancy entity to detect them. The fault detection method for identifying all transmission failures shall be implemented using lists of communication nodes including a receive timeout value for each transmitting end node of interest to the node. This list may be communicated to the link redundancy entity manually or dynamically configured utilizing LRE management entity.

When a frame from a transmitting end node of interest fails to arrive before expiry of the associated Node_Receive timer, the receiving end node shall send a Failure_Notify message to the transmitting end node and send a Path_Check_Request message to beacon end nodes. Upon reception of a Failure_Notify message, the transmitting end node shall attempt to verify the transmit path by sending the Path_Check_Request message to beacon end nodes. When beacon end nodes receive these messages, they shall respond with Path_Check_Response messages. When Path_Check_Request fails to elicit response, an end node shall place its active port in faulted state and activate its inactive port, provided it is not in fault mode as well.

BRP beacon end nodes also behave in a similar way. When a frame from a transmitting end node of interest fails to arrive before expiry of the associated Node_Receive timer, the receiving beacon end node shall send a Failure_Notify message to the transmitting end node and send a Path_Check_Request message to a designated set of end nodes. When beacon end nodes receive Failure_Notify messages themselves, they shall verify their transmit path by sending a Path_Check_Request message to a designated set of end nodes. Upon receiving Path_Check_Request message, the designated end nodes shall respond with

Path_Check_Response message. When Path_Check_Request fails to elicit response, a beacon end node shall place its active port in faulted state and activate its inactive port, provided it is not in fault mode as well.

When the faulted port is restored, it shall stay idle until a switchover is initiated or the currently active port fails. When both ports are operational, the BRP end node shall periodically switch its message activity from one port to the other. This switchover is controlled by the Active_Port_Swap timer.

The LRE management entity is used to select an end node type (normal or beacon), configure protocol parameters (for example, beacon timer) and obtain the end node port status (active, failed, idle).

All detected failures shall be reported to the LRE management entity to trigger further diagnosis and repair. Fault diagnostics services shall be provided by LRE management entity or other accessible entities in the network.

7 BRP protocol specification

7.1 MAC addresses

BRP protocol shall use multicast address 01-15-4E-00-02-01. Both ports of a BRP node shall have the same MAC address for active communication.

7.2 EtherType

The BRP protocol shall use assigned EtherType 0x80E1.

7.3 Fault detection mechanisms

The following fault detection mechanisms are used:

- Link fault detection

  This mechanism covers physical layer failures in transmit and receive directions on a link directly connected to the end node.
- Receive path fault detection

  This is accomplished utilizing the beacon message transmission mechanism.
- Transmit path fault detection

  This is accomplished utilizing Failure_Notify, Path_Check_Request, and Path_Check_Response messages. The periodic switchover between active and inactive ports ensures coverage of all transmit paths in the network.

7.4 End node state diagram

The BRP end node state diagram is shown in Figure 5.

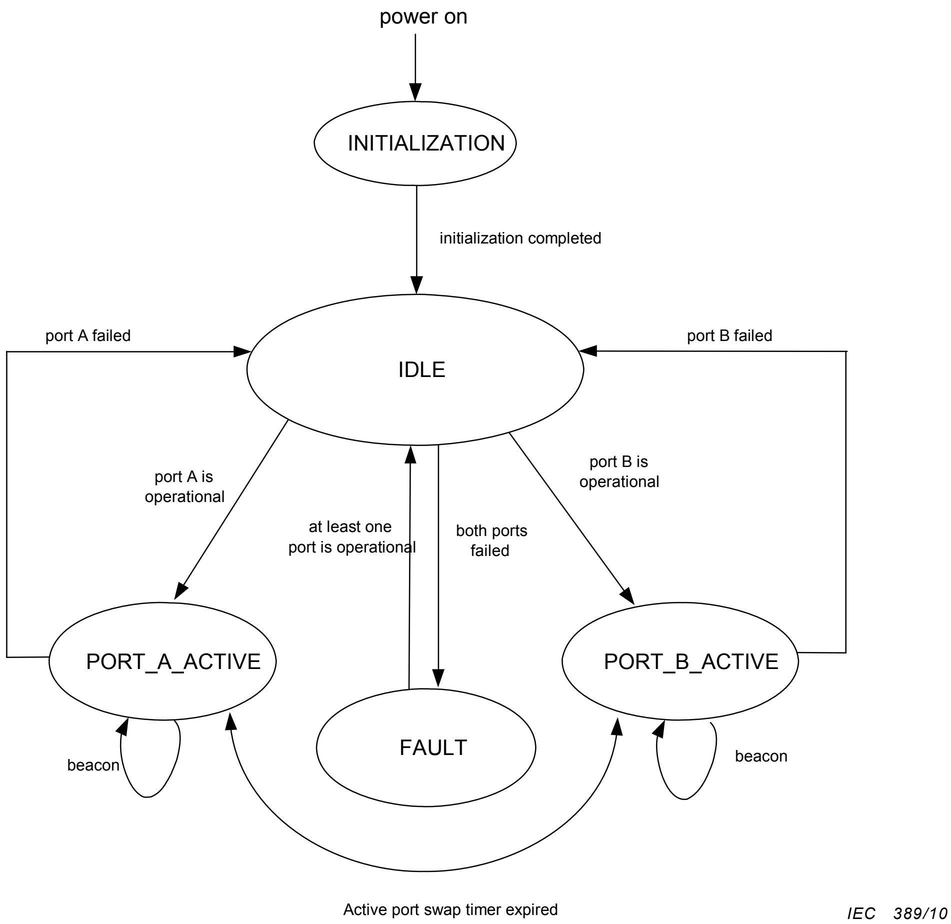

Figure 5 – BRP state diagram of end node

The BRP end node protocol state machine shall perform in accordance with the state transition table presented in Table 2.

When the node is powered up and passed the initialization process (the Initialization_Completed flag is set), it resets the protocol state machine and transitions to the IDLE state.

Since Port_A_Failed and Port_B_Failed flags were initially set, the node immediately transitions from the IDLE to the FAULT state.

If link A is active and a beacon message is received on this link, then the node transitions from the FAULT state back to the IDLE. A Learning_Update message is generated on this port and the node transitions from the IDLE to the PORT_A_ACTIVE state.

The node tests port B simultaneously with port A using the procedure described above. If both ports are operational, either one can be selected as the default.

Periodic reception of beacon messages (Beacon_A_Received is set) keeps the node in the PORT_A_ACTIVE state and trigger reset of the No_Beacon_A timer.

If, when in the PORT_A_ACTIVE state, link A becomes inactive (Link_A_Active is reset) or no beacon messages were received for a given time period (No_Beacon_A timer expired and Beacon_A_Received is reset), the node sets the Port_A_Failed flag and transitions to the IDLE state where it attempts to switch to port B.

Operation of port B is identical to operation of port A.

If a Node_Receive timer expires, the receiving node sends a Failure_Notify message to the associated transmitting end node and sends Path_Check_Request message on its active port to beacon end nodes. When the transmitting end node receives the Failure_Notify message, it attempts to verify transmission path on its active port by sending a Path_Check_Request message on this port to beacon end nodes. When beacon nodes receive these messages, they issue Path_Check_Response messages addressed to the requesting node.

When Path_Check_Request fails to elicit response (Path_A_Check/Path_B_Check timer expired), the node sets the Path_A_Failed/Path_B_Failed flag and Port_A_Failed/ Port_B_Failed flag, and transitions to the IDLE state where it attempts to switch to port B/A.

If both ports failed, then the node transitions from the IDLE to the FAULT state and stays there until one of the ports becomes operational. In FAULT state, a node continuously monitors link status (Link_A_Active/Link_B_Active flags) and beacon arrival status (Beacon_A_Received/Beacon_B_Received flags). If Path_A_Failed and/or Path_B_Failed flags were set, the node also sends Path_Check_Request and monitors arrival of Path_Check_Response message for corresponding ports. When one of the ports becomes operational (Port_A_Failed/Port_B_Failed is reset), the node transitions back to the IDLE state and then to PORT_A_ACTIVE/PORT_B_ACTIVE as appropriate.

When a node receives a Path_Check_Request message in PORT_A_ACTIVE or PORT_B_ACTIVE states, it responds with the Path_Check_Response message and stays in current state.

When in PORT_A_ACTIVE/PORT_B_ACTIVE state and the Active_Port_Swap timer expires, the node transitions to PORT_B_ACTIVE/PORT_A_ACTIVE state provided PORT_B_FAILED/PORT_A_FAILED is not set.

The No_Beacon timer period is a configuration parameter selected for a specific system. The mandatory default value of the beacon period is 450 μs, resulting in the default value of the No_Beacon period of 950 μs. The timeout period is chosen in such a way that at least two beacon messages from each beacon end node have to be lost before fault is declared on a port.

A BRP compliant end node shall be able to receive beacon messages over both of its ports sent from both beacon end nodes at the mandatory default value of the beacon period.

The Path_A_Check and Path_B_Check timer periods are configuration parameters selected for a specific system. The mandatory default value is 2 ms.

The Active_Port_Swap timer period is a configuration parameter selected for a specific system. The mandatory default value is 1 h.

Table 1 specifies the flags used in the BRP end node state machine.

Table 1 – BRP end node flags

Name	Description	Data Type
Initialization_Completed	Used to indicate initialization completed successfully	BOOL
Link_A_Active	Used to indicate physical layer link status of port A	BOOL
Beacon_A_Received	Used to indicate beacon message was received on port A	BOOL
Path_A_Failed	Used to indicate if Path_Check_Response message was received for Path_Check_Request message on port A	BOOL
Link_B_Active	Used to indicate physical layer link status of port B	BOOL
Beacon_B_Received	Used to indicate beacon message was received on port B	BOOL
Path_B_Failed	Used to indicate if Path_Check_Response message was received for Path_Check_Request message on port B	BOOL
Path_A_Request	Used to indicate if Path_Check_Request message was sent on port A	BOOL
Path_B_Request	Used to indicate if Path_Check_Request message was sent on port B	BOOL
Port_A_Failed	Used to indicate if port A has failed	BOOL
Port_B_Failed	Used to indicate if port B has failed	BOOL
NOTE In this table, BOOL means Boolean.		

Table 2 specifies the BRP end node state transition table.

Table 2 – BRP end node state transition table

State number	Current state	Event /Condition =>Action	Next state
1	INITIALIZATION	**Initialization is completed** => Set Initialization_Completed Reset Link_A_Active Reset Beacon_A_Received Stop No_Beacon_A timer Reset Path_A_Failed Stop Path_A_Check timer, reset Path_A_Request Reset Link_B_Active Reset Beacon_B_Received Stop No_Beacon_B timer Reset Path_B_Failed Stop Path_B_Check timer Reset Path_B_Request Set Port_A_Failed Set Port_B_Failed Stop Node_Receive timers Stop Active_Port_Swap timer	IDLE
2	IDLE, FAULT, PORT_A_ACTIVE, PORT_B_ACTIVE	**Port A link pass status** => Set Link_A_Active	STAY IN CURRENT STATE
3	IDLE, FAULT, PORT_A_ACTIVE, PORT_B_ACTIVE	**Port A link fail status** => Reset Link_A_Active	STAY IN CURRENT STATE
4	IDLE, FAULT, PORT_A_ACTIVE, PORT_B_ACTIVE	**Port B link pass status** => Set Link_B_Active	STAY IN CURRENT STATE
5	IDLE, FAULT, PORT_A_ACTIVE, PORT_B_ACTIVE	**Port B link fail status** => Reset Link_B_Active	STAY IN CURRENT STATE
6	IDLE, FAULT, PORT_A_ACTIVE, PORT_B_ACTIVE	**Beacon message received on port A** => Set Beacon_A_Received Start No_Beacon_A timer	STAY IN CURRENT STATE
7	IDLE, FAULT, PORT_A_ACTIVE, PORT_B_ACTIVE	**No_Beacon_A timer expired** => Reset Beacon_A_Received	STAY IN CURRENT STATE
8	IDLE, FAULT, PORT_A_ACTIVE, PORT_B_ACTIVE	**Beacon message received on port B** => Set Beacon_B_Received Start No_Beacon_B timer	STAY IN CURRENT STATE
9	IDLE, FAULT, PORT_A_ACTIVE,	**No_Beacon_B timer expired** =>	STAY IN CURRENT STATE

State number	Current state	Event /Condition =>Action	Next state
	PORT_B_ACTIVE	Reset Beacon_B_Received	
10	PORT_A_ACTIVE	**Failure_Notify message is received** => Send Path_Check_Request message on Port A Set Path_A_Request Start Path_A_Check timer	PORT_A_ACTIVE
11	PORT_B_ACTIVE	**Failure_Notify message is received** => Send Path_Check_Request message on port B Set Path_B_Request Start Path_B_Check timer	PORT_B_ACTIVE
12	PORT_A_ACTIVE, FAULT	**Path_A_Check timer expired** => Set Path_A_Failed Reset Path_A_Request	STAY IN CURRENT STATE
13	PORT_B_ACTIVE, FAULT	**Path_B_Check timer expired** => Set Path_B_Failed Reset Path_A_Request	STAY IN CURRENT STATE
14	PORT_A_ACTIVE, FAULT	**Path_Check_Response message is received on port A** => Stop Path_A_Check timer Reset Path_A_Failed Reset Path_A_Request	STAY IN CURRENT STATE
15	PORT_B_ACTIVE, FAULT	**Path_Check_Response message is received on port B** => Stop Path_B_Check timer Reset Path_B_Failed Reset Path_B_Request	STAY IN CURRENT STATE
16	IDLE, FAULT, PORT_A_ACTIVE, PORT_B_ACTIVE	**Link_A_Active is set** **AND** **Beacon_A_Received is set** **AND** **Path_A_Failed is reset** => Reset Port_A_Failed	STAY IN CURRENT STATE
17	IDLE, FAULT, PORT_A_ACTIVE, PORT_B_ACTIVE	**Link_A_Active is reset** **OR** **Beacon_A_Received is reset** **OR** **Path_A_Failed is set** => Set Port_A_Failed	STAY IN CURRENT STATE
18	IDLE	**Port_A_Failed is reset** => Send Learning_Update message on port A Start Node_Receive timers	PORT_A_ACTIVE

State number	Current state	Event /Condition =>Action	Next state
		Start Active_Port_Swap timer	
19	PORT_A_ACTIVE	**Port_A_Failed is set** => Stop Path_A_Check timer Reset Path_A_Request Stop Node_Receive timers Stop Active_Port_Swap timer	IDLE
20	IDLE, FAULT, PORT_A_ACTIVE, PORT_B_ACTIVE	**Link_B_Active is set** **AND** **Beacon_B_Received is set** **AND** **Path_B_Failed is reset** => Reset Port_B_Failed	STAY IN CURRENT STATE
21	IDLE, FAULT, PORT_A_ACTIVE, PORT_B_ACTIVE	**Link_B_Active is reset** **OR** **Beacon_B_Received is reset** **OR** **Path_B_Failed is set** => Set Port_B_Failed	STAY IN CURRENT STATE
22	IDLE	**Port_B_Failed is reset** => Send Learning_Update message on port B Start Node_Receive timers Start Active_Port_Swap timer	PORT_B_ACTIVE
23	PORT_B_ACTIVE	**Port_B_Failed is set** => Stop Path_B_Check timer Reset Path_B_Request Stop Node_Receive timers Stop Active_Port_Swap timer	IDLE
24	IDLE	**Port_A_Failed is set** **AND** **Port_B_Failed is set**	FAULT
25	FAULT	**Link_A_Active is set** **AND** **Beacon_A_Received is set** **AND** **Path_A_Failed is set** **AND** **Path_A_Request is reset** => Set Path_A_Request Send Path_Check_Request message on port A Start Path_A_Check timer	FAULT
26	FAULT	**Link_B_Active is set** **AND** **Beacon_B_Received is set** **AND** **Path_B_Failed is set** **AND** **Path_B_Request is reset**	FAULT

State number	Current state	Event /Condition =>Action	Next state
		=> Set Path_B_Request Send Path_Check_Request message on port B Start Path_B_Check timer	
27	FAULT	**Port_A_Failed is reset** **OR** **Port_B_Failed is reset**	IDLE
28	PORT_A_ACTIVE, PORT_B_ACTIVE	**Path_Check_Request message received on active port** => Send Path_Check_Response message on active port	STAY IN CURRENT STATE
29	PORT_A_ACTIVE, PORT_B_ACTIVE	**Frame received from transmit node of interest on active port** => Restart associated Node_Receive timer	STAY IN CURRENT STATE
30	PORT_A_ACTIVE	**Node_Receive timer expired** => Send Failure_Notify message on port A to associated transmit node Send Path_Check_Request message on port A Set Path_A_Request Start Path_A_Check timer	PORT_A_ACTIVE
31	PORT_B_ACTIVE	**Node_Receive timer expired** => Send Failure_Notify message on port B to associated transmit node Send Path_Check_Request message on port B Set Path_B_Request Start Path_B_Check timer	PORT_B_ACTIVE
32	PORT_A_ACTIVE	**Active_Port_Swap timer expired** **AND** **Port_B_Failed is reset** => Stop Path_A_Check timer Reset Path_A_Request Send Learning_Update message on port B Start Active_Port_Swap timer	PORT_B_ACTIVE
33	PORT_A_ACTIVE	**Active_Port_Swap timer expired** **AND** **Port_B_Failed is set** => Start Active_Port_Swap timer	PORT_A_ACTIVE
34	PORT_B_ACTIVE	**Active_Port_Swap timer expired** **AND** **Port_A_Failed is reset** => Stop Path_B_Check timer	PORT_A_ACTIVE

State number	Current state	Event /Condition =>Action	Next state
		Reset Path_B_Request Send Learning_Update message on port A Start Active_Port_Swap timer	
35	PORT_B_ACTIVE	**Active_Port_Swap timer expired** **AND** **Port_A_Failed is set** => Start Active_Port_Swap timer	PORT_B_ACTIVE

7.5 Beacon end node state diagram

If the end node is configured as a beacon, it periodically generates beacon messages. The Beacon end node state diagram is shown in Figure 6.

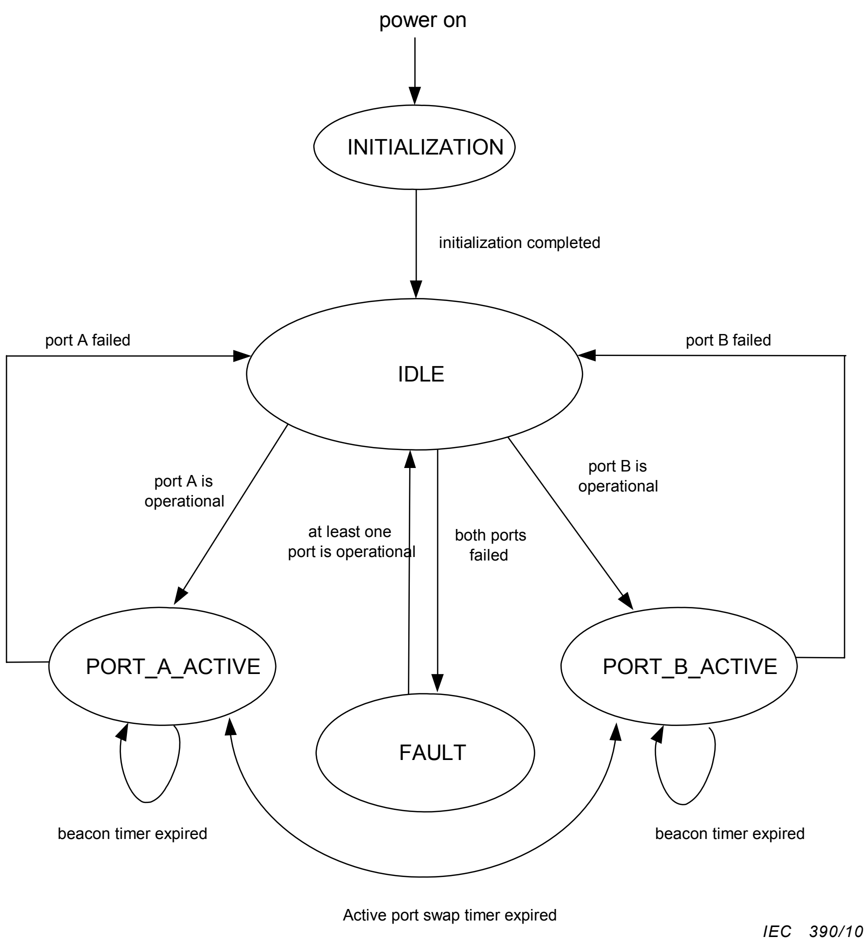

Figure 6 – BRP state diagram for beacon end node

When the beacon end node is powered up and passed the initialization process (the Initialization_Completed flag is set), it resets the protocol state machine and transitions to the IDLE state.

Since Port_A_Failed and Port_B_Failed flags were initially set, the node immediately transitions from the IDLE to the FAULT state.

If link A is active, then the node transitions from the FAULT state back to the IDLE. The node then generates a beacon message on port A, starts the beacon timer and transitions to the PORT_A_ACTIVE state.

The node tests port B simultaneously with port A executing procedure identical to the one described above. If both ports are operational, either one can be selected by default.

When the beacon timer expires, the node transmits the beacon message, restarts the beacon timer and continues staying in the PORT_A_ACTIVE state.

If, when in the PORT_A_ACTIVE state, link A becomes inactive (Link_A_Active is reset), the node sets the Port_A_Failed flag, stops the beacon timer and transitions to the IDLE state where it attempts to switch to port B.

Operation of port B is identical to operation of port A.

If a Node_Receive_Timer expires, the receiving beacon end node sends a Failure_Notify message to the associated transmitting end node and sends Path_Check_Request message on its active port to designated set of end nodes. When the transmitting end node receives the Failure_Notify message, it attempts to verify transmission path as described in 7.4.

When a beacon end node receives Failure_Notify message, it attempts to verify transmission path on its active port by sending Path_Check_Request message on this port to designated set of nodes. When the designated set of nodes receives this message, they respond with Path_Check_Response message.

When Path_Check_Request fails to elicit response (Path_A_Check/Path_B_Check timer expired), the node sets the Path_A_Failed/Path_B_Failed flag and Port_A_Failed/ Port_B_Failed flag, and transitions to the IDLE state where it attempts to switch to port B/A.

If both ports failed, then the node transitions from the IDLE to the FAULT state and stays there until one of the ports becomes operational. In FAULT state, a node continuously monitors link status (Link_A_Active/Link_B_Active flags). If Path_A_Failed and/or Path_B_Failed flags were set, the node also sends Path_Check_Request and monitors arrival of Path_Check_Response message for corresponding ports. When one of the ports becomes operational (Port_A_Failed/Port_B_Failed is reset) the node transitions back to the IDLE state and then to PORT_A_ACTIVE/PORT_B_ACTIVE as appropriate.

When a node receives a Path_Check_Request message in PORT_A_ACTIVE or PORT_B_ACTIVE states, it responds with the Path_Check_Response message and stays in current state.

When in PORT_A_ACTIVE/PORT_B_ACTIVE state and the Active_Port_Swap timer expires, the node transitions to PORT_B_ACTIVE/PORT_A_ACTIVE state provided PORT_B_FAILED/PORT_A_FAILED is not set.

The No_Beacon timer period is a configuration parameter selected for a specific system. The mandatory default value of the beacon period is 450 μs resulting in the default value of the No_Beacon period of 950 μs. The timeout period is chosen in such a way that at least two beacon messages from each beacon end node have to be lost before fault is declared on a port.

A BRP compliant beacon end node shall be able to broadcast the beacon message every 450 ms via its active port.

The Path_A_Check and Path_B_Check timer periods are configuration parameters selected for a specific system. The mandatory default value is 2 ms.

The Active_Port_Swap timer period is a configuration parameter selected for a specific system. The mandatory default value is 1 h.

Table 3 specifies the flags used in the BRP beacon end node state machine.

Table 3 – BRP beacon end node flags

Name	Description	Data Type
Initialization_Completed	Used to indicate initialization completed successfully	BOOLEAN
Link_A_Active	Used to indicate physical layer link status of port A	BOOLEAN
Path_A_Failed	Used to indicate if Path_Check_Response message was received for Path_Check_Request message on port A	BOOLEAN
Link_B_Active	Used to indicate physical layer link status of port B	BOOLEAN
Path_B_Failed	Used to indicate if Path_Check_Response message was received for Path_Check_Request message on port B	BOOLEAN
Path_A_Request	Used to indicate if Path_Check_Request message was sent on port A	BOOLEAN
Path_B_Request	Used to indicate if Path_Check_Request message was sent on port B	BOOLEAN
Port_A_Failed	Used to indicate if port A has failed	BOOLEAN
Port_B_Failed	Used to indicate if port B has failed	BOOLEAN

Table 4 specifies the BRP beacon end node state transition table.

Table 4 – BRP beacon end node state transition table

State number	Current state	Event /Condition =>Action	Next state
1	INITIALIZATION	**Initialization is completed** => Set Initialization_Completed Reset Link_A_Active Reset Path_A_Failed Stop Path_A_Check timer Reset Path_A_Request Reset Link_B_Active Reset Path_B_Failed Stop Path_B_Check timer Reset Path_B_Request Set Port_A_Failed Set Port_B_Failed Stop Node_Receive timers Stop Active_Port_Swap timer	IDLE
2	IDLE, FAULT, PORT_A_ACTIVE, PORT_B_ACTIVE	**Port A link pass status** => Set Link_A_Active	STAY IN CURRENT STATE
3	IDLE, FAULT, PORT_A_ACTIVE, PORT_B_ACTIVE	**Port A link fail status** => Reset Link_A_Active	STAY IN CURRENT STATE
4	IDLE, FAULT, PORT_A_ACTIVE, PORT_B_ACTIVE	**Port B link pass status** => Set Link_B_Active	STAY IN CURRENT STATE
5	IDLE, FAULT, PORT_A_ACTIVE, PORT_B_ACTIVE	**Port B link fail status** => Reset Link_B_Active	STAY IN CURRENT STATE
6	PORT_A_ACTIVE, PORT_B_ACTIVE	**Frame received from transmit node of interest on active port** => Restart associated Node_Receive timer	STAY IN CURRENT STATE
7	PORT_A_ACTIVE	**Node_Receive timer expired** => Send Failure_Notify message on port A to associated transmit node Send Path_Check_Request message on port A Set Path_A_Request Start Path_A_Check timer	PORT_A_ACTIVE
8	PORT_B_ACTIVE	**Node_Receive timer expired** => Send Failure_Notify message on port B to associated transmit node Send Path_Check_Request message on port B Set Path_B_Request Start Path_B_Check timer	PORT_B_ACTIVE

State number	Current state	Event /Condition =>Action	Next state
9	PORT_A_ACTIVE	**Failure_Notify message is received** => Send Path_Check_Request message on port A Set Path_A_Request Start Path_A_Check timer	PORT_A_ACTIVE
10	PORT_B_ACTIVE	**Failure_Notify message is received** => Send Path_Check_Request message on port B Set Path_B_Request Start Path_B_Check timer	PORT_B_ACTIVE
11	PORT_A_ACTIVE, FAULT	**Path_A_Check timer expired** => Set Path_A_Failed Reset Path_A_Request	STAY IN CURRENT STATE
12	PORT_B_ACTIVE, FAULT	**Path_B_Check timer expired** => Set Path_B_Failed Reset Path_A_Request	STAY IN CURRENT STATE
13	PORT_A_ACTIVE, FAULT	**Path_Check_Response message is received on port A** => Stop Path_A_Check timer Reset Path_A_Failed Reset Path_A_Request	STAY IN CURRENT STATE
14	PORT_B_ACTIVE, FAULT	**Path_Check_Response message is received on port B** => Stop Path_B_Check timer Reset Path_B_Failed Reset Path_B_Request	STAY IN CURRENT STATE
15	IDLE, FAULT, PORT_A_ACTIVE, PORT_B_ACTIVE	**Link_A_Active is set AND Path_A_Failed is reset** => Reset Port_A_Failed	STAY IN CURRENT STATE
16	IDLE, FAULT, PORT_A_ACTIVE, PORT_B_ACTIVE	**Link_A_Active is reset OR Path_A_Failed is set** => Set Port_A_Failed	STAY IN CURRENT STATE
17	IDLE	**Port_A_Failed is reset** => Send Beacon message on port A Start Beacon timer Start Node_Receive timers Start Active_Port_Swap timer	PORT_A_ACTIVE

State number	Current state	Event /Condition =>Action	Next state
18	PORT_A_ACTIVE	**Port_A_Failed is set** => Stop beacon timer Stop Path_A_Check timer Reset Path_A_Request Stop Node_Receive timers Stop Active_Port_Swap timer	IDLE
19	IDLE, FAULT, PORT_A_ACTIVE, PORT_B_ACTIVE	**Link_B_Active is set** **AND** **Path_B_Failed is reset** => Reset Port_B_Failed	STAY IN CURRENT STATE
20	IDLE, FAULT, PORT_A_ACTIVE, PORT_B_ACTIVE	**Link_B_Active is reset** **OR** **Path_B_Failed is set** => Set Port_B_Failed	STAY IN CURRENT STATE
21	IDLE	**Port_B_Failed is reset** => Send Beacon message on port B Start Beacon timer Start Node_Receive timers Start Active_Port_Swap timer	PORT_B_ACTIVE
22	PORT_B_ACTIVE	**Port_B_Failed is set** => Stop beacon timer Stop Path_B_Check timer Reset Path_B_Request Stop Node_Receive timers Stop Active_Port_Swap timer	IDLE
23	IDLE	**Port_A_Failed is set** **AND** **Port_B_Failed is set**	FAULT
24	FAULT	**Link_A_Active is set** **AND** **Path_A_Failed is set** **AND** **Path_A_Request is reset** => Set Path_A_Request Send Path_Check_Request message on port A Start Path_A_Check timer	FAULT
25	FAULT	**Link_B_Active is set** **AND** **Path_B_Failed is set** **AND** **Path_B_Request is reset** => Set Path_B_Request Send Path_Check_Request message on port B	FAULT

State number	Current state	Event /Condition =>Action	Next state
		Start Path_B_Check timer	
26	FAULT	**Port_A_Failed is reset** **OR** **Port_B_Failed is reset**	IDLE
27	PORT_A_ACTIVE, PORT_B_ACTIVE	**Path_Check_Request message received on active port** => Send Path_Check_Response message on active port	STAY IN CURRENT STATE
28	PORT_A_ACTIVE, PORT_B_ACTIVE	**Beacon timer expired** => Transmit beacon message on active port Start beacon timer	STAY IN CURRENT STATE
29	PORT_A_ACTIVE	**Active_Port_Swap timer expired** **AND** **Port_B_Failed is reset** **=>** Stop Path_A_Check timer Reset Path_A_Request Start Active_Port_Swap timer	PORT_B_ACTIVE
30	PORT_A_ACTIVE	**Active_Port_Swap timer expired** **AND** **Port_B_Failed is set** **=>** Start Active_Port_Swap timer	PORT_A_ACTIVE
31	PORT_B_ACTIVE	**Active_Port_Swap timer expired** **AND** **Port_A_Failed is reset** **=>** Stop Path_B_Check timer Reset Path_B_Request Start Active_Port_Swap timer	PORT_A_ACTIVE
32	PORT_B_ACTIVE	**Active_Port_Swap timer expired** **AND** **Port_A_Failed is set** **=>** Start Active_Port_Swap timer	PORT_B_ACTIVE

8 BRP message structure

8.1 General

The BRP messages contain header, payload and the ISO/IEC 8802-3 (IEEE 802.3) FCS.

In Table 5 to Table 10:

- destination_MAC_Address is the multicast address defined in 7.1 for beacon and Learning_Update messages, while Failure_Notify, Path_Check_Request and Path_Check_Response messages use unicast addresses of receivers;
- IEEE 802.1Q tag priority = 7 (highest priority);
- all multi-byte fields shall be encoded in big endian (except the Ethernet addresses).

8.2 ISO/IEC 8802-3 (IEEE 802.3) tagged frame header

Table 5 specifies the format for the common header with ISO/IEC 8802-3 (IEEE 802.3) tagged frame.

NOTE The tag frame priority should be preserved when the BRP message is transferred through the LAN.

Table 5 – BRP common header with ISO/IEC 8802-3 (IEEE 802.3) tagged frame format

Octet position	Field	Type	Remarks
0	Destination_MAC_Address	UINT8[6]	
6	Source_MAC_Address	UINT8[6]	
12	802.1Q tag type	UINT16	= 0x8100
14	802.1Q tag control	UINT16	= 0xE000 + optional VLAN_ID
16	BRP EtherType	UINT16	= 0x80E1
18	BRP sub-type	UINT8	= 0x01
19	BRP version	UINT8	= 0x01

8.3 Beacon message

Table 6 specifies the format for the beacon message.

Table 6 – BRP beacon message format

Octet position	Field	Type	Remarks
20	Message type	UINT8	= 0x80
21	Source IP address	UINT32	= 0x0, if source has no IP address
25	Sequence Id	UINT32	
29	Beacon timeout	UINT32	In µs
33	Reserved	UINT8[31]	
64	CRC	UINT32	

8.4 Learning_Update message

Table 7 specifies the format for the Learning_Update message.

Table 7 – BRP Learning_Update message format

Octet position	Field	Type	Remarks
20	Message type	UINT8	= 0x40
21	Source IP address	UINT32	= 0x0, if source has no IP address
25	Sequence Id	UINT32	
29	Reserved	UINT8[35]	
64	CRC	UINT32	

8.5 Failure_Notify message

Table 8 specifies the format for the Failure_Notify message.

Table 8 – BRP Failure_Notify message format

Octet position	Field	Type	Remarks
20	Message type	UINT8	= 0x20
21	Source IP address	UINT32	= 0x0, if source has no IP address
25	Sequence Id	UINT32	
29	Reserved	UINT8[35]	
64	CRC	UINT32	

8.6 Path_Check_Request message

Table 9 specifies the format for the Path_Check_Request message.

Table 9 – BRP Path_Check_Request message format

Octet position	Field	Type	Remarks
20	Message type	UINT8	= 0x10
21	Source IP address	UINT32	= 0x0, if source has no IP address
25	Sequence Id	UINT32	
29	Source port	UINT8	= 0x1 or 0x2
30	Reserved	UINT8[34]	
64	CRC	UINT32	

8.7 Path_Check_Response message

Table 10 specifies the format for the Path_Check_Response message.

Table 10 – BRP Path_Check_Response message format

Byte	Field	Type	Remarks
20	Message type	UINT8	= 0x08
21	Source IP address	UINT32	= 0x0, if source has no IP address
25	Sequence Id	UINT32	= Sequence Id of Path_Check_Request message
29	Source port	UINT8	= Source Port of Path_Check_Request message
30	Reserved	UINT8[34]	
64	CRC	UINT32	

9 BRP fault recovery time

The following types of faults may occur in an BRP based network.

- Leaf link faults. These faults are detectable in the end node physical layer. The fault recovery time shall be less than 10 μs.
- Faults occurred in the direction of flow of beacon messages plus those occurred in the opposite direction to the flow of beacon messages but are detectable in the node/switch

physical layer. The fault recovery time in this case is two beacon timeouts which is less than 1 ms.

- Faults occurred in the opposite direction to the flow of beacon messages but are not detectable in the node/switch physical layer. Since the fault recovery time in this case is longer than in the two cases described above, it is considered the worst case.

NOTE Faults in the inactive paths transmitting towards the beacon have no effect on operational performance until the next network switchover. At switchover, they are detected using the above methods with the given worst case recovery time.

The worst case fault recovery time is:

$$t_{fr} = t_{nr} + t_{id} + t_{pcr},$$

where:

t_{fr} is the fault recovery time;
t_{nr} is the Node_Receive timer time out;
t_{id} is the infrastructure propagation delay of the Failure_Notify message;
t_{pcr} is the path check request timer time out.

EXAMPLE

Consider a network of 500 nodes with 3 layers of 8-port switches, similar to the one shown in Figure 1.

Assuming that all links have a data rate of 100 Mbit/s and a data frame size of 1 522 octets, the data frame transmit time plus inter-frame gap time is about 124 µs.

The Failure_Notify message size is 68 octets, its transmit time plus inter-frame gap time is about 8 µs.

Assuming the worst case message queuing in the switch, the Failure_Notify message delay in each switch is:

$$124\ \mu s + 8\ \mu s = 132\ \mu s.$$

The total delay of the Failure_Notify message travelling through the longest path of the network infrastructure is:

$$t_{id} = 8\ \mu s + (132 \times 6)\ \mu s + 8\ \mu s = 808\ \mu s = 0{,}81\ ms.$$

Assuming that Node_Receive timer time out t_{nr} = 2 ms, and Path_Check_A_Request timer time out t_{pcr} = 2 ms, and also assuming that Path_Check_B_Request timer is set to the same time as the Path_Check_A_Request timer:

$$t_{fr} = 2\ ms + 0{,}81\ ms + 2\ ms = 4{,}81\ ms.$$

10 BRP service definition

10.1 Supported services

The BRP services provide ability to set end node parameters and read these parameters and node status. The following services are provided:

- Set_Node_Parameters;
- Get_Node_Parameters;
- Add_Node_Receive_Parameters;
- Remove_Node_Receive_Parameters;
- Get_Node_Status.

10.2 Common service parameters

The following service parameters are common to several BRP services.

Node_Name
This parameter contains end node name.

(String32)

Source_MAC_Address
This parameter is the MAC address of the node from which the service request has been sent.

(String16)

Destination_MAC_Address
This parameter is the MAC address of the node to which the service request has been sent.

(String16)

Node_Type
This parameter contains description of the end node type (DANB or Beacon).

(String32)

VLAN_ID
This parameter contains the VLAN identifier.

(String32)

Status
This parameter contains description of the positive response to a service request

(String128)

Error_Info
This parameter contains description of the negative response to a service request

(String128)

10.3 Set_Node_Parameters service

Table 11 shows the parameters of the Set_Node_Parameters service.

Table 11 – BRP Set_Node_Parameters service parameters

Parameter name	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
Node_Name	M	M(=)		
Source_MAC_Address	M	M(=)		
Destination_MAC_Address	M	M(=)		
Node_Type	M	M(=)		
Beacon_Timer_Reload_Value	C	C(=)		
No_Beacon_Timer_Reload_Value	C	C(=)		
Path_A_Check timer reload value	M	M(=)		
Path_B_Check timer reload value	M	M(=)		
Active_Port_Swap timer reload value	M	M(=)		
Number_Of_Designated_Nodes	C	C(=)		
Designated_Node_List	C	C(=)		
VLAN_ID	C	C(=)		
Result (+)			S	S(=)
Node_Name			M	M(=)
Source_MAC_Address			M	M(=)
Destination_MAC_Address			M	M(=)
Status			M	M(=)
Result (-)			S	S(=)
Node_Name			M	M(=)
Source_MAC_Address			M	M(=)
Destination_MAC_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.

Beacon_Timer_Reload_Value
This parameter contains the value of the beacon timer in microseconds.

(Unsigned 32)

No_Beacon_Timer_Reload_Value
This parameter contains the value of the No_Beacon timer in microseconds.

(Unsigned 32)

Path_A_Check timer reload value
This parameter contains the value of the Path_A_Check timer in microseconds.

(Unsigned 32)

Path_B_Check timer reload value
This parameter contains the value of the Path_B_Check timer in microseconds.

(Unsigned 32)

Active_Port_Swap timer reload value
This parameter contains the value of the Active_Port_Swap timer in seconds.

(Unsigned 32)

Number_Of_Designated_Nodes
This parameter contains the number of nodes in designated node list.

(Unsigned 16)

Designated_Node_List
This parameter contains the list of MAC addresses of designated nodes. It is applicable to beacon end nodes.

(Array of OctetString16)

Result (+)
This parameter indicates that the service request succeeded. The following fields are included in the response:

Node_Name
Source_MAC_Address
Destination_MAC_Address
Status

Result (-)
This parameter indicates that the service request failed and specifies error conditions, when applicable. The following fields are included in the response:

Node_Name
Source_MAC_Address
Destination_MAC_Address
Error_Info

10.4 Get_Node_Parameters service

Table 12 shows the parameters of the Get_Node_Parameters service.

Table 12 – BRP Get_Node_Parameters service parameters

Parameter name	Req	Ind	Rsp	Cnf
Argument	**M**	**M(=)**		
Node_Name	**M**	**M(=)**		
Source_MAC_Address	**M**	**M(=)**		
Destination_MAC_Address	**M**	**M(=)**		
Result (+)			**S**	**S(=)**
Node_Name			**M**	**M(=)**
Manufacturer	**M**	**M(=)**		
Version	**M**	**M(=)**		
Destination_MAC_Address			**M**	**M(=)**
Node_Type			**M**	**M(=)**
Beacon_Timer_Reload_Value			**C**	**C(=)**
No_Beacon_Timer_Reload_Value			**C**	**C(=)**
Path_A_Check timer reload value			**M**	**M(=)**
Path_B_Check timer reload value			**M**	**M(=)**
Active_Port_Swap timer reload value			**M**	**M(=)**
Number_Of_Designated_Nodes			**C**	**C(=)**
Designated_Node_List			**C**	**C(=)**
VLAN_ID			**C**	C(=)
Result (-)			**S**	**S(=)**
Node_Name			**M**	**M(=)**
Source_MAC_Address			**M**	**M(=)**
Destination_MAC_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. There are no specific parameters for this service.

Result (+)
This parameter indicates that the service request succeeded. The following fields are included in the response:

Manufacturer
This parameter contains the name of the manufacturer
(VisibleString255)

Version
This parameter contains the version of the BRP. Future versions of the BRP shall be downward compatible with the version specified in this clause. A BRP end node shall accept packets from end nodes supporting BRP versions lower than the one it supports. A BRP end node shall drop unknown packets and shall ignore extended payload contents in known packets from end nodes supporting BRP versions higher than the one it supports.
(Unsigned32)

Beacon_Timer_Reload_Value
This parameter contains the value of the Beacon timer in microseconds. (Unsigned 32)

No_Beacon_Timer_Reload_Value
This parameter contains the value of the No_Beacon timer in microseconds.

(Unsigned 32)

Path_A_Check timer reload value
This parameter contains the value of the Path_A_Check timer in microseconds.

(Unsigned 32)

Path_B_Check timer reload value
This parameter contains the value of the Path_B_Check timer in microseconds.

(Unsigned 32)

Active_Port_Swap timer reload value
This parameter contains the value of the Active_Port_Swap timer in seconds.

(Unsigned 32)

Number_Of_Designated_Nodes
This parameter contains the number of nodes in designated node list.

(Unsigned 16)

Designated_Node_List
This parameter contains the list of MAC addresses of designated nodes. It is applicable to Beacon end nodes.

(Array of OctetString16)

Result (-)
This parameter indicates that the service request failed and specifies error conditions, when applicable. The following fields are included in the response:

Node_Name
Source_MAC_Address
Destination_MAC_Address
Error_Info

10.5 Add_Node_Receive_Parameters service

Table 13 shows the parameters of the Add_Node_Receive_Parameters service.

Table 13 – BRP Add_Node_Receive_Parameters service parameters

Parameter name	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
Node_Name	M	M(=)		
Source_MAC_Address	M	M(=)		
Destination_MAC_Address	M	M(=)		
Transmit_Node_MAC_Address	M	M(=)		
Node_Receive_Timeout	M	M(=)		
Result (+)			S	S(=)
Node_Name			M	M(=)
Source_MAC_Address			M	M(=)
Destination_MAC_Address			M	M(=)
Status			M	M(=)
Result (-)			S	S(=)
Node_Name			M	M(=)
Source_MAC_Address			M	M(=)
Destination_MAC_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.

Transmit_Node_MAC_Address
This parameter contains MAC address of transmit node of interest.

(VisibleString16)

Node_Receive_Timeout
This parameter contains associated node receive timeout in microseconds.

(Unsigned 32)

Result (+)
This parameter indicates that the service request succeeded. The following fields are included in the response:

Node_Name
Source_MAC_Address
Destination_MAC_Address
Status

Result (-)
This parameter indicates that the service request failed and specifies error conditions, when applicable. The following fields are included in the response:

Node_Name
Source_MAC_Address
Destination_MAC_Address
Error_Info

10.6 Remove_Node_Receive_Parameters service

Table 14 shows the parameters of the Remove_Node_Receive_Parameters service.

Table 14 – BRP Remove_Node_Receive_Parameters service parameters

Parameter name	Req	Ind	Rsp	Cnf
Argument	**M**	**M(=)**		
Node_Name	**M**	**M(=)**		
Source_MAC_Address	**M**	**M(=)**		
Destination_MAC_Address	**M**	**M(=)**		
Transmit_Node_MAC_Address	**M**	**M(=)**		
Result (+)			**S**	**S(=)**
Node_Name			**M**	**M(=)**
Source_MAC_Address			**M**	**M(=)**
Destination_MAC_Address			**M**	**M(=)**
Status			**M**	**M(=)**
Result (-)			**S**	**S(=)**
Node_Name			**M**	**M(=)**
Source_MAC_Address			**M**	**M(=)**
Destination_MAC_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.

Transmit_Node_MAC_Address
This parameter contains MAC address of transmit node to be removed from Node_Receive timers.

(VisibleString16)

Result (+)
This parameter indicates that the service request succeeded. The following fields are included in the response:

Node_Name
Source_MAC_Address
Destination_MAC_Address
Status

Result (-)
This parameter indicates that the service request failed and specifies error conditions, when applicable. The following fields are included in the response:

Node_Name
Source_MAC_Address
Destination_MAC_Address
Error_Info

10.7 Get_Node_Status service

Table 15 shows the parameters of the Get_Node_Status service.

Table 15 – BRP Get_Node_Status service parameters

Parameter name	Req	Ind	Rsp	Cnf
Argument	M	M(=)		
Node_Name	M	M(=)		
Source_MAC_Address	M	M(=)		
Destination_MAC_Address	M	M(=)		
Result (+)			S	S(=)
Node_Name			M	M(=)
Source_MAC_Address			M	M(=)
Destination_MAC_Address			M	M(=)
Node_Type			M	M(=)
Node_Status			M	M(=)
Port_A_Status			M	M(=)
Port_B_Status			M	M(=)
Result (-)			S	S(=)
Node_Name			M	M(=)
Source_MAC_Address			M	M(=)
Destination_MAC_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. There are no specific parameters for this service.

Result (+)
This parameter indicates that the service request succeeded. The following fields are included in the response:

Node_Status
This parameter contains the value representing node status.

(OctetString16)

Port_A_Status
This parameter contains the value representing port A status.

(OctetString16)

Port_B_Status
This parameter contains the value representing port B status.

(OctetString16)

Result (-)
This parameter indicates that the service request failed and specifies error conditions, when applicable. The following fields are included in the response:

Node_Name
Source_MAC_Address
Destination_MAC_Address
Error_Info

11 BRP Management Information Base (MIB)

```
-- ***************************************************************************

IEC-62439-5-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 MODULE-IDENTITY
       LAST-UPDATED "200811080000Z"  --  November 8, 2008
       ORGANIZATION "IEC/SC 65C"
       CONTACT-INFO ""

       DESCRIPTION  "This MIB module defines the Network Management interfaces
                     for the Beacon Redundancy Protocol defined by the IEC
                     standard 62439-5."

       REVISION     "200711080000Z"  --  November 8, 2007
       DESCRIPTION  "Initial version of the Network Management interface for the
                     Beacon Redundancy Protocol"

       REVISION    "200811100000Z"  --  November 10, 2008
       DESCRIPTION  "
           Separation of IEC 62439 into a suite of documents
           This MIB applies to IEC 62439-5, no change in functionality
                "

       ::= { IEC 62439-5}


-- ***************************************************************************
-- 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 BRP Network Management
-- ***************************************************************************

NodeName OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(1..32))
        MAX-ACCESS  read-only
        STATUS      mandatory
```

```
        DESCRIPTION
            "specifies the unique node name"
        ::= { brp 1 }

Manufacturer OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(1..255))
        MAX-ACCESS  read-only
        STATUS      mandatory
        DESCRIPTION
            "specifies the name of the manufacturer"
        ::= { brp 2 }

Version OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(1..32))
        MAX-ACCESS  read-only
        STATUS      mandatory
        DESCRIPTION
            "specifies the version of BRP"
        ::= { brp 3 }

MACAddress OBJECT-TYPE
        SYNTAX MACAddress
        MAX-ACCESS  read-only
        STATUS      mandatory
        DESCRIPTION
            "specifies node MAC address"
        ::= { brp 4 }

NodeType OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(1..32))
        MAX-ACCESS  read-write
        STATUS      mandatory
        DESCRIPTION
            "specifies the node type"
        ::= { brp 5 }

NodeStatus OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(1..32))
        MAX-ACCESS  read-only
        STATUS      mandatory
        DESCRIPTION
            "specifies the node status"
        ::= { brp 6 }



PortAStatus OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(1..32))
        MAX-ACCESS  read-only
        STATUS      mandatory
        DESCRIPTION
            "specifies port A status"
        ::= { brp 7 }


PortBStatus OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(1..32))
        MAX-ACCESS  read-only
        STATUS      mandatory
        DESCRIPTION
            "specifies port B status"
        ::= { brp 8 }

VLANID OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE(1..32))
        MAX-ACCESS  read-only
        STATUS      mandatory
        DESCRIPTION
            "specifies VLAN ID"
        ::= { brp 9 }

END
```

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 Seamleass Redundancy (HSR)*

IEC 62439-4, *Industrial communication networks – High availability automation networks – Part 4: Cross-network Redundancy Protocol (CRP)*

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*

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

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