BS EN 61375-3-4:2014

BSI Standards Publication

Electronic railway equipment — Train communication network (TCN)

Part 3-4: Ethernet Consist Network (ECN)

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of EN 61375-3-4:2014. It is identical to IEC 61375-3-4:2014.

The UK participation in its preparation was entrusted by Technical Committee GEL/9, Railway Electrotechnical Applications, to Panel GEL/9/-/4, Railway applications - Train communication network and multimedia systems.

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.

Published by BSI Standards Limited 2014

ISBN 978 0 580 68698 6
ICS 45.060.01

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 31 May 2014.

Amendments/corrigenda issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 61375-3-4

May 2014

ICS 45.060

English Version

Electronic railway equipment - Train communication network (TCN) - Part 3-4: Ethernet Consist Network (ECN) (IEC 61375-3-4:2014)

Matériel électronique ferroviaire - Réseau embarqué de train (TCN) - Partie 3-4: Réseau Ethernet de Rame (ECN) (CEI 61375-3-4:2014)

Elektronische Betriebsmittel für Bahnen - Zugbus - Teil 3-4: ECN - Ethernet-Zugverband-Netzwerk (IEC 61375-3-4:2014)

This European Standard was approved by CENELEC on 2014-04-23. 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 CEN-CENELEC Management Centre 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 CEN-CENELEC Management Centre has the same status as the official versions.

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

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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Foreword

The text of document 9/1873/FDIS, future edition 1 of IEC 61375-3-4, prepared by IEC/TC 9 "Electrical equipment and systems for railways" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 61375-3-4:2014.

The following dates are fixed:

• latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2015-01-23
• latest date by which the national standards conflicting with the document have to be withdrawn	(dow)	2017-04-23

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Standard IEC 61375-3-4:2014 was approved by CENELEC as a European Standard without any modification.

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

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

NOTE When an international publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

Publication	Year	Title	EN/HD	Year
IEC 61076-2-101	-	Connectors for electronic equipment - Product requirements - Part 2-101: Circular connectors - Detail specification for M12 connectors with screw-locking	EN 61076-2-101	-
IEC 61076-3-104	-	Connectors for electronic equipment - Product requirements - Part 3-104: Detail specification for 8-way, shielded free and fixed connectors for data transmissions with frequencies up to 1000 MHz	EN 61076-3-104	
IEC 61156-6	-	Multicore and symmetrical pair/quad cables for digital communications - Part 6: Symmetrical pair/quad cables with transmission characteristics up to 1 000 MHz - Work area wiring - Sectional specification	-	-
IEC 61375-1	-	Electronic railway equipment - Train communication network (TCN) - Part 1: General architecture	EN 61375-1	-
IEC 61375-2-1	-	Electronic railway equipment - Train communication network (TCN) - Part 2-1: Wire Train Bus (WTB)	EN 61375-2-1	-
IEC 61375-2-5	-	Electronic railway equipment - Train backbone - Part 2-5: Ethernet Train Backbone	EN 61375-2-5	-
IEC 62439 series	-	High availability automation networks	EN 62439[1)]	-
ISO/IEC 7498 series	-	Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model	-	-
ISO/IEC 8824 series	-	Information technology - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1)	-	-
ISO/IEC 11801	-	Information technology - Generic cabling for customer premises	-	-

[1)] EN 62439 is superseded by EN 62439-6:2010, which is based on IEC 62439-6:2010.

Publication	Year	Title	EN/HD	Year
IEEE 802.3	-	IEEE Standard for 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) - Acess Method and Physical Layer Specifications	-	-
IEEE 802.1Q	-	IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks	-	-
IEEE 802.1D	-	IEEE Standard for Local and Metropoitan Area Networks - Media Access Control (MAC) Bridges	-	-
ANSI/TIA/EIA 568-B.1	2001	Commercial Building Telecommunications Cabling Standard - Part 1: General requirements	-	-
ANSI X3.263	1995	EN-Information Technology - Fibre Distributed Data Interface (FDDI) - Token Ring Twisted Pair Physical Layer Medium Dependent (TP-PMD)	-	-

CONTENTS

INTRODUCTION

This part of IEC 61375 series of international standards specifies the Consist Network based on Ethernet technology, i.e. the Ethernet Consist Network (ECN) within the TCN architecture as defined in IEC 61375-1, and End Devices which can attach to the ECN. In addition gateway services between Train Backbone and ECN are specified.

The general architecture of the TCN (see IEC 61375-1) defines a hierarchical structure with two levels of networks, Train Backbone(s) and Consist Network(s). This hierarchical structure specifies Consist Networks based on different technologies such as MVB, CANopen and ECN interfacing one Train Backbone. ECNs based on different design and implementation may be interfaced to the same Train Backbone reaching the result that the Train Backbone ensures interoperability between Consist Networks with different implementations.

The common part, consisting of Clauses 1 to 4, defines requirements and specifications which are common to all ECN implementations and End Devices and gateways.

The common part defines

- the data communication interface of End Devices connected to the ECN,
- functions and services provided by the ECN to End Devices,
- the gateway functions for data transfer between Train Backbone and the ECN, and
- performances of the ECN.

ELECTRONIC RAILWAY EQUIPMENT – TRAIN COMMUNICATION NETWORK (TCN) –

Part 3-4: Ethernet Consist Network (ECN)

1 Scope

This part of IEC 61375 specifies the data communication network inside a Consist based on Ethernet technology, the Ethernet Consist Network (ECN).

The applicability of this part of IEC 61375 to the Consist Network allows for interoperability of individual vehicles within Open Trains in international traffic.

This part of IEC 61375 may be additionally applicable to closed trains and Multiple Unit Trains when so agreed between purchaser and supplier.

2 Normative references

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

IEC 61076-2-101, *Connectors for electronic equipment – Product requirements – Part 2-101: Circular connectors – Detail specification for M12 connectors with screw-locking*

IEC 61076-3-104, *Connectors for electronic equipment – Product requirements – Part 3-104: Detail specification for 8-way, shielded free and fixed connectors for data transmissions with frequencies up to 1 000 MHz*

IEC 61156-6, *Multicore and symmetrical pair/quad cables for digital communications – Part 6: Symmetrical pair/quad cables with transmission characteristics up to 1 000 MHz – Work area wiring – Sectional specification*

IEC 61375-1, *Electronic railway equipment – Train Communication Network (TCN) – Part 1: General architecture*

IEC 61375-2-1, *Electronic railway equipment – Train Communication Network (TCN) – Part 2-1: Wire Train Bus (WTB)*

IEC 61375-2-5, *Electronic railway equipment – Train Communication Network (TCN) – Part 2-5: Ethernet Train Backbone (ETB)*

IEC 62439 (all parts), *Industrial communication networks – High availability automation networks*

ISO/IEC 7498, *Information technology – Open Systems Interconnection (OSI) – The Basic reference model*

ISO/IEC 8824 (all parts), *Information technology – Abstract Syntax Notation One (ASN.1)*

ISO/IEC 11801, *Information technology – Generic cabling for customer premises*

TIA/EIA-568-B, *Commercial Building Telecommunications Cabling Standard – Part 1: General Requirements (ANSI/TIA/EIA-568-B.1-2001)*

ANSI X3.263:1995, *EN-Information Technology - Fibre Distributed Data Interface (FDDI) - Token Ring Twisted Pair Physical Layer Medium Dependent (TP-PMD) (order number ANSI INCITS 263)*

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

IEEE 802.1Q, *IEEE Standard for Local and metropolitan area networks – Virtual Bridged Local Area Networks*

IEEE 802.3, *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*

3 Terms, definitions, symbols, abbreviations and conventions

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 61375-1 and the following apply.

3.1.1
auto negotiation
auto negotiation function allows two network devices on a point-to-point link to choose the best possible configuration; e.g. full/half duplex mode, transmission speed

3.1.2
auto polarity
auto polarity function corrects the signal polarity automatically

3.1.3
crossover function
crossover function connects the transmitter of PHY to the receiver of PHY at the end of point-to-point transmit-receive-pair link

3.1.4
full duplex mode
full duplex mode allows both sending and receiving frames at a time between stations on a link

3.1.5
intra-car connection
connection (link) between communication devices inside a car

3.1.6
inter-car connection
connection (link) between communication devices at the interface between two cars excluding the interface between Consists

3.1.7
link layer
layer in the OSI model establishing point-to-point and broadcast and multicast connections between devices attached to the logical communication channel consisting of one or more physical links

3.1.8
physical layer
layer in the OSI model providing the means of transmitting raw bits over a physical link

3.1.9
power over ethernet
Power over Ethernet technology uses the Ethernet cable for both signalling and power supply, there are PSE (Power Sourcing Equipment) terminal and PD (Power Device) terminal

3.1.10
presentation layer
layer in the OSI model for representing and formatting information of applications

3.1.11
session layer
layer in the OSI model for managing a session between applications

3.1.12
tag
a field inserted in the MAC frame of IEEE 802.3, which is inserted after the source MAC address field

3.1.13
token
a signal that is used for medium access control to avoid collisions, and transmitted between communication devices

3.1.14
virtual LAN
virtual LAN technology divides one physical LAN into several logically separated networks on Link Layer; i.e. there are separated broadcast domains in one physical LAN

3.2 Symbols and abbreviated terms

ACK	Acknowlegement
ACM	Access Control Machine
ALG	Application Layer Gateway
ANSI	American National Standard Institute, a standardisation body in the United States
ARP	Address Resolution Protocol
ASN.1	Abstract Syntax Notation Number 1 on data presentation (ISO/IEC 8824)
AWG	American Wire Gauge
bps	bits per second
BT	Bit Time
CCF	Common Cause Failure
CI	Control In
CNN	Consist Network Node
CS	Consist Switch
DA	Destination Address
DHCP	Dynamic Host Configuration Protocol
DI	Data In
DNS	Domain Name System
DO	Data Out

DSCP	Differentiated Services Code Point, defined in RFC 2474
ECN	Ethernet Consist Network
ED	End Device
EIA	Electronics Industries Association, a standardisation body in the United States
EMC	electro-magnetic compatibility
EMU	Electric Multiple Unit
ETB	Ethernet Train Backbone
ExP	External Port
FCS	Frame Check Sequence
FTP	File Transfer Protocol
FQDN	Full Qualified Domain Name
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers, New York
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
InP	Internal Port
I/O	Input and Output
IP	Internet Protocol
LAN	Local Area Network
LPR	Local Port for Reception
LPT	Local Port for Transmission
LSB	Least Significant Bit
MAC	Medium Access Control, a sub-layer within the Link Layer ruling which device is entitled to send on the bus
MAU	Medium Attachment Unit
MD	Message Data
MDI	Media Dependent Interface
MDI-X	MDI implementing crossover function
MRP	Media Redundancy Protocol
MSB	Most Significant Bit
MTBF	Mean Time Between Failures
MVB	Multifunction Vehicle Bus
NAT	Network Address Translation
ND	Network Device
NTP	Network Time Protocol
OSI	Open System Interconnection, a universal communication model defined in the ISO/IEC 7498
OSPF	Open Shortest Path First
PC	Personal Computer
PCS	Physical Coding Sublayer
PD	Process Data
PHY	Physical Layer, Physical Layer device
PMA	Physical Media Attachment

PMD	Physical Medium Dependent
PoE	Power over Ethernet
QoS	Quality of service
RD	Receive Data
RDA	Receive Data Amplified
RFC	Request for Comments, Internet Standard published by the Internet Engineering Task Force (IETF)
R-NAT	Railway Network Address Translation
RX	Receive
SFD	Start Frame Delimiter
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SS	Signal Status
STP	Shielded Twisted Pair cable, a cable in which each pair of two conductors are twisted together and shielded
TBN	Train Backbone Node
TCN	Train Communication Network, a set of communicating vehicle and Train Backbones
TCP	Transmission Control Protocol
TD	Transmit Data
TDA	Transmit Data Amplified
TDRD	Transmit Data and Receive Data
TFLPR	Timer for Failure of Local Port for Reception
TFTP	Trivial File Transfer Protocol
TFTPU	Timer for Failure of Trunk Port Up link
TIA	Telecommunications Industry Association
TLT	Timer for Limit Time
TNM	Train Network Management
TNMS	Timer for CNN Management Sending
TNORD	Timer for No Reception Down link
TNORU	Timer for No Reception Up link
TPCM	Trunk Port Control Machine
TPD	Trunk Port Down link
TPU	Trunk Port UP link
TPUD	Trunk Port Up link and Down link
TREQ	Timer for Transmit Request
TRLPR	Timer for Recovery of Local Port for Reception
TRTPD	Timer for Recovery of Trunk Port Down link
TRTPU	Timer for Recovery of Trunk Port Up link
TRRC	Transmission, Reception and Repeat Control
TTRT	Target Token Rotation Timer
TX	Transmit
UDP	User Datagram Protocol

UTP Unshielded Twisted Pair cable, a cable in which each pair of two conductors are twisted together and not shielded

VLAN Virtual LAN

VTLT Value to Timer for Limit Time

VTREQ Value to Timer for Transmit Request

VTTRT Value to Target Token Rotation Timer

WTB Wire Train Bus

3.3 Conventions

The conventions defined in IEC 61375-1 as well as the following apply.

3.3.1 Bit numbering conventions

In the representation of message formats defined in this standard the bit numbering follows the representation of power of two value in a byte or word.

3.3.2 Byte order conventions

In the representation of message formats defined in this standard encoding of integer values is big-endian if not otherwise stated.

The format of a message is specified in a graphical form followed by a table form to show the details. Octets in the format are ordered from left to right and from top to bottom when they are encoded in an Ethernet frame, if not otherwise stated.

3.3.3 Data types

3.3.3.1 General

In the representation of message formats defined in this standard data types are specified according to ASN.1. However, encoding rules of ASN.1 are not applied to ignore identifier, length, and end-of-contents octets. Data types which are added are as follows.

NOTE Most types are same as defined in IEC 61375-2-1.

3.3.3.2 Notation for the boolean type

A simple type with two distinguished values, TRUE and FALSE.

NOTE This is the same definition as IEC 61375-2-1.

Syntax is as follows.

BooleanType::= BOOLEAN1

This shall be encoded as one bit, a value 1 for TRUE and a value 0 for FALSE.

3.3.3.3 Notation for the unsigned integer type

A simple type with two distinguished values which are positive numbers or zero. Three types are defined that have a fixed size in bits defined by the postfix #, which is 8, 16, or 32.

NOTE This is the same definition as IEC 61375-2-1, but # is limited to 8, 16, and 32.

Syntax is as follows.

UnsignedType::= UNSIGNED#, (# = {8,16,32})

Range of UNSIGNED8: 0..255

Range of UNSIGNED16: 0..65535

Range of UNSIGNED32: 0..2^{32}–1

They shall be encoded in a binary number consisting of 8, 16, or 32 bits.

3.3.3.4 Notation for the octetstring type

The definition of octetstring type shall conform to ASN.1.

This shall be encoded as successive octets in the order they appear in the data value.

4 Common part

4.1 General

Clause 4 defines common requirements and specifications for End Devices, Network Devices, TBNs, and whole ECNs.

4.2 Architecture

4.2.1 Network structure

The logical view of the ECN is shown in Figure 1. ECN interconnects End Devices located in one Consist. When an ECN is connected to a Train Backbone it shall be connected to the Train Backbone via one train backbone node (TBN) or one set of redundant TBNs of the Train Backbone. It is a common requirement that only one TBN can forward user data packets between the ECN and the Train Backbone. However, all the redundant TBNs could optionally forward user data packets between the ECN and the Train Backbone.

NOTE 1 In case of WTB, only one TBN is active for one ECN. In case of ETB, all the redundant TBNs are active. See IEC 61375-2-1 and 61375-2-5.

ECN shall be based on switched Ethernet. An ECN consists of Consist Switches, connectors, cables, and optionally repeaters and transmits data frames between End Devices and between End Devices and TBNs. ECN may have sub-networks inside it and routers connecting the subnetworks can be deployed.

One Consist can have one or more ECNs in it, and those ECNs may or may not interface the same Train Backbone(s). An End Device connects to one Consist Network or to one set of Consist Networks prepared for redundancy reasons. An End Device could connect to different Consist Networks via different interfaces on the device, but it is regarded that a physical End Device has multiple logical End Devices in it.

EXAMPLE An End Device can connect to a Consist Network for train monitoring services and connect to another Consist Network for multimedia services.

Ethernet ports between End Devices and Consist Switches and between TBNs and Consist Switches shall follow IEEE 802.3 standard. Ethernet ports which are used for connections between Consist Switches should conform to IEEE 802.3 standard, but they are not mandatorily required to conform to IEEE 802.3 standard for the purpose of achieving railway specific requirements.

Topology of ECN may vary with ECN implementations, but common requirements are defined in this part of the standard.

NOTE 2 This is why Consist Switches in Figure 1 are not connected directly.

The TBN to which the ECN attaches shall provide a gateway function which provides data transfer between the ECN and the Train Backbone. The Train Backbone to which an ECN attaches may be WTB or ETB. Communications between Consist Networks can be possible directly or indirectly over the Train Backbone; i.e. the gateway function may be implemented as a routing function in the network layer or as an Application Layer gateway.

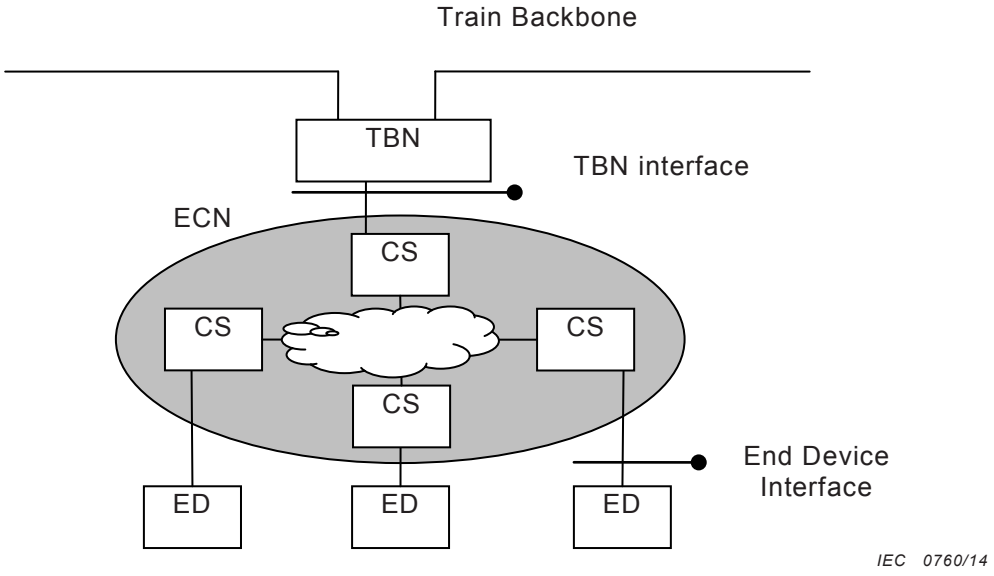


Figure 1 – Logical view of the ECN

4.2.2 Network topology

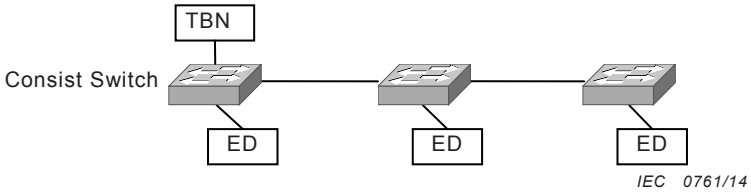
Any physical topology can be deployed according to the requirements from applications, but ECN shall not form a loop or loops in logical topology. The list below shows examples.

- The physical topology of the ECN could be linear or ring or ladder or others in order to implement different level of redundancy.
- An ECN could have one or more sub-networks.

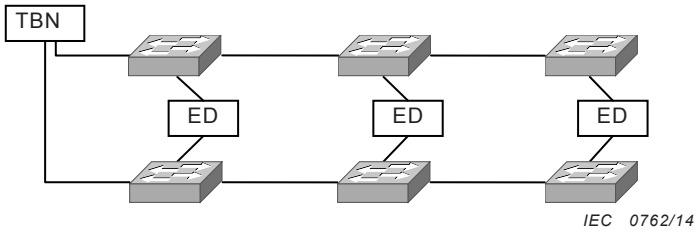
Linear, ring, and ladder topologies are typical topologies as introduced in IEC 61375-1. For End Device link redundancy, an End Device may be connected to two different Consist Switches by two independent communication links, which is introduced in IEC 61375-1 and also defined as dual homing in 4.5.4 of this standard. Figure 2 shows examples of ECNs with various physical topologies and End Device link redundancy.

NOTE See also 4.5 and Annex A with respect to topology from redundancy point of view.

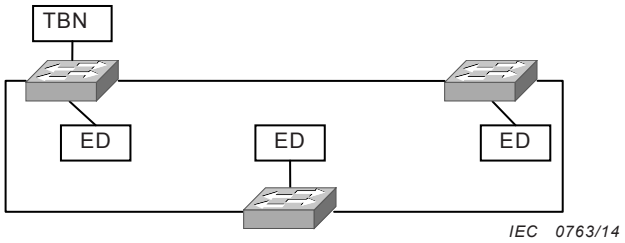
1) Linear topology



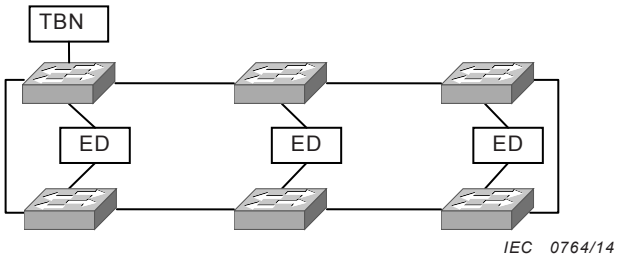
2) Linear topology (parallel network) with dual homing



3) Ring topology



4) Ring topology with dual homing



5) Ladder topology with dual homing

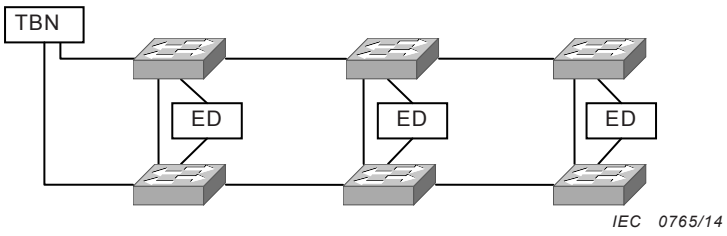


Figure 2 – Examples of ECN physical topologies

4.2.3 End Device classes

End Devices are classified from the viewpoint of installation as shown in Table 1.

Table 1 – End Device classes (1)

End Device class	Description
Temporary End Device	Temporary End Device is an End Device which is not fixedly mounted on the train, but it is connected to the ECN temporarily for the purpose of maintenance for example. A notebook PC which is used to retrieve operational status of equipments is a typical Temporary End Device.
Standard End Device	Standard End Device is an End Device which is fixedly mounted on the train. This is the main class of End Devices.

Standard End Device is furthermore classified from the viewpoint of communication requirements as shown in Table 2.

Table 2 – End Device classes (2)

End Device class	Description
Consist Local End Device	Consist Local End Device is an End Device which communicates with only devices in the same ECN. This class of End Device does not always need to know train topology.
Train Communication End Device	Train Communication End Device is an End Device which uses the Train Backbone and communicates with devices in other CNs or devices directly attached to TBNs. This class of End Device shall be able to know that train topology has been changed in order not to communicate with wrong devices after inauguration. However, it does not need to know train topology by itself; i.e. it does not initiate communications over the Train Backbone. Topography counter of the train backbone is the typical example of information of the train topology. Train Communication End Device shall meet the same requirements as Consist Local End Device.
Train Topology aware End Device	Train Topology aware End Device is an End Device which initiates communications over the Train Backbone and needs to know train topology; i.e. train network addresses on devices outside of the ECN. For example, a controller device (Train Topology aware End Device) makes connections to I/O devices (Train Communication End Devices) in remote ECN over the backbone. In this case, the controller device needs to know addresses of remote I/O devices by using the train topology database, but remote I/O devices does not always need to do so. Train Topology aware End Device shall meet the same requirements as Train Communication End Device.

NOTE Protocols delivering information regarding the train topology are specified in IEC 61375-2-3.

4.2.4 Network Device types and Consist Switch classes

Network Devices in ECN are classified from the viewpoint of functionality as shown in Table 3.

Table 3 – Network Device types

Network Device type	Description
Repeater	This type of Network Device could be used to respect Ethernet physical rules between two communication devices. The main characteristic for this Network Device is to be transparent as possible for all protocols, Link Layer and above.
Consist Switch	This type of Network Device is the main type for ECN. Consist Switch shall relay frames in Link Layer between two devices. Consist Switch is classified into managed and unmanaged Consist Switch as defined in Table 4.
Router	This is a Network Device which has at least two IP interfaces and ensures communication between multiple IP subnets in network layer. TBNs between ETB and ECN contain routers specialized for train on-board communication. TBN routers could implement some usual network applications like DHCP server, DNS server, NTP server, and so on. NOTE: TBNs between ETB and ECN could also be application gateways. DHCP, DNS, and NTP servers could also reside on other Network Devices and End Devices.

Consist Switches are classified from the viewpoint of the functions as shown in Table 4.

Table 4 – Consist Switch classes

Consist Switch class	Description
Unmanaged Consist Switch	Unmanaged Consist Switch is a Consist Switch which has only limited functions. As a minimum, this class of switch shall support IEEE 802.1D MAC bridging as defined in 4.9, but needs not support additional functions such as online management function and IP communication function.
Managed Consist Switch	Managed Consist Switch is a Consist Switch which has functions of MAC bridge, online management, IP communication and so on. Managed Consist Switch shall meet the same requirements as the Unmanaged Consist Switch.

4.3 Data class

IEC 61375-1 defines five principal data classes:

- Supervisory Data
- Process Data
- Message Data
- Stream Data
- Best Effort Data

EXAMPLE Messages exchanged between Consist Switches, for the purpose of network topology management, are typical examples of Supervisory Data used in ECN.

Table 5 shows typical service parameters for each data class and Table 6 shows typical service parameter values for each data class. However specific definition of the service parameters and values shall be determined according to the requirements from the specific applications, ECN should support these typical service parameter values for each data class.

NOTE QoS is used to realize the service parameters. See 4.6.

Table 5 – Data class service parameters

Service parameter	Description	Measuring Unit
Cycle time	Time between two successive frames which are cyclically transmitted.	Seconds
Data size	Length of data field (payload) in a frame transmitted in Link Layer.	Octets
Latency	Transmission time of a frame in Link Layer between two EDs. Transmission starting time shall not be later than the beginning to transmit data to Link Layer service in the communication protocol stack. Transmission ending time shall not be before receiving the entire data frame in Link Layer in the communication protocol stack.	Seconds
Jitter	Variance in transmission time for subsequent frame transmissions.	Seconds

Table 6 – Typical values for data class service parameters

Data class	Service Parameter	Value
Process Data	minimum cycle time	20 ms
	maximum data size	1 500 octets
	maximum latency	10 ms
	maximum jitter	10 ms
Message Data	minimum cycle time	Not applicable
	maximum data size	1 500 octets
	maximum latency	100 ms
	maximum jitter	Not applicable
Stream Data	minimum cycle time	Not applicable
	maximum data size	1 500 octets
	maximum latency	125 ms
	maximum jitter	25 ms
Best Effort Data	minimum cycle time	Not applicable
	maximum data size	1 500 octets
	maximum latency	Not applicable
	maximum jitter	Not applicable
Supervisory Data	minimum cycle time	10 ms
	maximum data size	1 500 octets
	maximum latency	10 ms
	maximum jitter	10 ms

4.4 Functions and services

ECN shall provide functions and services listed below.

- Frame relaying

  ECN shall receive MAC frames defined in IEEE 802.3 from End Devices and forward the MAC frames to the designated End Devices identified by the destination address fields of

the MAC frames. For the purpose of implementing this function, specifications for Consist Switches are defined according to IEEE 802.1D in 4.9. Consist Switches shall be able to relay both basic (untagged) and tagged MAC frames .

- Virtual LAN

  ECN shall be able to provide VLAN functions defined in IEEE 802.1Q. VLAN functions required in ECN are defined in 4.9.

  NOTE 1 Careful configuration of VLAN is important, because configuration faults can easily isolate End Devices completely.

- Redundancy management

  ECN shall be able to provide redundancy and redundancy management when it is necessary from application requirements. ECN redundancy is defined in 4.5.

  An implementation of ECN may not provide redundancy when it is not necessary.

- Quality of service

  ECN shall be able to provide QoS by prioritizing traffic when it is necessary from application requirements. Quality of service in ECN is defined in 4.6

- Gateway functions

  When an ECN is attached to a Train Backbone, the TBN shall provide gateway functions for data transfer between the Train Backbone and the ECN. Gateway functions are defined in 4.11.

- Train network management

  When an ECN is attached to a Train Backbone, the TBN shall provide train network management services according to that of the Train Backbone. Train network management is defined in 4.12.

ECN should provide functions and services listed below.

- Dynamic IP address assignment

  ECN should provide functions for dynamic IP address assignment for devices. Devices can also use static IP address assignment. Requirements for IP address assignment and management are defined in 4.7 and 4.8.

- Name resolution

  ECN should provide functions for name resolution between IP addresses and names such as hostnames and function names. Requirements for name resolution are defined in 4.7.

  NOTE 2 Definition of functional addressing is out of the scope of this part of the standard.

4.5 Redundancy

4.5.1 General

This subclause describes requirements and definitions for redundancy in ECN.

Redundancy managed at network level and redundancy managed at ED level are described in this subclause. A specific implementation of ECN should select one or more redundancy method to fulfil application requirements. Supported failure cases and comparison in reliability and availability are described in Annex A to help the selection.

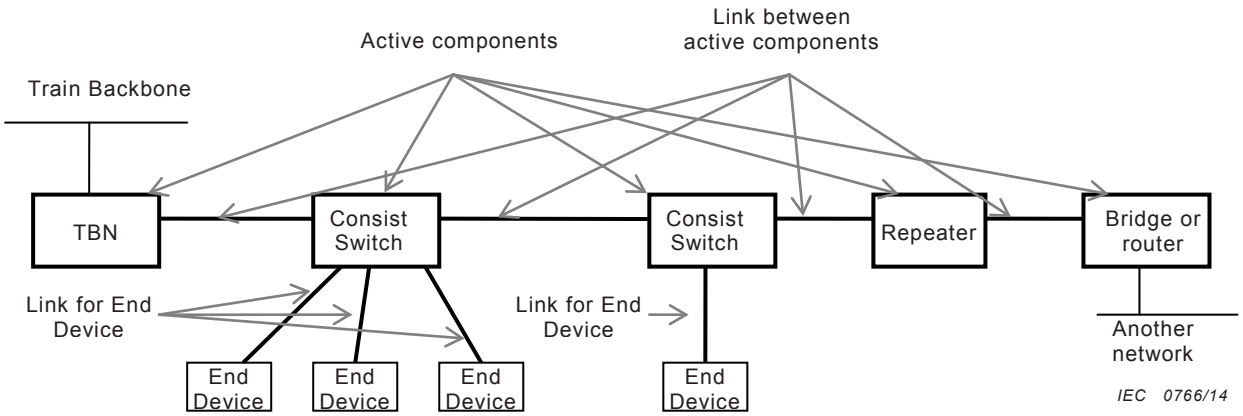
NOTE Redundancy of End Devices themselves is out of the scope of this part of the standard, but the advantage of End Device redundancy is also described in Annex A.

4.5.2 Definitions

4.5.2.1 Network component

A network component is defined as a unit affected by a component failure, which means an active component of network device, a link between the active components or a link for End Device interface in this part of the standard. An example of the network components is shown in Figure 3.

NOTE Active components of network devices are described in IEC 61375-1, 4.2.2 (Component types).



NOTE Bold boxes and bold lines indicate examples of network components.

Figure 3 – Example of network components

4.5.2.2 Recovery time

When redundancy scheme managed at network level is applied in the ECN, recovery time of network function of ECN in case of failure is expected to be shorter than the time during which operations of the Consist can be maintained without loss of train application functions.

In case of failure occurrence in an ECN, normal communication function of the ECN is interrupted and re-started after recovery time with redundancy.

Recovery time in ECN shall include

- time for detection of failure,
- redundancy switch over time (see NOTE), and
- time for re-configuration in ECN, if occurred.

NOTE Switch over time means time for switching its function from failed component to other component.

Recovery time of network shall be measured in the conformance test.

4.5.3 Redundancy managed at network level

Redundancy managed at network level, adopting network topology which has redundancy in it, is a method to recover network function in case of failure at network components. Examples of ECNs with typical network topologies are shown in 4.2.2.

Requirements for redundancy managed at network level are as follows.

- When redundancy scheme is applied in ECN, a single network component failure shall not prevent the rest of the network from working without separation of the network so that the application can maintain its function.
- When a network component comes up late or a network component comes up again (reboot), connectivity loss duration time caused by the reconfiguration of the network shall be equal to or less than the value of the recovery time requirement.
- Forwarding loop shall not be formed in any time to avoid broadcast storm for instance.

MRP defined in IEC 62439 may be used to manage ring topology. Ladder topology protocol defined in Annex D may be used to manage ladder topology.

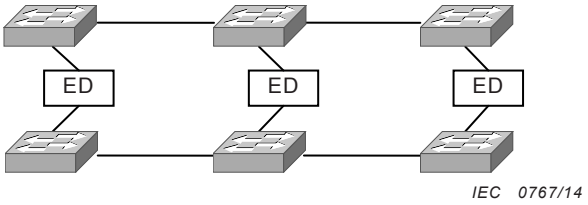
4.5.4 Redundancy managed at End Device level

Availability-critical End Devices should have redundancy managed at End Device level, having redundant links to the network. End Device can continue to communicate in case of failure on one of the redundant links. If redundant links are connected to multiple Consist Switches, the device can continue to communicate in case of a Consist Switch failure. End Device has typically two links, which is called dual homing. End Device in dual homing shall use separate physical network interfaces and shall not create loop on the ECN. Unmanaged switch shall not be used to emulate dual homing scheme. Examples with dual homing are shown in Figure 4.

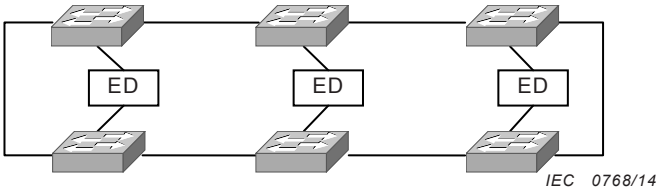
One example of using dual homing is that packets are duplicated and sent from both interfaces. On receiving the packets, the device accepts the packet that is received first and discards another one. In order to identify the duplicated packets, they may have the sequence number field in the messages. In case this method is used, disruption of communication does not happen in case of a failure.

It can be also possible that one of the redundant links of the End Device is used and the other link takes over in case of the link failure. In this case switch over between redundant links may be recognized as switch over between redundant devices from other devices. In case this method is used, disruption of communication may occur in case of a failure.

1) Dual homing in parallel networks



2) Dual homing in ring topology



3) Dual homing in ladder topology

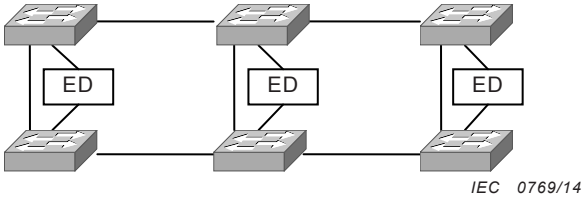


Figure 4 – Examples of dual homing

4.6 Quality of service

4.6.1 General

ECN shall be able to provide QoS by prioritizing traffic when it is necessary from application requirements.

Quality of service shall be provided by Consist Switches, and End Device can assign priorities to the packets which the End Device transmits if necessary.

NOTE Assigning priorities to the packets by Consist Switches, for example according to the ports, protocols, and addresses, is not prohibited.

4.6.2 Priority level

According to IEEE 802.1D there are 8 priority levels, the highest priority level is 7 and the lowest priority level is 0. Default priority level shall be 0.

Consist Switches shall support 2 priority queues at minimum when QoS is provided. When 2 priority queues are supported, priority levels from 0 to 3 and 4 to 7 can be grouped respectively. When 4 priority queues are supported, priority levels from 0 to 1, 2 to 3, 4 to 5, and 6 to 7 can be grouped respectively.

Mapping of priority levels to data classes shall be determined according to the requirements from applications used in the ECN since data classes to be used and their performance

parameters depend on applications. Table 7 shows a default mapping of priorities to each data class in case of four priorities.

In case of communication over ETB, priority level of a packet shall conform to IEC 61375-2-5.

Table 7 – Mapping of priorities to data classes

Priority	Priority level in binary (X: do not care)	Data class	Requirement (M: Mandatory R: Recommended)
Highest	11X	Supervisory Data	M
2nd highest	10X	Process Data	R
3rd highest	01X	Message Data and Stream Data	R
Lowest (default)	00X	Best Effort Data	M

NOTE 1 Priorities for specific Process Data, Message Data and Stream Data are defined in IEC 61375-2-3.

NOTE 2 If bandwidth of data classes with higher priorities is not limited, lower priority data can have no chance to be transmitted.

4.6.3 Assignment of priority level

When End Device assigns priorities to the sending packets, the End Device should use DSCP field in IP datagram as defined in RFC2474. End Device may use Priority Code Point field in tagged MAC frame.

The binary representation of DSCP field shall be as follows.

LLL000

where

LLL: priority level (0-7) defined in 4.6.2

4.6.4 Consist Switch behavior

When Consist Switch supports quality of service, Consist Switch shall be able to evaluate the priority level of the packet as defined 4.6.3 and queue the packet according to the priority level and number of queues it has as defined in IEEE 802.1D.

When Consist Switch supports quality of service, Consist Switch should support strict priority based switching on all of priority queues; i.e. all higher priority frames shall egress from port before the lower priority frames egress.

4.6.5 Ingress rate limiting

Ingress rate limiting is an optional feature of the Consist Switch. Consist Switch provides possibility to limit the rate of frames ingressing from End Devices or from TBNs.

If frames need to be discarded to keep the rate limit, low priority frames shall be discarded first.

NOTE Ingress rate limiting prevents the ECN from being unintentionally flooded with frames originating from one faulty ED for instance.

4.6.6 Egress rate shaping

Egress rate shaping is an optional feature of the Consist Switch. Consist Switch provides the possibility to limit the rate of frames egressing to End Devices or to TBNs.

If frames need to be discarded to keep the rate limit, low priority frames shall be discarded first.

4.7 IP address and related definitions

4.7.1 Consist Network address

Each communication device which supports IP communication and is connected to ECN shall have one or several IP address(es) as Consist Network address(es). The Consist Network address shall be unique within a Consist Network.

NOTE Communication devices connected to different Consist Networks can have identical or different Consist Network addresses.

Consist Network address shall use IPv4 private address space defined in IETF RFC1918, class A private address should be used.

When

– class A private address is used, and
– ECN is connected to ETB, and
– Consist Network address is not identical to train network address,

addresses from 10.0.0.0 to 10.127.255.255 (10.0/9) shall be used. The binary presentation shall be following.

00001010.0ddddddd.dddddddd.dddddddd / 9

Where:

Notation	Description
[d]	This field is used freely for host identification in the ECN. This field could be divided, for example; – ECN is divided into sub-networks, – uses same values of train network address in most three significant bits for identifying multiple ECNs, or – uses only lower 14 bits for ensuring NAT is possible. (R-NAT in Annex B is one example) NOTE When using R-NAT, devices have IP address rationally within only 14 bits. If within deterministic fixed EMU train, following assign method is helpful for unification without confusion. This method also contributes prefixed IP address assignment for End Devices. Lower 14 bits: r.ccccc.eeeeeeee r: Redundancy/Subnet identifier 0/1 c: Car Number 1 to 31 (sufficient number for fixed EMU) e: End Device identifier 1 to 255 (sufficient number within a car)

This subnet (10.0/9) applied in ECN is called a local ECN subnet.

4.7.2 Train Network Address

Train wide addressing of a communication device shall be possible with a train network address which is unique in the train if the ECN is connected to ETB. Train network address may change with each train inauguration. It is not mandatory for all communication devices to

be addressable train widely, for many of them local ECN address is enough. Source and destination addresses in the communication on ETB shall be train network addresses. Train network address and Consist Network address may be identical.

If train network address is not identical to Consist Network address, ECN shall support a service which maps train network addresses to Consist Network addresses. Addresses which do not conform to specifications for train network address shall not be used as source or destination addresses in ETB as defined in IEC 61375-2-5.

NOTE Network Address Translation (NAT) and Application Layer Gateway (ALG) including proxy are typical services for mapping addresses.

Train network address shall use IPv4 private address defined in IETF RFC 1918 and follow the definitions in IEC 61375-2-5. The binary presentation of train network address shall be as follows.

00001010.1bbxssss.sshhhhhh.hhhhhhhh / 18

Where:

Notation	Description
[b]	Identifier of the ETB which the ECN connects to.
[x]	Reserved. Shall be 0.
[s]	Consist Network identification assigned according to the results of inaugurations. Value 0 is reserved for ETB backbone subnet.
[h]	Unique host identification inside ECN, up to 16382 hosts by Consist. Some upper bits could be used to define internal dedicated Consist local subnets. In this case, address mask (at ECN side) should take in account this decomposition (shall be extended).

4.7.3 Group Address

Communication devices may be grouped on Consist level or train level. Communication devices may belong to several groups. On Consist level all members of the group belong to one Consist Network. Consist group addresses assigned to those groups shall be unique within the Consist Network. Memberships of Consist groups are normally static. On train level all members of the group belong to one or several Consist Networks. Train group addresses assigned to those groups shall be unique within the train. Memberships of train groups may change with each train inauguration.

Group address shall be IP multicast address defined in IETF RFC 2365.

When ECN is connected to ETB, IP multicast address at ECN level shall be 239.255.0.0/16 (local scope defined in RFC 2365).

IP multicast address at train level is 239.192.0.0/14 (organization scope defined in RFC 2365) as defined in IEC 61375-2-5.

TBN shall not forward IP multicast datagram to ETB if the destination address is an IP multicast address at ECN level.

4.7.4 Name resolution and naming definitions

4.7.4.1 Name resolution

Name resolution for Consist Network addresses and train network addresses should be implemented by local database in the communication device or by DNS.

ECN should provide DNS server function. Location of the server depends on implementation; servers could be implemented on any End Devices and Network Devices in the ECN or on TBNs which the ECN is attached to. In case that the ECN is attached to ETB, it is recommended that the server is implemented in TBN. DNS server should be redundant.

Each communication device which could be a destination device for communication over ETB shall be addressable in train wide domain name space.

NOTE Train wide domain name space is managed according to IEC 61375-2-5, “ltrain” for example.

4.7.4.2 End Device self-identification

For self-addressing End Device internal hostname shall be declared:

“localhost” 127.0.0.1

4.7.4.3 End Device local identification

By default, all hosts are declared in “lcst” domain which is local to each ECN.

EXAMPLE “mpu” or “mpu.lcst.” are associated with the same local End Device “mpu” IP address.

4.8 IP address and network configuration management

4.8.1 Consist Network address management

Consist Network address in a device can be configured statically or dynamically.

When Consist Network address is configured dynamically, DHCP should be used.

When DHCP is used, ECN shall provide DHCP server function. Location of the server depends on implementation; servers could be implemented on any End Devices and Network Devices in the ECN or on TBNs which the ECN is attached to. In case that the ECN is attached to ETB, it is recommended to be implemented in TBN. DHCP server should be redundant.

4.8.2 Train network address management

When train network IP address is assigned to a device, the device may or may not configure the train network address to its Ethernet port.

TBN as a router shall support NAT to map the train network addresses to the Consist Network addresses for devices which do not configure the train network addresses at their own Ethernet interfaces. R-NAT defined in Annex B can be used to simplify the address translation algorithm at TBNs.

Since NAT may cause problems for specific protocols, e.g. necessity for replacing addresses in the payload of IP datagrams, an extended NAT dealing with the problems should be used for specific protocols. Otherwise, End Devices which are addressable by train network addresses should have IP alias function; i.e. two different IP addresses can be configured to one Ethernet interface. Local ECN addresses are used for communications local in ECN, and train network addresses are used for communications over ETB. TBN shall be able to forward IP datagram according to the destination address which is train network address.

After a new inauguration, renewal of train network address is mandatory. This is applied to train network addresses managed at each communication device and train network addresses managed in various services including routing, NAT, DHCP server, and DNS server.

In case that train network addresses are managed by End Devices with DHCP client, End Devices and DHCP servers shall support DHCP FORCERENEW message defined in IETF RFC 3203. DHCP servers shall send FORCERENEW message to DHCP clients with train

network addresses after inauguration, and DHCP clients shall renew train network addresses on receiving the FORCERENEW message.

NOTE Inauguration occurrence is limited to startup initialization, coupling and uncoupling time. Losing or finding a router at train level does not always have as consequence a new inauguration. Changing train IP address decision is always under train application responsibility acknowledgement. See IEC 61375-2-5.

4.8.3 Static network configuration parameters

Table 8 shows network configuration parameters for End Devices when static network address configuration is used.

Table 8 – End Device static network configuration parameters

(M: Mandatory, C: Conditional, O: Optional)

Parameter	Type	Description
Hostname	M	Hostname shall be unique in an ECN.
Default domain name	C	This is mandatory when DNS is used. For the definition of domain name, see 4.7.4.
IPv4 address	M	For the definition of Consist Network address, see 4.7.
IPv4 address mask	M	For the definition of Consist Network address, see 4.7.
IPv4 DNS server address	C	This is mandatory when DNS is used.
IPv4 default route	O	TBN is a typical default gateway.
IPv4 static route	O	Could be used to access specific devices and subnets.

4.8.4 DHCP configuration parameters

Table 9 shows requirements for DHCP options to be supported when DHCP is used.

Table 9 – DHCP options

(M: Mandatory, C:Conditional, O: Optional)

Option number	Require-ment	Name	Description
1	M	Subnet mask	IPv4 address mask
3	M	Router option	List of IPv4 routers available on the subnet
6	C	Domain Name server option	List of DNS server addresses. This is mandatory for EDs when DNS is used.
12	O	Host Name option	Name of the DHCP client
28	O	Broadcast Address option	Broadcast address in use on the DHCP client's subnet
42	C	Network time protocol servers option	List of NTP server addresses. This is mandatory for EDs when NTP or SNTP is used.
43	O	Vendor Specific Information	This is used to exchange vendor specific information between servers and clients. This option may be supported.
51	M	IP address lease time	Allowed lease time for the assigned IP address
53	M	DHCP message type	Shall be used to identify the type of the DHCP message
54	M	Server Identifier	This option is used to identify the DHCP server address.
55	M	Parameter request list	Could be used for DHCP client to request specific configuration parameters.
56	O	Message	This option is used to send error message from the DHCP server to DHCP clients. DHCP client may use this option to indicate the reason of declining the offer.
61	O	Client-Identifier	DHCP client fills unique identifier. This option can be used to keep the same IP address for the DHCP client, see NOTE.
82	O	Relay Agent Information option	This option may be used to indicate the location of the DHCP client.
NOTE In order to keep always the same IP address from the DHCP server, depending on the location or device type of End Devices, End Device sends DHCP option 61 (client-identifier) or the Consist Switch where the End Device is connected inserts DHCP Option 82 defined in IETF RFC 3046.			

4.8.5 IP address management for TBN redundancy

To manage Train Backbone connection redundancy inside an ECN, ECN could be connected by more than one TBN to the Train Backbone.

TBN redundancy is managed conforming to WTB or ETB.

When a redundant TBN group is implemented and the TBNs are routers between ECN and Train Backbone, the redundant TBN group shall export a common Consist Network address for the routing service at ECN side. When a new TBN is elected as an active router, the TBN shall send a gratuitous ARP to the ECN in order to update ARP tables in End Devices.

4.9 Network Device interface

4.9.1 General

Subclause 4.9 defines interfaces for Network Devices; i.e. repeaters, Consist Switches, and routers. A Consist Switch and a router could act as an End Device; in that case they also shall conform to End Device interfaces in network layer and other upper layers defined in 4.10.

There are two classes of Consist Switches as defined in 4.2.4; Unmanaged Consist Switches and Managed Consist Switches. Managed Consist Switch shall support all the requirements for the Unmanaged Consist Switch.

4.9.2 Function requirements

Table 10 shows the summary of Consist Switch interfaces; details are described in the following subclauses.

Table 10 – Summary of Network Device interfaces

Status in (M: Mandatory, O: Optional, C: Conditional, -: Not available or not required)

Layer	Requirements	Status				References and notes
		Repeater	Unmanaged CS	Managed CS	Router	
Physical Layer for ED connection	100BASE-TX	-	M	M	-	IEEE 802.3
	10BASE-T	-	O	O	-	IEEE 802.3
	Full Duplex Mode	-	M	M	-	IEEE 802.3
	Auto Negotiation	-	C	C	-	IEEE 802.3 For Temporary ED only
	MDI/MDI-X auto crossover	-	O	O	-	
	Power over Ethernet (PoE)	-	O	O	-	IEEE 802.3
	Class D (Category 5e), STP cable with 2 twisted pairs	-	O	O	-	ISO/IEC 11801 IEC 61156-6
	Class D (Category 5e), UTP cable with 2 twisted pairs	-	O	O	-	ISO/IEC 11801 IEC 61156-6
	M12 D-coded connector (socket)	-	O	O	-	IEC 61076-2-101
	IEC 61076-3-104 socket (outlet)	-	O	O	-	IEC 61076-3-104
	RJ45 connector (socket)	-	O	O	-	TIA/EIA-568-B For Temporary ED only
Physical Layer for ND connection	IEEE 802.3 physical layer	C	C	C	C	IEEE 802.3 Mandatory if transceiver with amplified signals is not used 100BASE-TX is recommended
	Transceiver with amplified signals	O	O	O	O	Annex B See NOTE 1
	Full Duplex Mode	-	M	M	M	IEEE 802.3

Layer	Requirements	Status				References and notes
		Repeater	Unmanaged CS	Managed CS	Router	
	Auto Negotiation	-	O	O	O	IEEE 802.3
	MDI/MDI-X auto crossover	O	O	O	O	
	Class D (Category 5e), STP cable with 2 twisted pairs	O	O	O	O	ISO/IEC 11801 IEC 61156-6 For 100BASE-TX and 10BASE-T
	Class D (Category 5e), UTP cable with 2 twisted pairs	O	O	O	O	ISO/IEC 11801 IEC 61156-6 For 100BASE-TX and 10BASE-T
	M12 D-coded connector (socket)	C	C	C	C	IEC 61076-2-101 For 100BASE-TX and 10BASE-T
Link Layer	MAC services with basic/tagged MAC frame	-	M	M	M	IEEE 802.3
	Flow control	-	O	O	-	IEEE 802.3
	Frame relaying	-	M	M	-	IEEE 802.1D
	Frame filtering	-	M	M	-	IEEE 802.1D
	VLAN services	-	M	M	-	IEEE 802.1Q
	Frame queueing	-	M	M	-	IEEE 802.1D
	Frame tagging/untagging	-	M	M	-	IEEE 802.1D
	Management and remote management	-	-	M	-	IEEE 802.1D
	Ingress rate limiting	-	O	O	-	
	Egress rate shaping	-	O	O	-	
	Port mirroring	-	O	O	-	
Network Layer	IP version 4	-	-	M	M	IETF RFC 791
	IPv4 forwarding	-	-	-	M	
	ICMP	-	-	M	M	IETF RFC 792
	ARP	-	-	M	M	IETF RFC 826
Transport Layer	UDP	-	-	M	M	IETF RFC 768
	TCP	-	-	M	M	IETF RFC 793
	IGMP version 2/3 (router)	-	-	-	O	IETF RFC 2236,3376
	IGMP version 2 (host)	-	-	M	O	IETF RFC 2236
	IGMP version 3 (host)	-	-	O	O	IETF RFC 3376
	IGMP snooping	-	-	M	-	IETF RFC 4541
Application Layer	DHCP (client)	-	-	C	C	IETF RFC 2131
	DHCP Relay Agent Information option	-	-	O	-	IETF RFC 3046
	DHCP (server)	-	-	O	O	IETF RFC 2131
	DNS (client)	-	-	C	C	IETF RFC 1034,1035
	DNS (server)	-	-	O	O	IETF RFC 1034,1035
	SNTP (client)	-	-	O	O	IETF RFC 1361
	NTP version 3 (client)	-	-	O	O	IETF RFC 1305

Layer	Requirements	Status				References and notes
		Repeater	Unmanaged CS	Managed CS	Router	
	NTP version 3 (server)	-	-	O	O	IETF RFC 1305
	SNMP version 2 (agent)	-	-	O	O	IETF RFC 1901

NOTE 1 If transceiver with amplified signal, which is additionally attached to the physical layer conforming to IEEE 802.3, is used, IEEE 802.3 physical layer is not mandatory.

NOTE 2 The Network Device interface for the ladder topology defined in Annex D contains the exceptions which are not compliant to IEEE 802.3 or IEEE 802.1D.

4.9.3 Performance requirements

Consist Switch shall support at minimum 2 priority queues as defined in 4.6.2.

Consist Switch should support strict priority based switching on all of priority queues as defined in 4.6.4.

4.9.4 Physical Layer

4.9.4.1 Protocols

4.9.4.1.1 Network Device interface for End Devices

Network Device interface for connecting End Devices shall support 100BASE-TX, and 10BASE-T could be additionally supported in order to increase electric robustness and EMC immunity for example.

- 100BASE-TX Physical Layer
  - Physical Coding Sublayer (PCS) and Physical Medium Attachment (PMA) sublayer, type 100BASE-X, defined in IEEE 802.3
  - Physical Medium Dependent (PMD) sublayer and baseband medium, type 100BASE-TX, defined in IEEE 802.3
- 10BASE-T Physical Layer
  - Twisted-pair medium attachment unit (MAU) and baseband medium, type 10BASE-T, defined in IEEE 802.3

Full Duplex mode, which is defined in IEEE 802.3, shall be supported to avoid collisions.

Auto negotiation function, which is defined in IEEE 802.3, shall be able to be supported for connecting Temporary End Devices. It is not recommended to be used for connecting Standard End Devices in order to avoid connection with unintended speed or duplex mode is established.

MDI/MDI-X automatic crossover function, which automatically configures MDI or MDI-X, may be supported.

Auto-polarity function is not recommended to be used due to the specific solution.

Power Sourcing Equipment (PSE) of Power over Ethernet (PoE), which is defined in IEEE 802.3, may be supported.

4.9.4.1.2 Network Device interface for other Network Devices

Network Device interface for connecting other Network Devices shall support physical layer defined in IEEE 802.3 when optional transceiver with amplified signal is not applied.

100BASE-TX is preferred, but 10BASE-T could be additionally supported in order to increase electric robustness and EMC immunity for example.

In order to raise noise immunity further, the transceiver with amplified signals could be optionally attached to 100BASE-TX PMD or 10BASE-T MAU, which is defined in Annex C.

1000BASE or higher interface could be used in order to support more bandwidth.

Full Duplex mode, which is defined in IEEE 802.3, shall be supported to avoid collisions.

Auto negotiation function, which is defined in IEEE 802.3, is not recommended to be used in order to avoid connection with unintended speed or duplex mode is established.

MDI/MDI-X automatic crossover function, which automatically configures MDI or MDI-X, may be supported.

Auto-polarity function is not recommended to be used due to the specific solution.

4.9.4.2 Cables

This subclause shall be applied when 100BASE-TX or 10BASE-T is used.

Cables shall conform to ISO/IEC 11801 and IEC 61156-6. Class D (Category 5e) with two twisted pairs shall be supported.

Shielded twisted pair (STP) cable should be used. Unshielded twisted pair (UTP) cable may be used.

Cable gauge recommended for intra-car connection is 0,5 mm^2 (AWG20), 0,34 mm^2 (AWG22), or 0,25 mm^2 (AWG24).

Cable gauge recommended for inter-car connection is 0,5 mm^2 (AWG20), or a higher surface.

4.9.4.3 Connectors

4.9.4.3.1 Network Device interface for End Devices

This subclause defines requirements for connectors used for connecting End Devices. This subclause shall be applied when 100BASE-TX or 10BASE-T is used.

M12 D-coded connector (socket), defined in IEC 61076-2-101, should be supported on the Network Device side. In this case, M12 D-coded plug connector shall be used on the cable side.

IEC 61076-3-104 socket (outlet) can be used on the Network Device side. In this case, IEC 61076-3-104 plug connector shall be used on the cable side.

RJ45 socket, defined in TIA/EIA-568-B, can be used for connecting Temporary End Devices on the Network Device side. In this case RJ45 plug connector shall be used on the cable side.

Figure 5 illustrates the connectors. Pinning for M12 connector shall be as illustrated in Table 11.

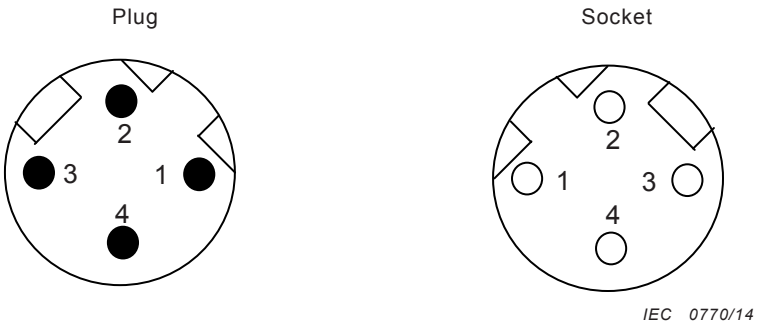


Figure 5 – D-coded M12 connector

Table 11 – Pinning for D-coded M12 connector

Pin	Signal
1	TD+
2	RD+
3	TD-
4	RD-

4.9.4.3.2 Network Device interface for other Network Devices

This subclause defines requirements for connectors used for connecting Network Devices. This subclause shall be applied when 100BASE-TX or 10BASE-T is used.

M12 D-coded connector (socket), defined in IEC 61076-2-101, shall be supported on the Network Device side. M12 D-coded plug connector shall be used on the cable side.

4.9.4.4 Shielding and grounding concepts

4.9.4.4.1 Intra Car shielding concepts

Inside a car, all shields of cables should be referred and connected to the mechanical earth of the car. To prevent EMC influences, a cable shield should be connected on a 360° circular basis in the connector.

4.9.4.4.2 Inter Car shielding concepts

Two use cases should be considered:

– The two adjacent cars are at the same potential
– The two adjacent cars are at a different potential

When the two adjacent cars are at the same potential, the Ethernet cable shield should have continuity and no interruption of shielding should be necessary.

When the two adjacent cars are at the different potential, the Ethernet cable shield should be interrupted to avoid ground current flowing between cars.

4.9.5 Link Layer

4.9.5.1 Consist Switch

Mandatory requirements for Consist Switches are defined in the following.

MAC service with basic (untagged) and tagged frame, which is defined in IEEE 802.3, shall be supported.

Frame relaying, which is defined in IEEE 802.1D, shall be supported. Frame relaying provides frame reception, frame transmission, and frame forwarding.

Frame filtering, which is defined in IEEE 802.1D, shall be supported. Frame filtering provides learning of addresses and filtering database.

VLAN service, which is defined in IEEE 802.1Q, shall be supported by Consist Switches.

Frame queueing, which is defined in IEEE 802.1D, shall be supported by Consist Switches. Frame queueing can handle multiple data classes during frame relaying to achieve quality of service.

NOTE When frame queueing is supported, Consist Switch reads DSCP field as defined in 4.6.

Frame tagging and untagging, which is defined IEEE 802.1Q, shall be supported by Consist Switches. Frame tagging can insert the tag in the basic (untagged) frame for the ingress ports, and frame untagging can remove the tag from the tagged frame for the egress port.

Mandatory requirements only for Managed Consist Switches are defined in the following.

Management and remote management, which are defined in IEEE 802.1D, shall be supported by Managed Consist Switches.

Optional requirements for Consist Switches are defined in the following.

Flow control, which is defined as MAC Control PAUSE operation in IEEE 802.3, may be supported. Flow control provides the ability to inhibit transmission of frames.

Ingress rate limiting and egress rate shaping, which are defined in 4.6.5 and 4.6.6, may be supported.

Port mirroring, which configures one or more ports to mirror the traffic from another port(s), may be supported.

4.9.5.2 Router

Routers shall support Link Layer requirements to End Device, see 4.10.

4.9.6 Network Layer

Managed Consist Switches and routers shall support Network Layer requirements to End Devices, see 4.10.

Routers shall additionally support IP (version4) forwarding.

4.9.7 Transport Layer

Managed Consist Switches and routers shall support Transport Layer requirements to End Devices, see 4.10.

Routers should support IGMP version 2 router requirements defined in IETF RFC 2236, and may support IGMP version 3 router requirements defined in IETF RFC 3376.

Managed Consist Switches shall support IGMP version 2 host requirements and may support IGMP version 3 host requirements.

NOTE IGMP version 3 is interoperable with IGMP version2 and version1. IGMP version 3 additionaly supports source filtering.

IGMP snooping, which is defined in IETF RFC 4541, shall be supported by Managed Consist Switches. IGMP snooping filters multicast frames destined to switch ports to which no multicast group members are connected.

4.9.8 Application layers

Managed Consist Switches and routers shall support Application layer requirements to End Devices, see 4.10

DHCP Relay Agent Information Option, which is defined in IETF RFC 3046, may be supported by Managed Consist Switches. Consist Switches may act as Relay Agents in order to assign specific IP addresses according to the information inserted by Consist Switches.

4.10 End Device interface

4.10.1 General

Subclause 4.10 defines interfaces for End Devices.

Table 12 shows the summary of End Device interfaces; details are specified in the following subclauses. There are four classes of End Devices as defined in 4.2.3.

Table 12 – Summary of End Device interfaces

Status in (M: Mandatory, O: Optional, C:Conditional)

Layer	Requirements	Status				References and notes
		Temporary	Consist Local	Train Communi-cation	Train Topology aware	
Physical Layer	100BASE-TX	M	M	M	M	IEEE 802.3
	10BASE-T	O	O	O	O	IEEE 802.3
	Full Duplex Mode	M	M	M	M	IEEE 802.3
	Auto Negotiation	M	O	O	O	IEEE 802.3
	MDI/MDI-X auto crossover	O	O	O	O	
	Power over Ethernet (PoE)	O	O	O	O	IEEE 802.3
	Class D (Category 5e), STP cable with 2 twisted pairs	O	O	O	O	ISO/IEC 11801 IEC 61156-6
	Class D (Category 5e), UTP cable with 2 twisted pairs	O	O	O	O	ISO/IEC 11801 IEC 61156-6
	M12 D-coded connector (socket)	O	O	O	O	IEC 61076-2-101
	IEC 61076-3-104 socket (outlet)	O	O	O	O	IEC 61076-3-104
	RJ45 connector (socket)	O	O	O	O	TIA/EIA-568-B
Link Layer	MAC services with basic MAC frame	M	M	M	M	IEEE 802.3
	MAC services with tagged MAC frame	O	O	O	O	IEEE 802.1Q
Network Layer	IP version 4	M	M	M	M	IETF RFC 791
	ICMP	M	M	M	M	IETF RFC 792
	ARP	M	M	M	M	IETF RFC 826
Transport Layer	UDP	M	M	M	M	IETF RFC 768
	TCP	M	M	M	M	IETF RFC 793
	IGMP version 2/3 (host)	O	O	O	O	IETF RFC 2236, 3376
Application Layer	DHCP (client)	O	O	C	C	IETF RFC 2131
	DHCP (server)	O	O	O	O	IETF RFC 2131
	DNS (client)	O	O	O	M	IETF RFC 1034, 1035
	DNS (server)	O	O	O	O	IETF RFC 1034, 1035
	SNTP (client)	O	O	O	O	IETF RFC 1361
	NTP version 3 (client)	O	O	O	O	IETF RFC 1305
	NTP version 3 (server)	O	O	O	O	IETF RFC 1305
	SNMP version 2 (agent)	O	O	O	O	IETF RFC 1901
	Telnet or SSH server	O	O	O	O	IETF RFC 854 IETF RFC 4251

4.10.2 Physical Layer

4.10.2.1 Protocols

The Physical Layer shall conform to IEEE 802.3 standard. 100BASE-TX shall be supported, and 10BASE-T could be used in order to increase electric robustness and EMC immunity for example.

- 100BASE-TX Physical Layer
  - Physical Coding Sublayer (PCS) and Physical Medium Attachment (PMA) sublayer, type 100BASE-X, defined in IEEE 802.3
  - Physical Medium Dependent (PMD) sublayer and baseband medium, type 100BASE-TX, defined in IEEE 802.3
- 10BASE-T Physical Layer
  - Twisted-pair medium attachment unit (MAU) and baseband medium, type 10BASE-T, defined in IEEE 802.3

Full Duplex mode, which is defined in IEEE 802.3, shall be supported to avoid collisions.

Auto negotiation function, which is defined in IEEE 802.3, shall be supported for connecting Temporary End Devices. It is not recommended to be used for connecting Standard End Devices in order to avoid connection with unintended speed or duplex mode is established.

MDI/MDI-X automatic crossover function, which automatically configures MDI or MDI-X, may be supported.

Auto-polarity function is not recommended to be used due to the specific solution.

Power Device (PD) in Power over Ethernet (PoE), which is defined in IEEE 802.3, may be supported.

4.10.2.2 Cables

Cables shall conform to ISO/IEC 11801 and IEC 61156-6. Class D (Category 5e) with two twisted pairs shall be supported.

Shielded twisted pair (STP) cable should be used. Unshielded twisted pair (UTP) cable may be used.

Cable gauge recommended is 0,5 mm^2 (AWG20), 0,34 mm^2 (AWG22), or 0,25 mm^2 (AWG24).

4.10.2.3 Connectors

For the Standard End Device M12 D-coded connector (socket), defined in IEC 61076-2-101, should be supported on the End Device side. In this case, M12 D-coded plug connector shall be used on the cable side.

IEC 61076-3-104 socket (outlet) can be used on the End Device side. In this case, IEC 61076-3-104 plug connector shall be used on the cable side.

RJ45 socket, defined in TIA/EIA-568-B, can be used for the Temporary End Device on the End Device side. In this case RJ45 plug connector shall be used on the cable side.

Figure 5 in 4.9.4.3 illustrates the connectors. Pinning shall be as illustrated in Table 11.

4.10.2.4 Shielding and grounding concepts

All shields of cables should be referred and connected to the mechanical earth of the car. To prevent EMC influences, a cable shield should be connected on a 360° circular basis in the connector.

4.10.3 Link Layer

MAC in the Link Layer shall conform to IEEE 802.3 standard.

MAC service with basic frame, which is defined in IEEE 802.3, shall be supported.

MAC service with tagged frame, which is defined in IEEE 802.1Q, may be supported.

4.10.4 Network layer

IP version4, which is defined in IETF RFC 791, shall be supported.

ICMP, which is defined in IETF RFC 792, shall be supported.

ARP, which is defined in IETF RFC 826, shall be supported.

NOTE See 4.6 for setting DSCP value by End Devices.

4.10.5 Transport Layer

UDP, which is defined in IETF RFC 768, shall be supported.

TCP, which is defined in IETF RFC 793, shall be supported.

IGMP version 2 host requirements should be supported, and IGMP version 3 host requirements may be supported.

4.10.6 Application layer

DHCP client function, which is defined in IETF RFC 2131, may be supported. In case that Train Communication End Devices and Train Topology aware End Devices manage train network addresses by themselves, DHCP shall be supported.

DNS client function, which is defined in IETF RFC 1034, may be supported for mapping between IP addresses and names (such as hostnames and function names represented in FQDN). Train Topology aware End Devices shall support DNS client function to resolve train network addresses from hostnames or function names; train network addresses may change by inaugurations.

SNTP client function which is defined in IETF RFC 1361 or NTP version 3 client function which is defined in IETF RFC 1305 may be supported for synchronizing the time. When NTP is used ECN shall provide NTP server function. Location of the server depends on implementation, but it is recommended to be implemented in TBN.

Other protocols such as FTP defined in IETF RFC 959, HTTP defined in IETF RFC 2616, and TFTP defined in IETF RFC 1350 may be supported.

SNMP version 2 agent function, which is defined in IETF RFC 1901, 1905 and 1906, should be supported.

Telnet server (IETF RFC 854) or SSH server (IETF RFC 4251 or others) may be implemented in order to manage End Devices.

NOTE 1 Information regarding train topology are specified in IEC 61375-2-3 and/or IEC 61375-2-4.

NOTE 2 Protocols delivering Process Data and Message Data defined in IEC 61375-2-3 can be used inside ECN.

NOTE 3 Any protocols delivering Process Data and Message Data can be used inside ECN.

4.11 Gateway functions

4.11.1 WTB gateway functions

Gateway functions between ECN and WTB shall be implemented in the TBN if the TBN is connected to the WTB defined in IEC 61375-2-1.

TBN between ECN and WTB is implemented as an Application Layer gateway (ALG). Figure 6 illustrates logical structure of the TBN.

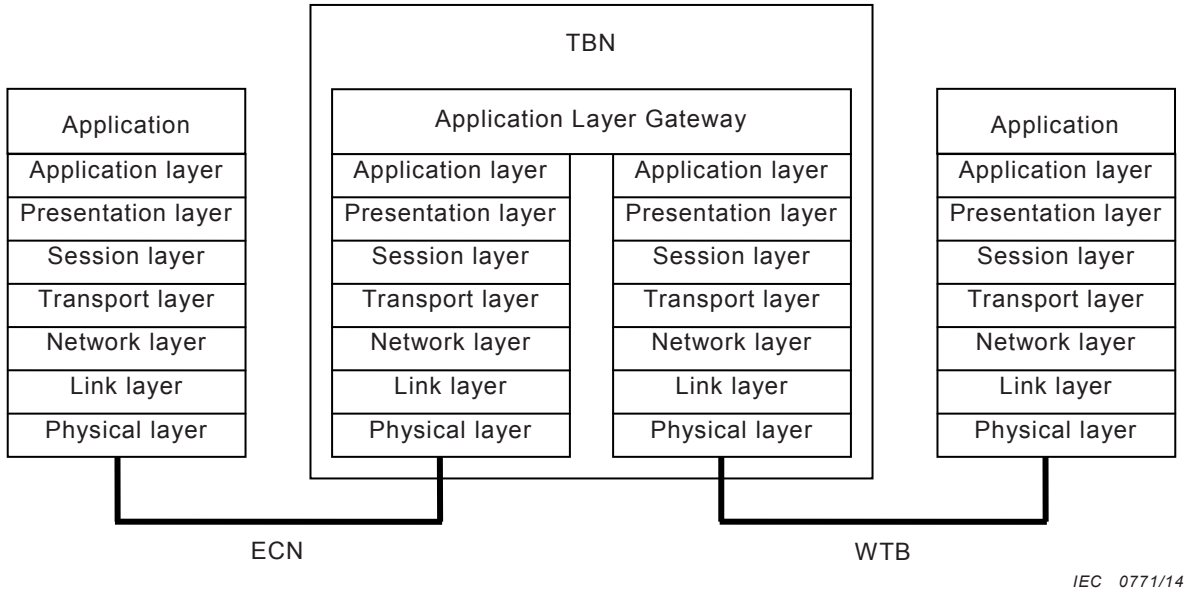


Figure 6 – Logical structure of the gateway between ECN and WTB

4.11.2 ETB gateway functions

Gateway functions between ECN and ETB shall be implemented in the TBN if the TBN is connected to the ETB defined in IEC 61375-2-5.

TBN between ECN and ETB is implemented as a router and/or as an Application Layer gateway (ALG).

If train network address assigned to the communication device in ECN is not identical to Consist Network address, TBN shall support a service which maps train network address to Consist Network address(es) as defined in 4.7. Addresses which do not conform to specifications for train network address shall not be used as source or destination addresses outside the ECN. Network address translation (NAT) defined in IETF RFC 3022 is the typical implementation when this mapping is implemented in the routing function of the TBN. See 4.8.

A redundant pair of TBNs shares an IP address at ECN side as a gateway address between ECN and ETB. See 4.8.5.

4.12 Network management

4.12.1 ECN network management

Communication devices in ECN should support SNMP agent functions for network management. SNMPv2 defined in IETF RFC 1901, 1905 and 1906 is the minimum requirement.

Standards MIBs defined in IETF RFC 1213 should be supported.

4.12.2 WTB network management

TNM functions for WTB shall be implemented in the TBN if the TBN is connected to the WTB defined in IEC 61375-2-1.

ECN network management services defined in 4.12.1 should be accessible by TNM function for the WTB.

4.12.3 ETB network management

SNMP is used to manage communication devices on ETB as defined in IEC 61375-2-5.

SNMP agent services implemented on communication devices in the ECN should be accessible through ETB.

5 Conformance test

To claim conformance to this part of the standard, equipments are expected to pass a suite of tests. The equipments to be tested shall include

- End Device,
- Network Device, and
- TBN.

NOTE TBN is also compliant with IEC 61375-2-1 or IEC 61375-2-5.

The conformance test plan for ECN is not in the scope of this part of the standard.

Annex A
(informative)

Reliability and availability comparison between ECN architectures

A.1 General

This annex shows reliabilities and availabilities in various ECN architectures to help select the appropriate ECN architecture. Examples of tolerant (and intolerant) failure cases of typical network topologies are described. Formulas calculating reliability and availability are also described.

A.2 Failure cases

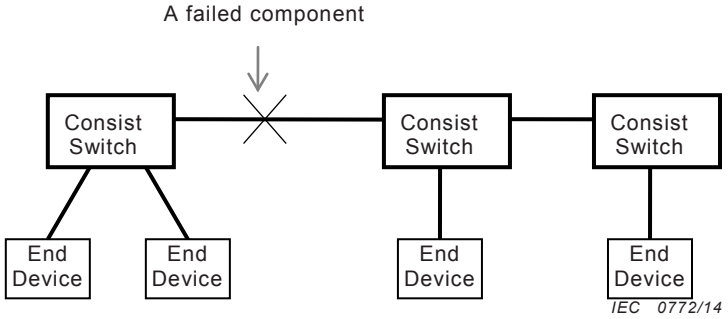
A.2.1 Definitions

A failure case is defined as one of the variations of the failure network components in number and location.

The term single network component failure means the condition in which one of the network components stops working as shown in Figure A.1.

The term double network component failures means the condition in which two of the network components stop working at a time as shown in Figure A.2.

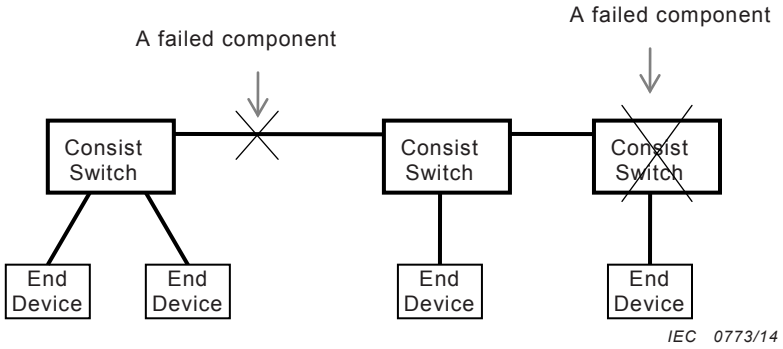
NOTE Network component is defined in 4.5.2.1; active component of network device, link between active components or link for End Device.



NOTE 1 A cross marked component indicates a failed component.

NOTE 2 Bold boxes and bold lines indicate network components.

Figure A.1 – Example of single network component failure



NOTE 1 A cross marked component indicates a failed component.

NOTE 2 Bold boxes and bold lines indicate network components.

Figure A.2 – Example of double network component failures

In case of network component failure(s) condition of the network can change to one of the following states from normal state which has no failure in the network.

– Malfunction state. In this state the network is separated.
– Partially functioning state. In this state the network is not separated, but the network cannot provide the same services as normal state.
– Fully functioning state. In this state the network can provide the same services as normal state.

A.2.2 Example of failure cases – Linear topology

Linear topology is not tolerant of single network component failure as shown in Figure A.3.

If a bypass function is applied to each active component as shown in Figure A.4, the network is partially functioning in case of a failure of the active component; i.e. the network is not separated but End Devices attached to the failed component cannot continue to communicate.

NOTE Active network components with bypass function are effective to avoid network separation and could be applied to other topologies.

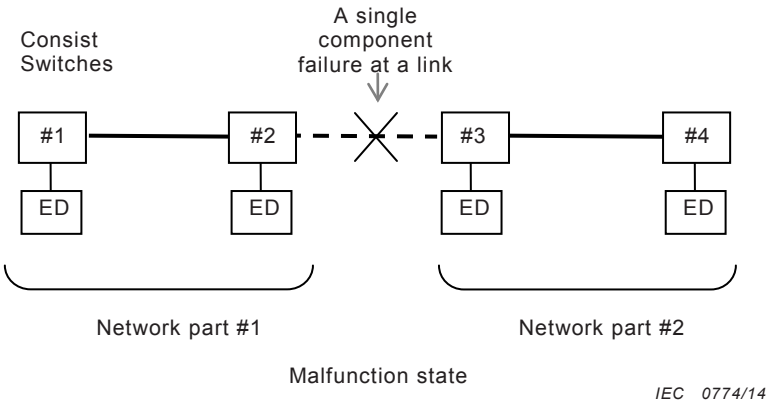


Figure A.3 – Example of a single component failure at a link on linear topology

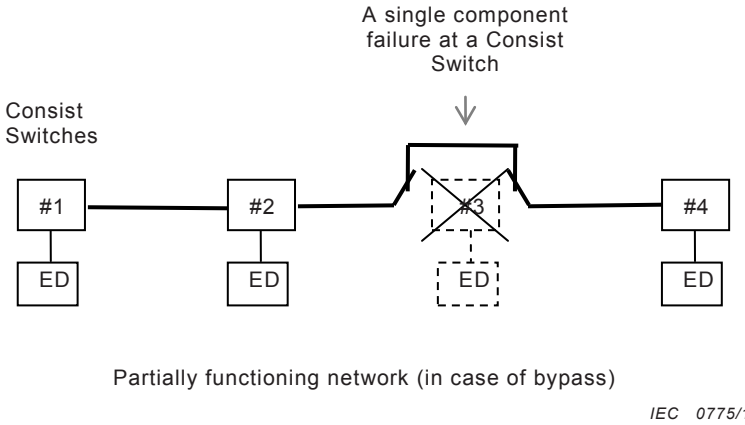


Figure A.4 – Example of a single component failure at an active component on linear topology

A.2.3 Example of failure cases – Parallel networks

A single component failure at a link between active components does not cause network malfunction, which is shown in Figure A.5.

In case of a single active component failure dual homing End Devices which have redundant links to multiple active components (Consist Switches) can continue to communicate; Figure A.6 shows the case with redundant links.

NOTE Parallel networks with bypass are tolerant of most of double component failures.

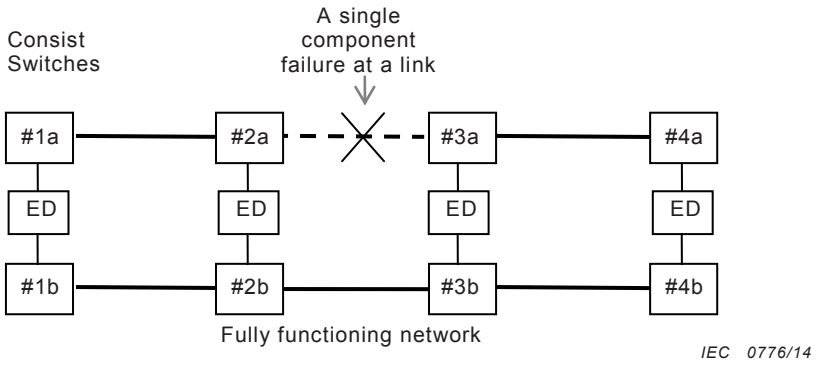


Figure A.5 – Example of a single component failure at a link on parallel networks

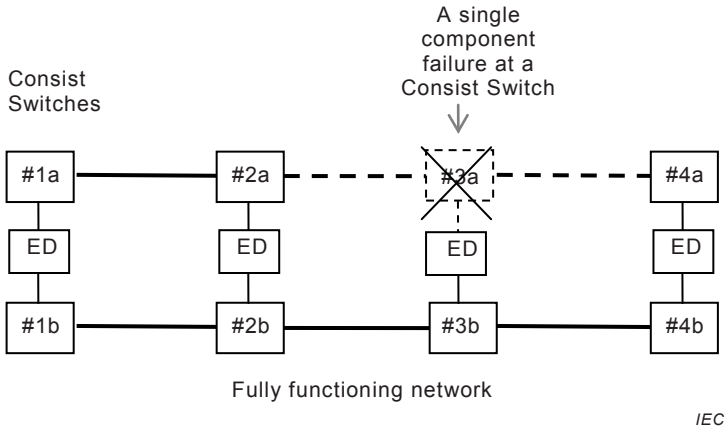


Figure A.6 – Example of a single component failure at an active component on parallel networks

A.2.4 Example of failure cases – Ring topology

A single component failure at a link between active components does not cause network malfunction, which is shown in Figure A.7.

A single component failure at an active component may cause network function reduced, which is shown in Figure A.8. However, dual homing End Devices which have redundant links to multiple active components (Consist Switches) can continue to communicate. Figure A.9 shows the case with redundant links.

NOTE Ring topology with bypass is tolerant of most of double component failures.

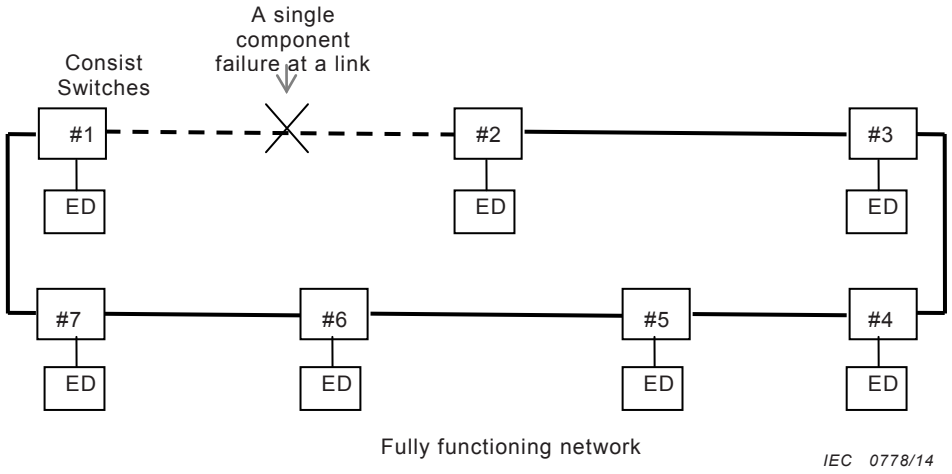


Figure A.7 – Example of a single component failure at a link on ring topology

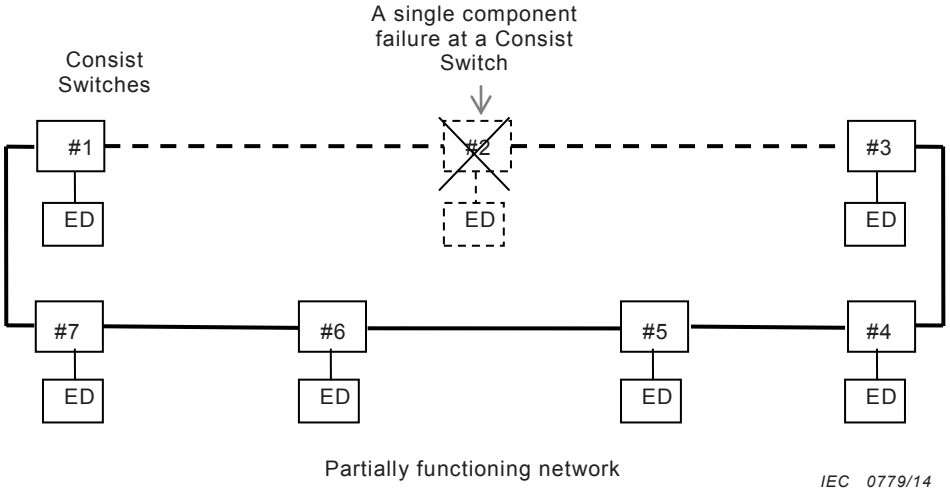


Figure A.8 – Example of a single component failure at an active component on ring topology

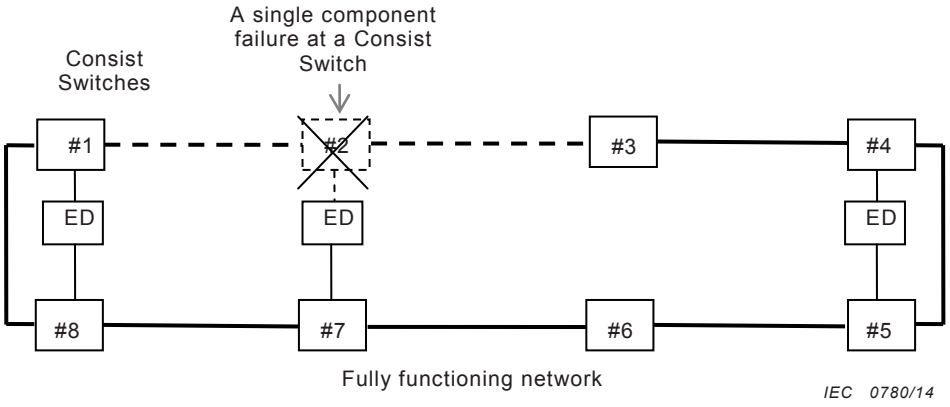


Figure A.9 – Example of a single component failure at an active component on ring topology (with dual homing ED)

A.2.5 Example of failure cases – Ladder topology

A single component failure at a link does not cause network malfunction, which is shown in Figure A.10.

In case of a single active component failure dual homing End Devices which have redundant links to multiple active components (Consist Switches) can continue to communicate; Figure A.11 shows the case with redundant links.

When double component failures occur at links of different locations, it may maintain full function unless the failures occur at the identical component for redundancy simultaneously, which is shown in Figure A.12.

When double component failures occur at active components, it may or may not maintain network function depending on the positions of failures. Network is malfunctioning in the failure case shown in Figure A.13, but it can be partially functioning if bypass is applied as shown in Figure A.13.

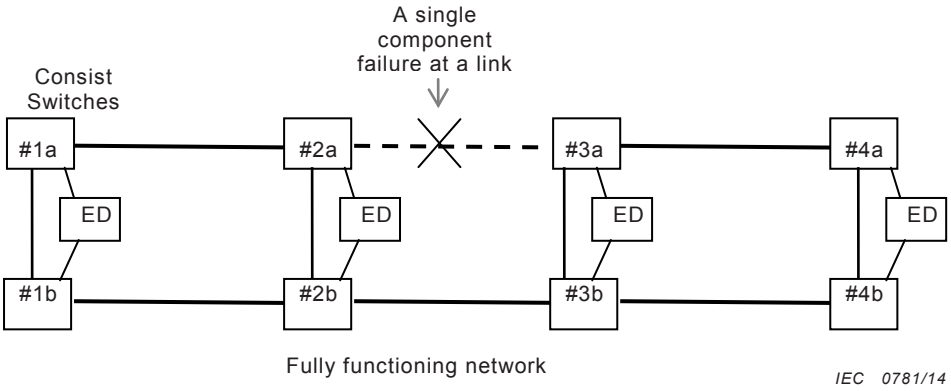


Figure A.10 – Example of a single component failure at a link on a ladder topology

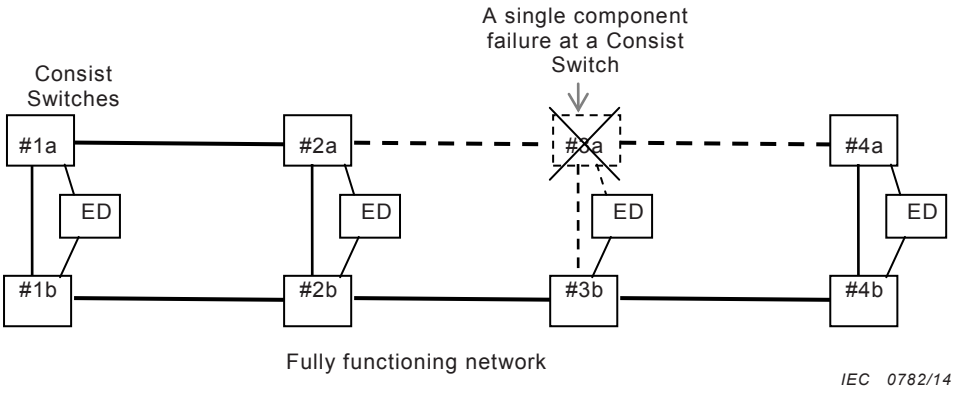


Figure A.11 – Example of a single component failure at an active component on ladder topology

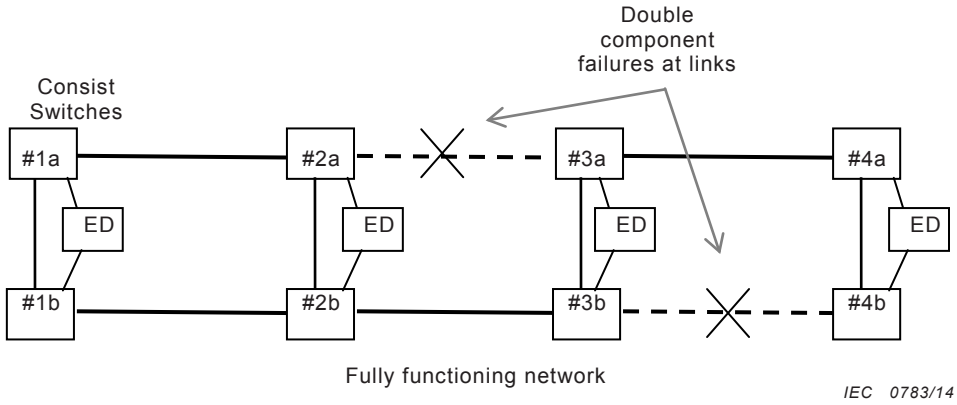


Figure A.12 – Example of double component failures at links on ladder topology

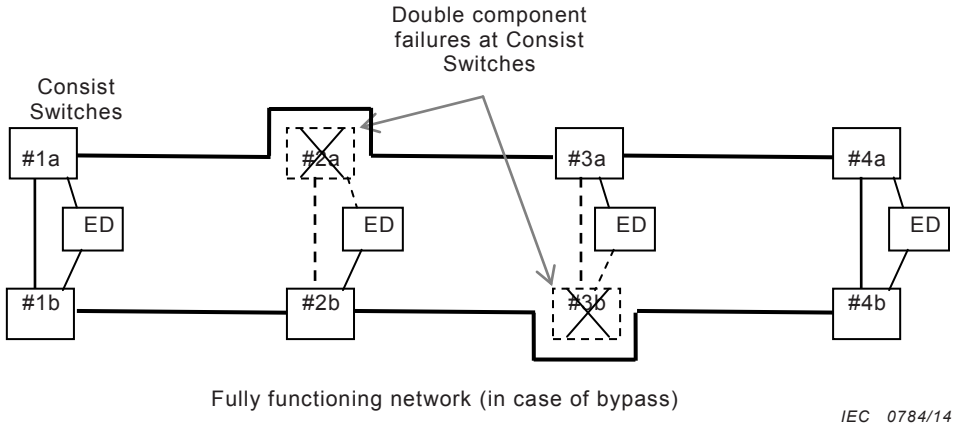


Figure A.13 – Example of double component failures at active components on ladder topology (with bypass)

A.3 Redundancy level of ECN architecture

There are three levels of redundancy as described in Table A.1. Figure A.14 shows examples of ECN architectures which support specified levels of redundancy.

Table A.1 – Redundancy level of ECN architecture

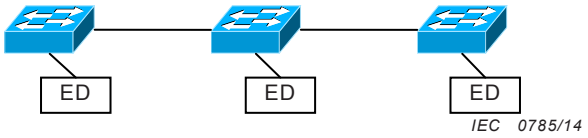
Redundancy level	Description	
	Failure component	**Influence of the failure**
Level 1	No redundancy	
Level 2	No single point of failure exists in the network, but some function is not operative in case of a failure.	
	CS failure	Network is recoverable, but EDs connected to the failed CS cannot communicate with other EDs.
	CS-CS link failure	Network is recoverable.
	CS-ED link failure	ED with the failed link cannot communicate with other EDs.
Level 3	No single point of failure exists, and all functions are operative. Double component failures are tolerable as much as possible.	
	CS failure	Network is recoverable, and EDs connected to the failed CS can still continue communicating.
	CS-CS link failure	Network is recoverable.
	CS-ED link failure	ED with the failed link can continue communicating.

NOTE 1 ED failure and redundancy of ED itself are outside the scope of this part of the standard.

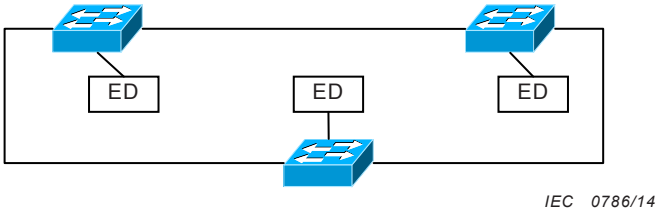
NOTE 2 A link failure includes failure of cable(s), connectors, and Ethernet interfaces (ports) at both ends.

NOTE 3 A CS failure is a failure of switch core, excluding port failure. The failure rate depends on complexity of hardware and software of CS.

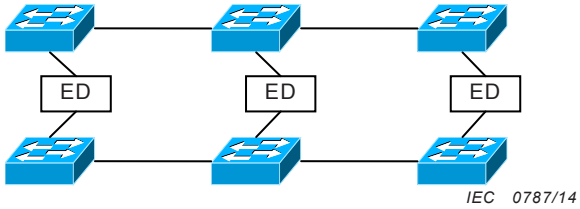
Level 1) Linear topology



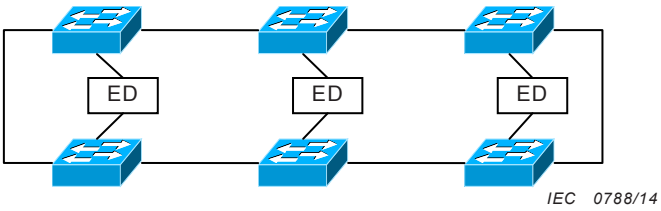
Level 2) Ring topology



Level 3a) Parallel network with dual homing



Level 3b) Ring topology with dual homing



Level 3c) Ladder topology with dual homing

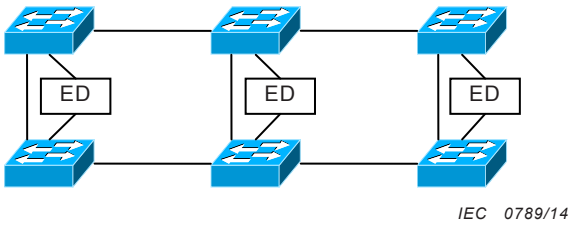


Figure A.14 – Example of ECN architecture classified by redundancy level

A.4 Reliability analysis of redundancy level

This clause analyzes reliability of ECN with specified redundancy level.

Three kinds of reliabilities are analyzed.See Table A.2.

a) Total failure rate
b) MTBF of network itself (network is separated in case of failure(s)); CS-ED link failure is not considered in the analysis
c) MTBF of communication between EDs (communication is not possible between EDs in case of failure); CS-ED link failure is considered in the analysis

Assumptions for simplification are as follows:

- Values of λ_S in different redundancy levels could not be equivalent, but same label λ_S is used.
- For calculation for MTBF of communication between EDs, only one ED per CS/CS-pair is considered.

Table A.2 – Reliability of redundancy level

Redundancy level	Total failure rate	MTBF of network	MTBF of communication between EDs
Level 1	$\sim N(\lambda_S + \lambda_T + \lambda_B)$	$\sim 1 / N(\lambda_S + \lambda_T)$	$\sim 1 / N(\lambda_S + \lambda_T + \lambda_B)$
Level 2	$\sim N(\lambda_S + \lambda_T + \lambda_B)$	$\sim \mu / (N^2(\lambda_S + \lambda_T)^2)$	$\sim 1 / N(\lambda_S + \lambda_B)$
Level 3a, 3b	$\sim 2N(\lambda_S + \lambda_T + \lambda_B)$	$\sim \mu / (2N^2 (\lambda_S + \lambda_T)^2)$	$\sim \mu / (2N^2 (\lambda_S + \lambda_T + \lambda_B)^2)$
Level 3c	$\sim 2N(\lambda_S + 3\lambda_T/2 + \lambda_B)$	$\sim \mu / 2N(3\lambda_S^2 + 4\lambda_S\lambda_T + \lambda_T^2)$	$\sim \mu / 2N(3\lambda_S^2 + 4\lambda_S\lambda_T + 2\lambda_S\lambda_B + \lambda_T^2 + \lambda_B^2)$

where:

N is the number of CSs or CS pairs for redundancy;

λ_S is the failure rate of a CS (core);

λ_T is the failure rate of a CS-CS link;

λ_B is the failure rate of a CS-ED link;

μ is the recovery rate.

NOTE 1 Fault models and formulas in IEC 62439 are used for calculation.

NOTE 2 For simplifying formulas in the text ‘N-1’ is represented as ‘N’ nevertheless this is not mathematically adequate. Therefore, level 3a and level 3b is not exactly the same, but they are nearly same.

Level 3 provides higher reliability compared to levels 1 and 2, but the reliability is reduced when common cause failures(CCF) of redundant components are considered. There are several methods to model common cause failures. Table A.3 shows reliabilities of level 3 when beta factor method is used. The value of the beta factor is typically 0,5 % to 10 % according to IEC 61508.

Table A.3 – Reliability when common cause failures are considered

Redundancy level	MTBF of network	MTBF of communication between EDs
Level 3a, 3b	$\sim \mu / \{\mu N\beta(\lambda_S+\lambda_T)+2N^2 (\lambda_S+\lambda_T)^2\}$	$\sim \mu / \{\mu N\beta(\lambda_S+\lambda_T+ \lambda_B)+ 2N^2 (\lambda_S+\lambda_T+\lambda_B)^2\}$
Level 3c	$\sim \mu / \{\mu N\beta(\lambda_S+\lambda_T)+2N(3\lambda_S^2+4\lambda_S\lambda_T+\lambda_T^2)\}$	$\sim \mu /\{\mu N\beta(\lambda_S+\lambda_T+ \lambda_B)+2N(3\lambda_S^2+4\lambda_S\lambda_T+2\lambda_S\lambda_B+\lambda_T^2+\lambda_B^2)\}$

NOTE 3 Only common cause failures in redundant CSs, CS-ED links and CS-CS link are considered. The values of beta factor(β) depend on components, but the same factor is used for the sake of simplicity.

Table A.5 shows examples of reliability and availabilities of ECN architectures, in case that the parameters described in Table A.4 are used for calculation. The values in Table A.5 show that the level 3 of architecture brings higher reliability and availability than levels 1 and 2. However, level 3c gives a slightly better reliability and availability than levels 3a and 3b due to multiple substitute paths in the redundant network, considering the common cause failures (CCF) the levels 3a, 3b, and 3c give nearly the same level of reliability and availability due to all based dual homing architecture.

Table A.4 – Parameters for reliability and availability calculation

(h: hour)

Parameter	Value	Comments
N: number of CSs or CS pairs	10	
λ_S: failure rate of a CS(core)	$5{,}00 \times 10^{-6}$ (h^{-1})	MTTF: 200 000 h
λ_T: failure rate of a CS-CS link	$3{,}33 \times 10^{-7}$ (h^{-1})	MTTF: 3 000 000 h
λ_B: failure rate of a CS-ED link	$3{,}33 \times 10^{-7}$ (h^{-1})	MTTF: 3 000 000 h
μ: recovery rate	$5{,}00 \times 10^{-2}$ (h^{-1})	Mean down time: 20 h
β: beta factor	0,01	1 % of the failure is common for redundant components.

Table A.5 – Reliability and availability example values

(h: hour)

Redundancy level	Total failure rate h^{-1}	MTBF of network h	MTBF of communication between EDs h	Availability of communication between EDs (Unavailability)
Level 1	$5{,}67 \times 10^{-5}$	$1{,}88 \times 10^{4}$	$1{,}76 \times 10^{4}$	0,9989 ($1{,}13 \times 10^{-3}$)
Level 2	$5{,}67 \times 10^{-5}$	$1{,}76 \times 10^{7}$	$1{,}88 \times 10^{4}$	0,9989 ($1{,}07 \times 10^{-3}$)
Level 3a, 3b without CCF	$1{,}13 \times 10^{-4}$	$8{,}79 \times 10^{6}$	$7{,}79 \times 10^{6}$	0,999997 ($2{,}57 \times 10^{-6}$)
Level 3c without CCF	$1{,}17 \times 10^{-4}$	$3{,}06 \times 10^{7}$	$2{,}93 \times 10^{7}$	0,9999993 ($6{,}82 \times 10^{-7}$)
Level 3a, 3b with CCF	$1{,}13 \times 10^{-4}$	$1{,}55 \times 10^{6}$	$1{,}44 \times 10^{6}$	0,999986 ($1{,}39 \times 10^{-5}$)
Level 3c with CCF	$1{,}17 \times 10^{-4}$	$1{,}77 \times 10^{6}$	$1{,}66 \times 10^{6}$	0,999988 ($1{,}20 \times 10^{-5}$)

A.5 Redundancy of End Devices

It has been demonstrated that ECN is a reliable network by itself, without considering EDs reliability. But EDs are not so reliable: an ED has the same order of importance of MTBF compared to a CS; as an example, 200 000 h for each. Therefore, it means that taken into account EDs the global reliability/availability of the network is reduced. This clause shows the impact of EDs, and redundant EDs, on the global reliability.

Table A.6 shows the impact of ED redundancy on MTBF on all architecture levels. Table A.7 shows the impact of ED redundancy on MTBF using ratios where ratio 1 corresponds to MTBF of 9 404 h. Values in both tables are calculated with parameters shown in Table A.4.

In case where an ED is redundant, the values given below in Table A.6 and Table A.7 show that reliability is increased considerably compared to the effect of redundancy on the architecture. For example, in a dual homing architecture (level 3 in Table A.6) with redundant EDs, the MTBFs are more than 40 times the MTBF reached with no ED redundancy. It is more than the MTBFs increase obtained from level 1 to level 3 without ED redundancy.

Table A.6 – Reliability with ED redundancy comparison

(h: hour)

Redundancy level	MTBF without ED redundancy h	MTBF with ED redundancy h
Level 1	9 404	19 785
Level 2	9 677	19 785
Level 3a, 3b	19 696	857 345
Level 3c	19 774	931 641

Table A.7 – Comparison of MTBFs ratios with ED redundancy

(ratio=1 corresponds to 9404 h, see Table A.6)

Redundancy level	MTBF ratio without ED redundancy	MTBF ratio with ED redundancy
Level 1	1	2,1
Level 2	1	2
Level 3a, 3b	2,1	43,5
Level 3c	2,1	47,1

Annex B
(informative)

Railway-Network Address Translation (R-NAT)

B.1 General

R-NAT is an algorithm for network address translation between ETB and ECN. This algorithm uses the rules for train and Consist network addresses, which simplify the management of address translation.

B.2 Local Consist subnet IP address

When R-NAT solution is deployed, a local ECN subnet IP address shall be associated with each ED. This local ECN subnet address is taken in subnet range 10.0/9, for example 10.0/18. Example of IP mapping is shown in Figure B.1. In the following, the term “local” is used in place of “local ECN subnet”.

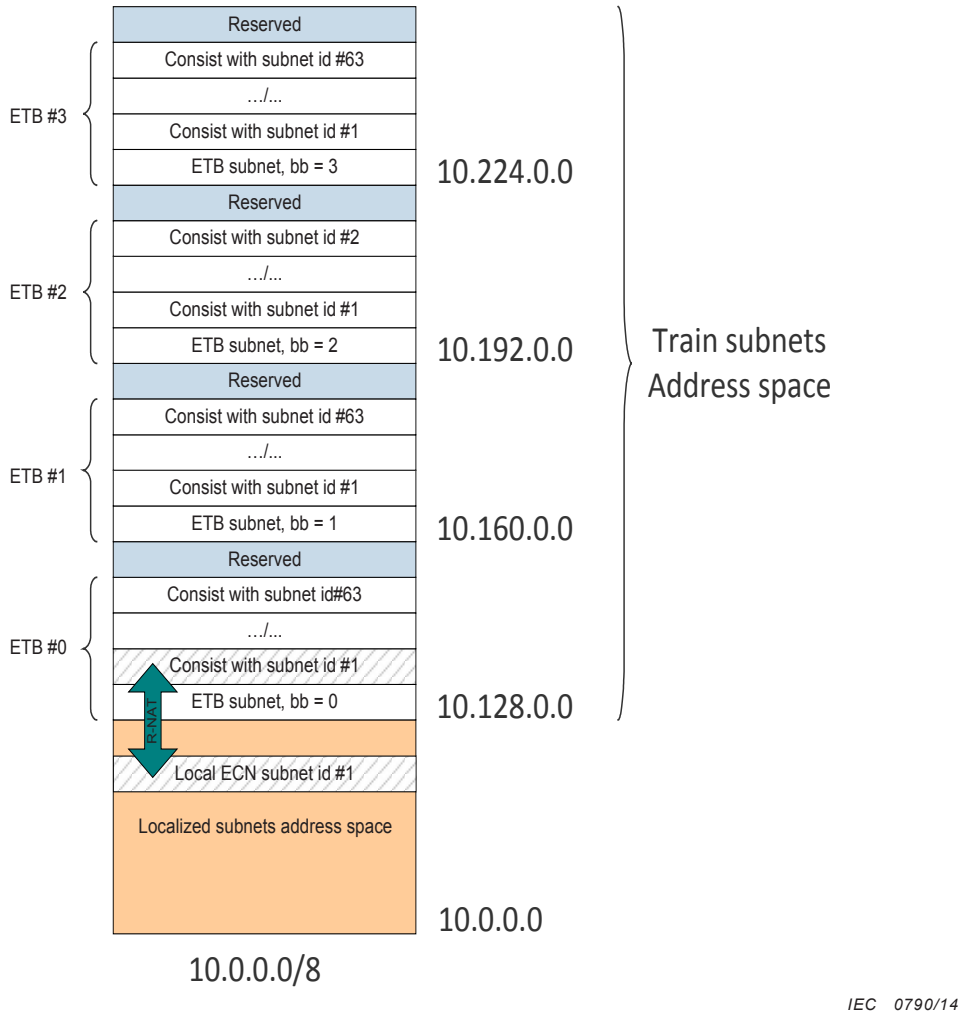


Figure B.1 – Example of ECN local IP range, “shadow” of train IP range for R-NAT

B.3 TBN R-NAT

Train wide communication between End Devices, which possess only a static IP source address, requires network address translation of IP addresses in the ECN/ETB IP routers. This network address translation shall in general comply to the rules defined in RFC 3022, but because of its special usage for the purpose of ECN/ETB routing it is referred to as “railway network address translation” (R-NAT).

When an IP packet is routed between ECN and ETB, the following address translation rules shall apply:

a) While routing from ECN to ETB, the static IP Source Address shall be translated from ECN address level to ETB address level, which especially means:
   – the address space of the ETB level is applied to the IP source address
   – the Consist Network Identifier of the source Consist Network shall be inserted in the IP source address

b) While routing from ETB to ECN, the dynamic IP Destination Address shall be translated from ETB address level to ECN address level, which especially means:
   – the address space of the ECN level is applied to the IP destination address
   – the Consist Network Identifier in the IP destination address shall be removed (replaced by “0”)

Example – The example shall illustrate the railway network translation, see Figure B.2. Three TBNs are shown which received the TBN addresses 05, 06 and 07 after train inauguration. An End Device with number 53, connected to TBN 05, sends an IP packet to the End Device 21 connected to TBN 07. The TBN 05 translates the IP source address from 10.0.0.53 (ECN address level) to the IP source address 10.129.64.53 (ETB address level). The TBN 07 afterwards translates the IP destination address 10.129.192.21 (ETB level) to the IP destination address 10.0.0.21 (ECN level).

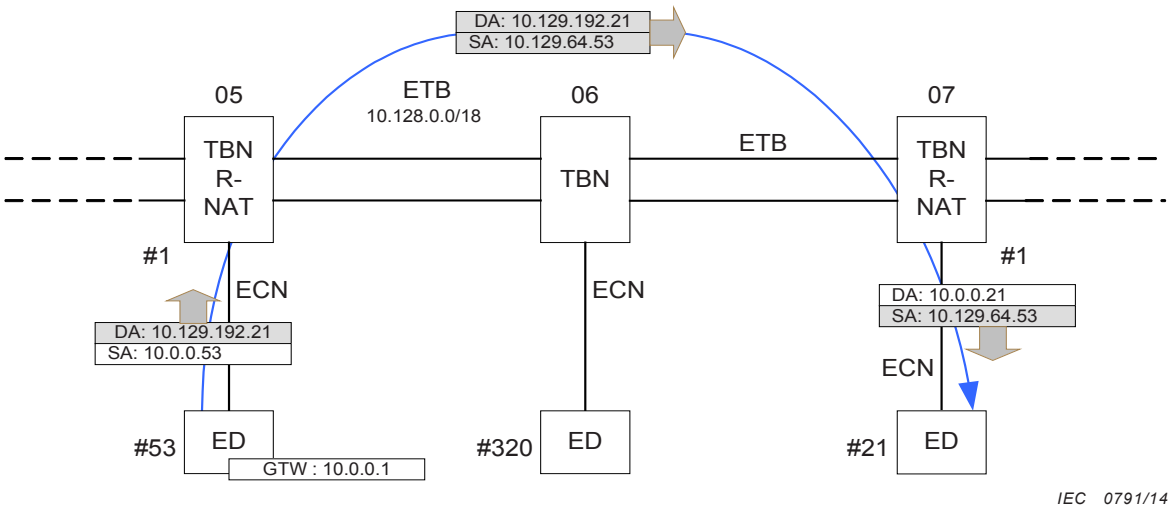


Figure B.2 – Example of Railway Network Translation (R-NAT)

NOTE R-NAT can be executed in IP routers while pre- and post-routing IP packets.

B.4 Interoperability issue between TBNs

As TBN with R-NAT and TBN without (R-)NAT both respect general IP mapping definitions, they are interoperable. Examples below illustrate this, see Figures B.3 and B.4:

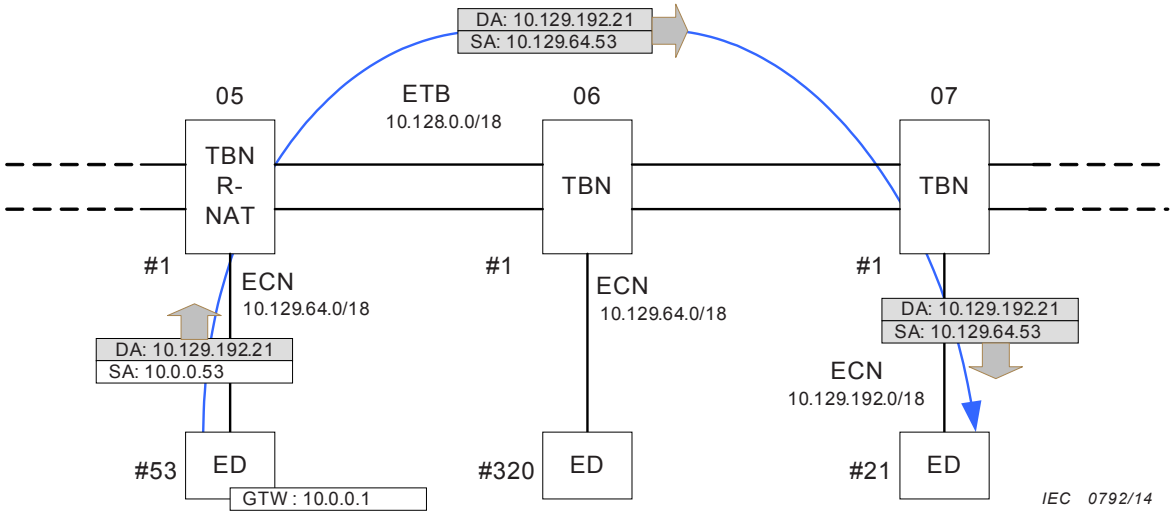


Figure B.3 – From R-NAT TBN to TBN

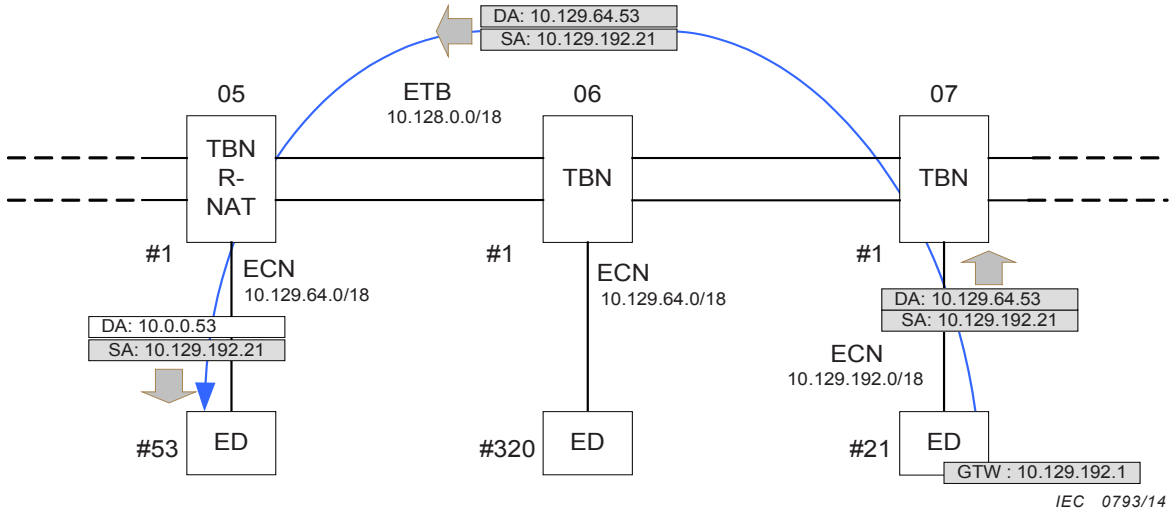


Figure B.4 – From TBN to R-NAT TBN

In both cases, on ETB, IP addresses are always inside train IP mapping. Local IP addresses, if defined, are never used as destination address to outgoing the ECN (to access ED in neighbor ECN).

Annex C
(normative)

Transceiver with amplified signals protocol definition

C.1 General

This annex defines optional transceiver with amplified signals, which may be attached outside of 10BASE-T MAU or 100BASE-TX PMD.

In order to raise noise immunity of the signal transmission on the media not only within a vehicle but also connecting vehicles with couplers, the transmission signals may be amplified than the normal voltage.

NOTE The specifications for the transceiver with amplified signals are the exceptions which are not compliant to IEEE 802.3.

There are two options according to the transmission bit rate, which can be selected depending on application.

a) Type A

   Transceiver with amplified signals for Physical Layer based on IEEE 802.3, clause 14 (10BASE-T).

b) Type B

   Transceiver with amplified signals for Physical Layer based on IEEE 802.3, clause 25 (100BASE-TX).

C.2 Type A: Transceiver with amplified signals for Physical Layer based on IEEE 802.3 (10BASE-T)

C.2.1 General

This clause defines the transceiver with amplified signals for Physical Layer based on IEEE 802.3, clause 14 (10BASE-T).

The items not defined in this clause shall be compliant with the IEEE 802.3, clause 14 (10BASE-T).

C.2.2 Transceiver unit

The block diagram of the transceiver unit is shown in Figure C.1. The differential transmission data signals TD+ and TD- from the IEEE 802.3 10BASE-T MAU are levelled up in the amplifier. Level conditioner is a circuit which lowers the received signals RDA+ and RDA- into the range of the receivable signal level, even if it is transmitted from a nearby transceiver unit.

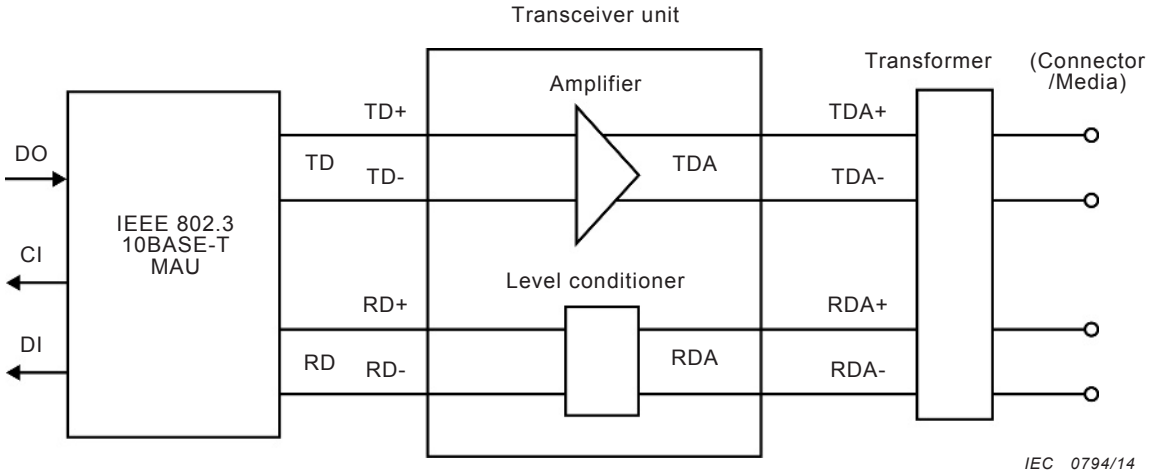


Figure C.1 – Block diagram of transceiver unit for 10BASE-T MAU

C.2.3 Transmission signal characteristics

Transmission signal characteristics shall conform to the description below.

a) For the transmission differential waveform, output voltage signal Vo defined by the circuit shown in Figure C.2, in which the twisted-pair model is shown in Figure C.3 with a 100 Ω resistive load, shall satisfy the template shown in Figure C.4 and Table C.1 with tolerance of ±10 %. The specifications of the twisted pair cable equivalent circuit shall be in accordance with 14.3.1.2 in IEEE 802.3 (10BASE-T).

b) The TP_IDL signal shall satisfy the conditions shown in Figure C.5 under the load shown in Figure C.6, where BT is a time slot period which is 100 ns for 10BASE-T.

c) When link pulses are used, the conditions shown in Figure C.7 shall be satisfied. When the connection status can be confirmed without using link pulses, this item may be ignored, where BT is the same as described above.

NOTE Templates of figures, Figure C.2 to Figure C.9, are quoted from the IEEE 802.3, clause 14 (10BASE-T).

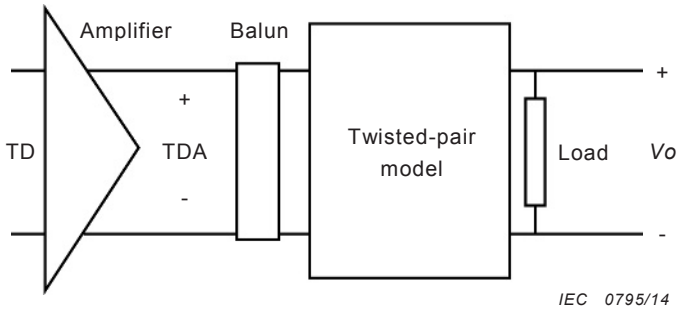


Figure C.2 – Differential output voltage test

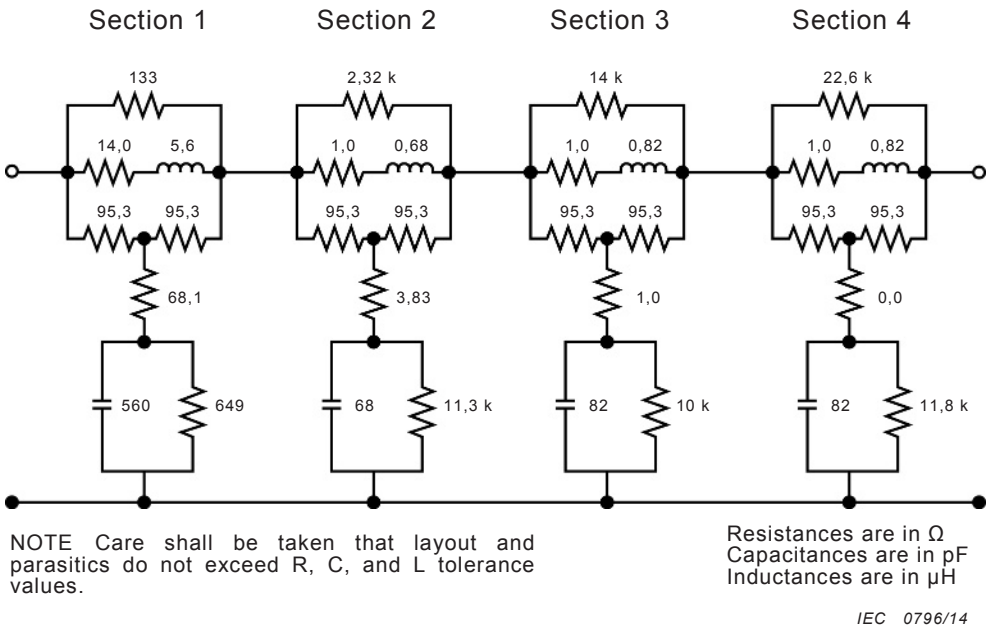
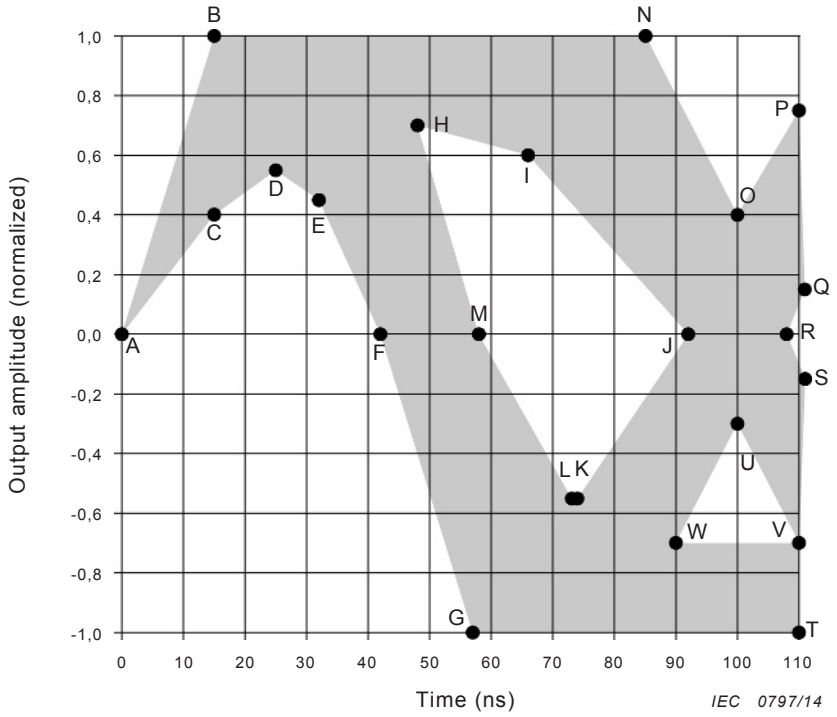


Figure C.3 – Twisted-pair model



NOTE Output amplitude 1,0 is equivalent to 3,636 V.

Figure C.4 – Amplified voltage template

Table C.1 – Output voltage template table

Reference	Time ns	Output amplitude (See NOTE)
A	0	0
B	15	1,0
C	15	0,4
D	25	0,55
E	32	0,45
F	42	0
G	57	-1,0
H	48	0,7
I	67	0,6
J	92	0
K	74	-0,55
L	73	-0,55
M	58	0
N	85	1,0
O	100	0,4
P	110	0,75
Q	111	0,15
R	108	0
S	111	-0,15
T	110	-1,0
U	100	-0,3
V	110	-0,7
W	90	-0,7
NOTE Output amplitude is normalized, in which value 1,0 is equivalent to 3,636 V.		

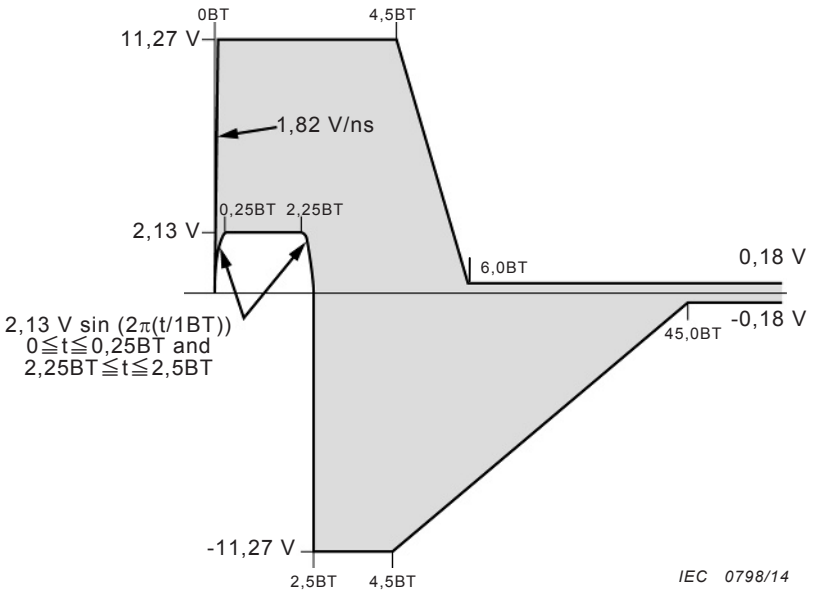
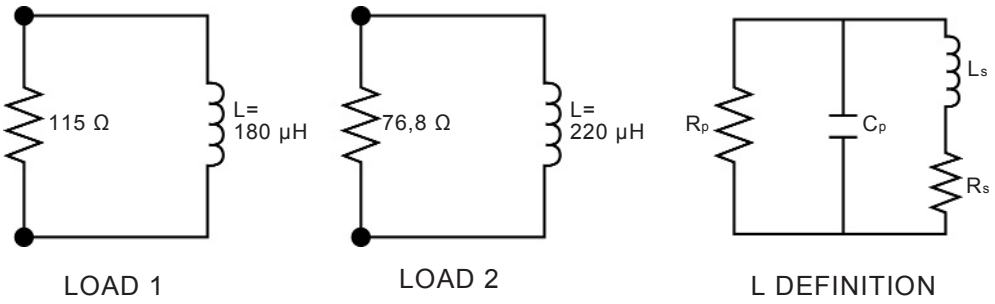


Figure C.5 – Amplified transmitter waveform for start of TP_IDL



NOTE All parameters are defined over the frequency range of 250 kHz to 6 MHz.

L_s =L±1 % $R_p \geqq$ 2 kΩ
C_p =12 pF±20 % $R_s \leqq$ 0,5 Ω

IEC 0799/14

Figure C.6 – Start-of-TP_IDL test load

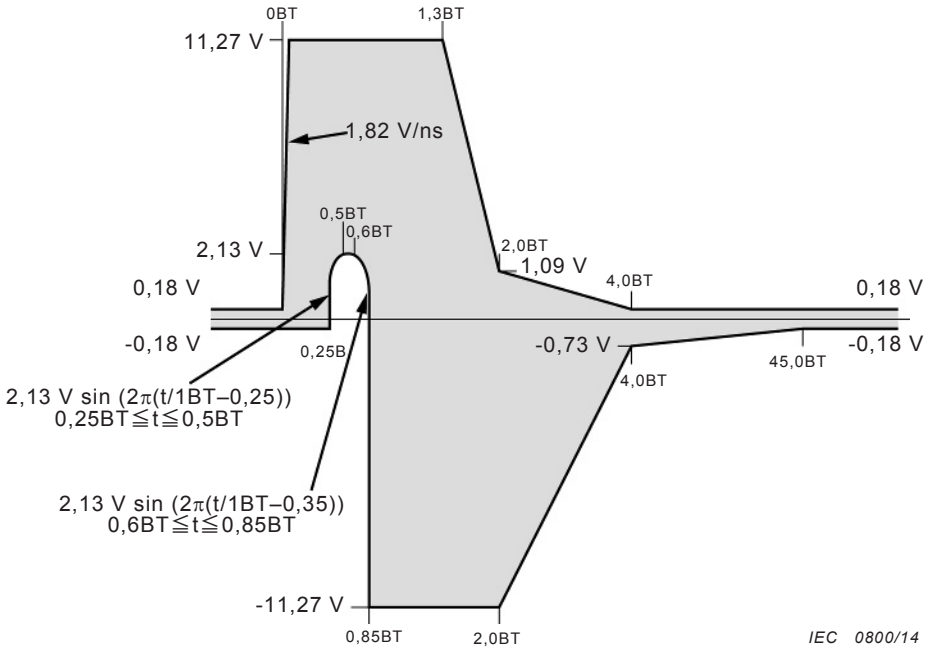


Figure C.7 – Amplified transmitter waveform for link test pulse

C.2.4 Reception signal characteristics

The reception waveform shall satisfy the conditions of the template shown in Figure C.8 and Figure C.9.

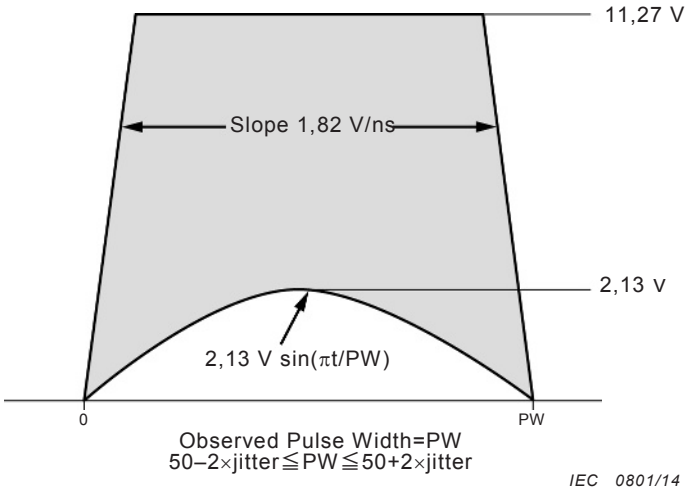


Figure C.8 – Amplified receiver differential input voltage – narrow pulse

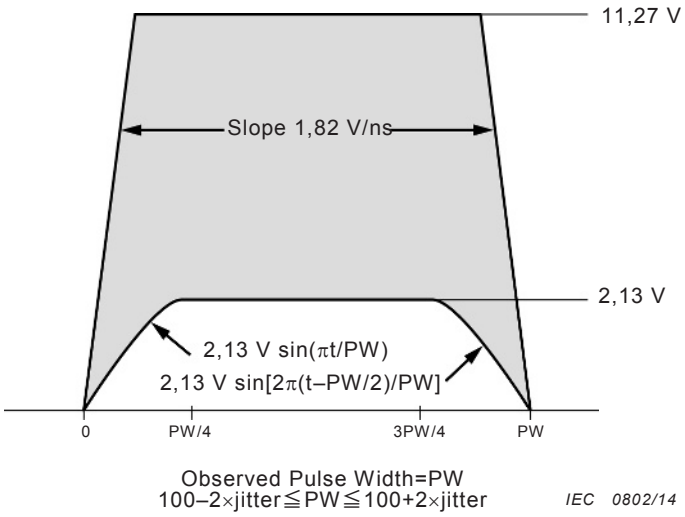


Figure C.9 – Amplified receiver differential input voltage – wide pulse

C.3 Type B: Transceiver with amplified signals for Physical Layer based on IEEE 802.3 (100BASE-TX)

C.3.1 General

This clause defines the transceiver with amplified signals for Physical Layer based on IEEE 802.3, clause 25 (100BASE-TX).

The items not defined in this clause shall be compliant with IEEE 802.3, clause 25 (100BASE-TX).

C.3.2 Transceiver unit

The block diagram of the transceiver unit is shown in Figure C.10. The differential transmission data signals Transmit+ and Transmit- from the IEEE 802.3 100BASE-TX PMD are levelled up in the amplifier circuit, which become signals TDA+ and TDA- and are led to the transformer. Level conditioner is a circuit which lowers the received signals RDA+ and

RDA- into the range of the receivable signal level of the PMD, even if it is transmitted from a nearby transceiver unit.

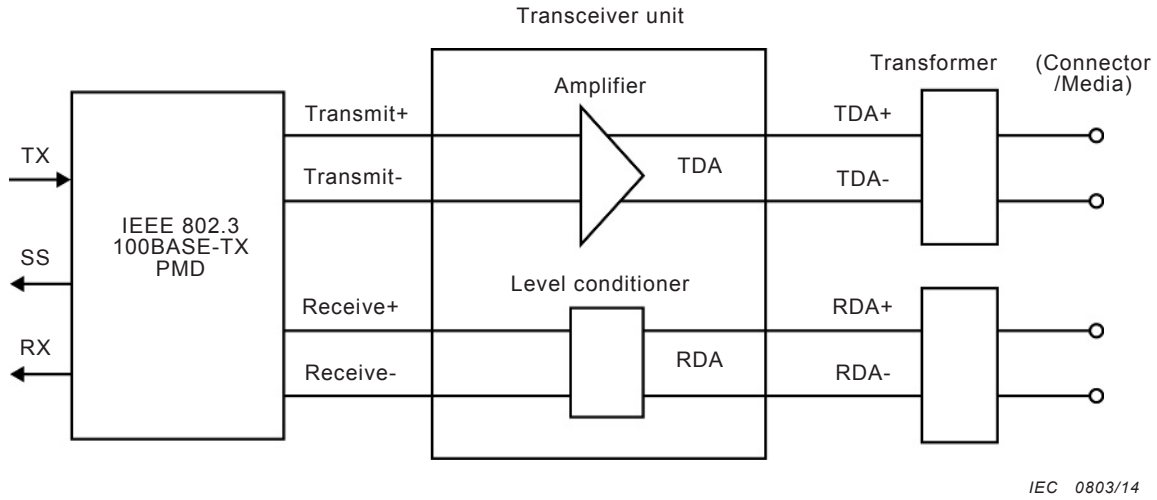


Figure C.10 – Block diagram of transceiver unit

C.3.3 Transmission signal characteristics

Transmission signal characteristics shall conform to Clause 9 of ANSI X3.263:1995 with the exceptions below.

a) Clause 9.1.1 Shielded twisted pair active output interface shall not be used.

NOTE In clause 9.1.1, active output interface for STP with characteristic impedance of 150 Ω is defined.

b) The test load shall accord with the description in clause 9.1.2 Unshielded twisted pair active output interface.

c) For the differential output voltage instead of the UTP differential output voltage, V_{out}, shall be:

$3\,800\ \text{mV} \leqq V_{out} \leqq 4\,200\ \text{mV}$

For twisted pair active output interface, the characteristic of Differential Signal, zero-peak shall be used and comply with the values in Table C.2, instead of the characteristics of both Differential Signal, UTP, zero-peak and Differential Signal, STP, zero-peak.

Table C.2 – Twisted pair active output interface

Characteristic	Minimum	Maximum	Units
Differential Signal, UTP, zero-peak	Not used	Not used	mVpk
Differential Signal, STP, zero-peak	Not used	Not used	mVpk
Differential Signal, zero-peak	3 800	4 200	mVpk

NOTE Other characteristics in Table 3 in clause 9 of ANSI X3.263-1995 remain the same.

C.3.4 Reception signal characteristics

Reception signal characteristics shall conform to clause 10.1 of ANSI X3.263-1995 with the exceptions below.

a) Signal_detect shall be asserted per clause 10.1.2 for any valid peak to peak signal, VSDA, greater than 4 000 mV. Signal_detect shall remain asserted in the presence of valid signals with a low density of transitions.

b) Signal_detect shall be deasserted when the peak to peak received signal, VSDD, is smaller than 800 mV.

Figure C.11 illustrates these requirements.

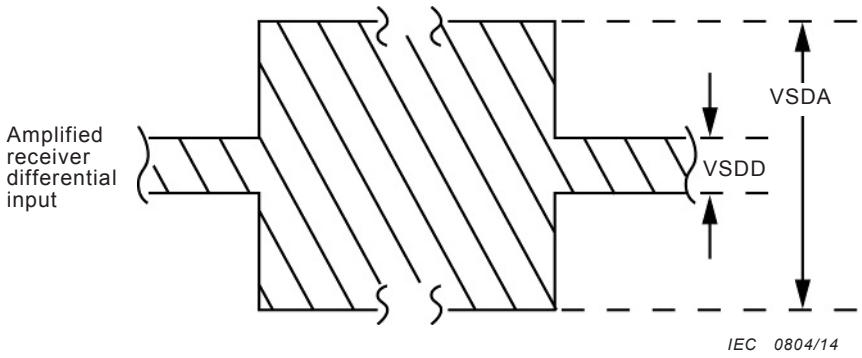


Figure C.11 – Signal_detect assertion threshold

NOTE Templates of Figure C.11 are from ANSI X3.263-1995, Clause 10.

Annex D
(informative)

Ladder topology protocol definition

D.1 General

This annex defines protocol for ladder topology which provides higher robustness and availability in communication for train application to minimize risk of hindrance to train running.

The purposes of the ladder topology defined in this annex are in the following.

- Continue communication on the ECN in case of a single component failure,
- Continue communication on the ECN in case of double component failures as much as possible except common cause failure,
- Transparency of network failure for the train application in End Devices, if the failure can be recovered in adequate time by avoiding the failure points.

In order to achieve the purposes, this ladder topology applies the following in the design philosophy;

- Double sub-networks of trunk links with Consist Switches, which constitutes a duplicated system,
- Local links between the duplicated Consist Switches,
- Transmission of data frames on both or either of the sub-networks depending on application data,
- Dedicated command frames which are additionally used in Link Layer protocol to manage failure and recovery,
- Redundancy management protocol which contains the information for the management of recovery.

The protocols for Consist Switch interface shall accord with the common part of this standard except the protocols needed to control redundancy in ladder topology.

NOTE This ladder topology protocol contains the exceptions which are not compliant to IEEE 802.1D or IEEE 802.3, which are stated as notes in the proper places of this annex.

The protocols for End Device interface of this Consist Switch shall accord with the common part of this standard.

In this annex, the term “Consist Switch” is replaced with “CNN” or “Consist Network Node”.

D.2 Architecture of Consist Network Node

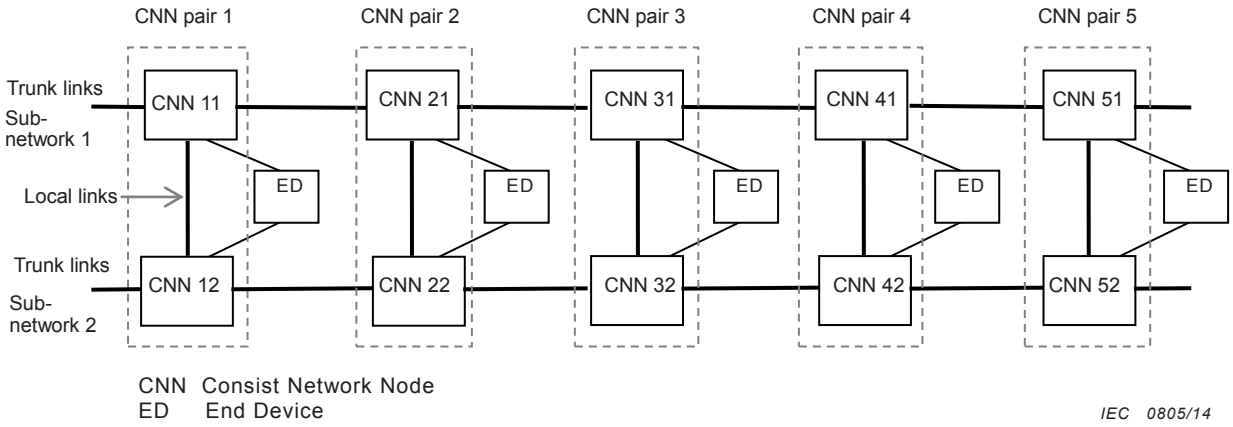
D.2.1 General

This clause defines protocols for the CNN (Consist Network Node) in ladder topology.

D.2.2 Concept of ladder topology

A concept of ladder topology is shown in Figure D.1, in which CNNs are interconnected in series with trunk links on each sub-network, indicated as sub-network 1 and sub-network 2, and also interconnected between CNNs on the other side of the network to make pairs with the local links respectively.

End Device has typically two links, which is called dual homing; refer to 4.5.4 .



NOTE 1 In this figure, the CNN numbers are not actual but abstract for explanation.

NOTE 2 Optional bypass relays are not illustrated for simplification.

Figure D.1 – Concept of ladder topology

D.2.3 Configuration of ladder topology

Configuration of ladder topology is shown in Figure D.2 for example of three CNNs in respective sub-networks in which only relevant parts for connection are expressed inside CNN for simplification.

In each sub-network in Figure D.2, the trunk link connects the TPD and the TPU of the CNNs, but TPU or TPD in outer side of the end CNNs are open.

For the local links, in case of PD (Process Data) and CNN management data, LPT (local port for the own sub-network) is exclusive for transmission of the data frame and LPR (local port for the other sub-network) is for reception. In other cases, each of them is used as a two way communication channel between the sub-networks. LPT of CNN in sub-network 1 is connected to LPR of CNN in sub-network 2, and vice versa for another local link.

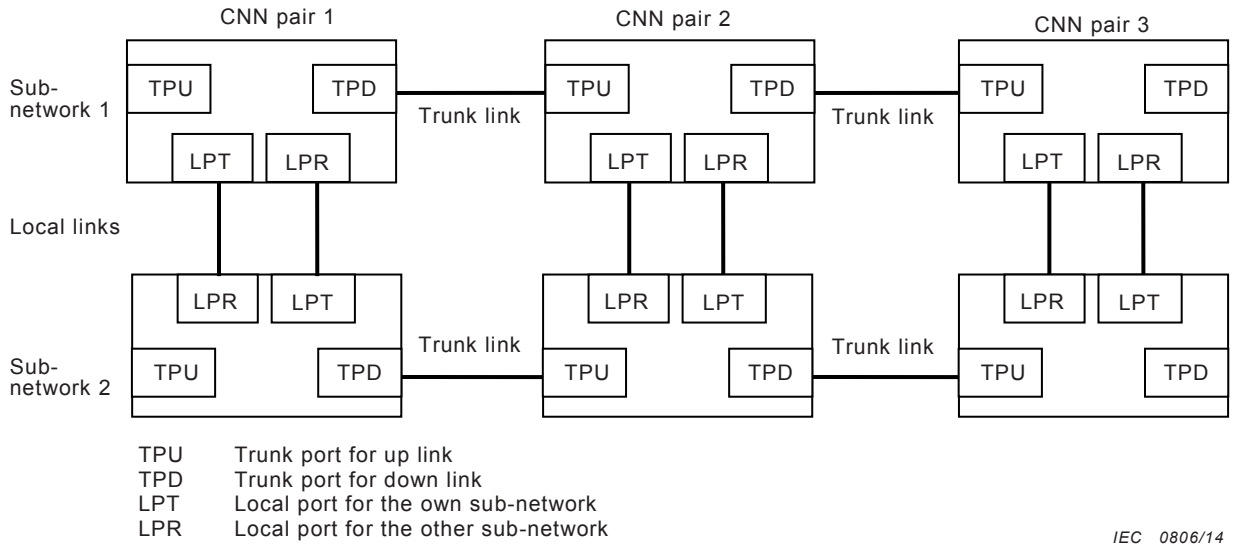


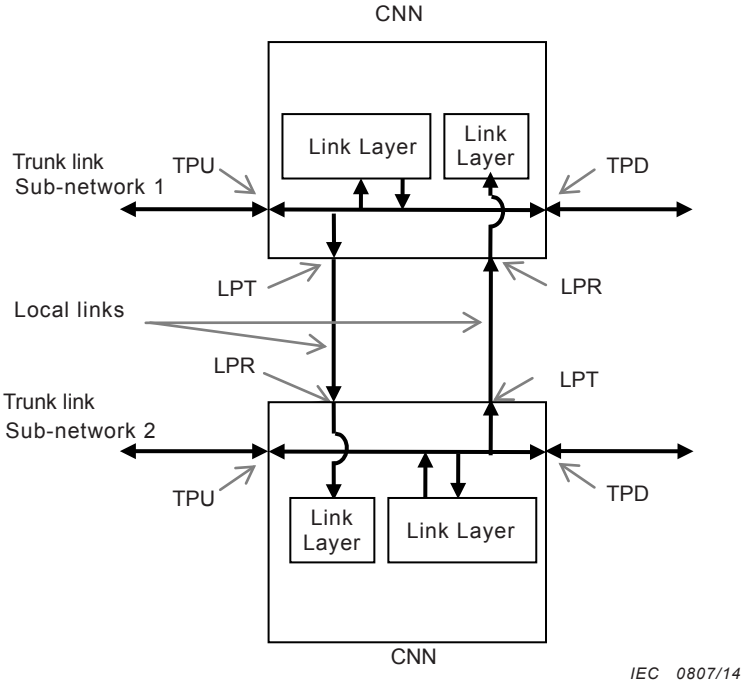
Figure D.2 – Configuration of ladder topology

Basic flows of data frames in duplicated CNNs, in case of PD and CNN management data, are shown in Figure D.3.

The received frame at one of the trunk ports (TPU or TPD) is passed to a Link Layer of the CNN, the other port of the trunk link (TPU or TPD) and the LPT simultaneously.

Conversely, data frame from Link Layer of the CNN is transmitted over trunk links and the LPT simultaneously.

Via the LPR, data frames transmitted from the LPT of the other sub-network is received by another Link Layer in the CNN.



NOTE Physical Layers are replaced with arrows which indicate the directions of data frames in the drawing.

Figure D.3 – Basic flows of data frames on trunk links and local links in ladder topology

D.2.4 Functional structure of Consist Network Node

Figure D.4 shows the functional structure of the CNN, which consists of switch section, real time MAC section and ladder topology management section.

Function of the switch shall conform to that of Consist Switch defined in this standard.

Real time MAC performs controlling the network to avoid traffic congestion for multiple accesses among CNNs by means of token passing, where token means the right to transmit its data frame to the network immediately.

NOTE 1 The protocol of the real time MAC is defined in D.3.2.5 in this annex. The function of the real time MAC is the exception which is not compliant to IEEE 802.1D.

Ladder topology management section includes CNN management, upper layer protocol stack, MAC sub-layer and Physical Layers. The CNN management performs redundancy control together with the real time MAC by using the dedicated command frames for detection and recovery of failure.

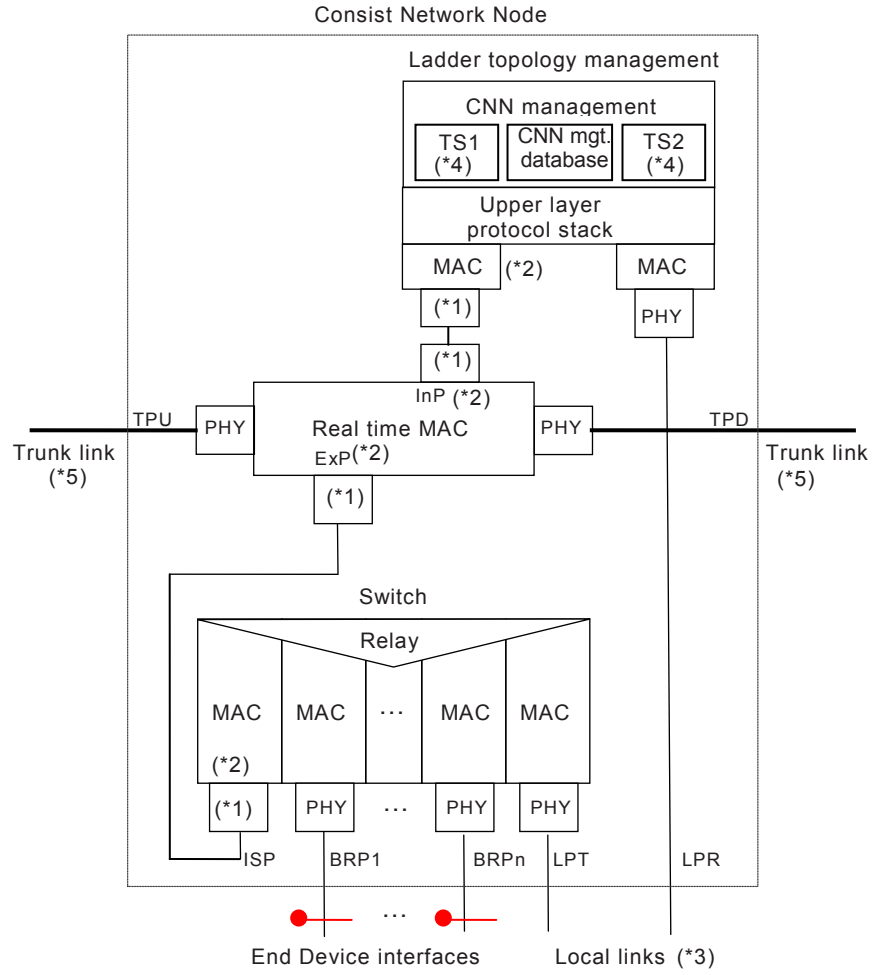
NOTE 2 The protocol of the CNN management is defined in Clause D.4 in this annex.

TPU and TPD in Figure D.4 determine the direction of token flowing. TPU shall be connected with TPD of the preceding CNN and TPD shall be connected with TPU of the succeeding CNN, so that token is always received at TPU and sent at TPD in the CNN.

When a CNN is an origin of data frame, it transmits the data frame to both the preceding CNN via TPU and the succeeding CNN via TPD over the trunk links simultaneously.

Conversely, when a CNN receives a data frame either at TPU or TPD, the real time MAC checks the header of the MAC frame, if it is one of the dedicated command frames, then it is handled inside the real time MAC, after that, another dedicated command frame is issued on the trunk link.

If the received frame is not the dedicated command frame, it is passed to the next CNN via the trunk port opposite to the receiving trunk port and simultaneously distributed to external End Devices via the switch, and also to CNN management via internal interface.



NOTE 1 For internal interfaces, either PHY or MII (Media Independent Interface) defined in IEEE 802.3 Clause 22 may be used.

NOTE 2 Flow control, which is defined as MAC Control PAUSE operation in IEEE 802.3, is supported in interfaces between MACs for the InP and the ExP.

NOTE 3 The local links are used for communication between the redundant CNNs in ladder topology.

NOTE 4 Traffic store is a buffer memory for Process Data, which is refreshed by the cyclic transmission and the size and the address space are common to all traffic stores in the network.

NOTE 5 Optional bypass relay of trunk link for powerless or failure condition of CNN is not illustrated in this figure.

Figure D.4 – Functional structure of Consist Network Node

D.2.5 Traffic Store for Process Data

The concept of Traffic Store in this ladder topology is similar to Traffic Store in WTB defined in IEC 61375-2-1, but the address and the size of a dataset of PD are flexible depending on application.

In Figure D.5, the concept of Traffic Store is illustrated as an example of Traffic Stores in the network with 3 CNNs. The dataset A in Traffic Store in CNN 1 is published on the network,

which is subscribed by the other CNNs, or CNN 2 and CNN 3. Similarly, the dataset B is published from the Traffic Store in CNN 2, and the Dataset C from the traffic store in CNN 3.

The offset address specifies the starting address of the dataset in the address space of the Traffic Store. One publisher and multiple subscribers for a dataset are configured as the same in both of the sub-networks. All contents of the datasets in traffic stores are refreshed to the same in a certain period of cyclic transmission.

The size of the address space of the Traffic Store shall be the same in the network, which should be 64 kilo-byte as default. Two sets of Traffic Store for the sub-network 1 and 2 shall be implemented in the CNNs and End Devices.

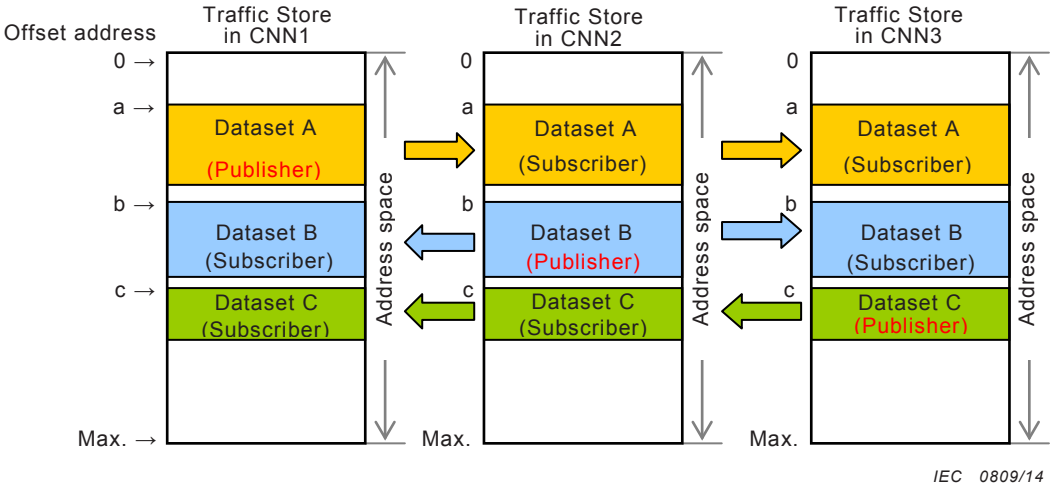


Figure D.5 – Concept of Traffic Store in ladder topology

D.2.6 Redundancy in ladder topology

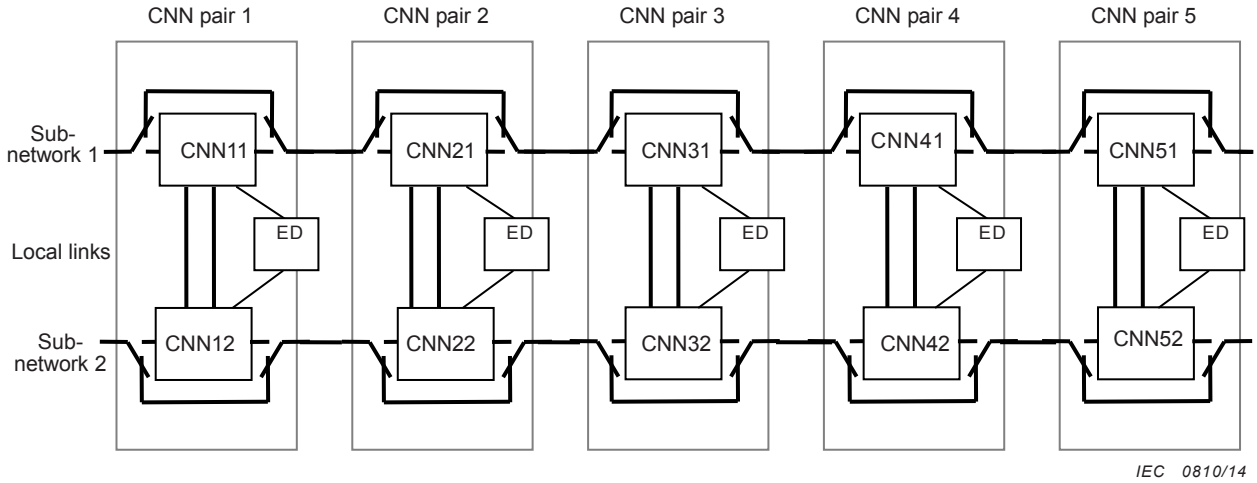
D.2.6.1 General

This subclause describes behaviour of redundancy in the ladder topology which employs the dedicated trunk links and the dedicated local links as redundant routes.

NOTE For the formal description of the state machine, refer to D.4.9.

D.2.6.2 Principles of redundancy in ladder topology

Figure D.6 shows an example of configuration of the ladder topology. A CNN is connected with its neibouring CNNs through the trunk links and with the partner CNN in the other side sub-network through the local links so that they compose a pair of CNNs, in which although bypass relays are optionally attached to the CNNs, the relays are illustrated in the example.



NOTE Bypass relay at both end CNNs are not necessary to be implemented, which are drawn for unification.

Figure D.6 – Example of configuration of ladder topology

The principles of the redundancy in the ladder topology are;

- All PD (Process Data) frames from End Devices are transmitted to both sub-networks, or trunk links of both sub-networks, simultaneously through both of paired CNNs, in which the data are identical, and the data frames can be received by End Devices at all other CNNs in both sub-networks.
- When a failure occurs at a link or a CNN on either of the sub-networks, which causes loss of the data frames, the other CNNs take charge of transmission of the data frame as substitutes for the failed CNN by means of detouring with the local links. This is called as the substitute transmission.
- The substitute transmission is only applied to PD. On the other hand, in case of failure, MD (Message Data) which is transmitted to one of the sub-networks sporadically shall be detoured by the routing protocol OSPF (Open Shortest Pass First) version 2 defined in RFC 2328 with the extensions of RFC 1793 and RFC 4136.

D.2.6.3 Substitute transmission

The substitute transmission is the backup system in which data transmission of CNNs in the sub-network separated by the failure are substituted by the other CNNs in the sub-network so that the data transmission continues as if they are in the same as before, even after the failure has occurred.

By means of this, End Devices connected with the pairs of CNNs in dual homing need not to care the failure, neither to switch the interface to the other side for receiving data, in case of not only a single component failure but also double component failures except common cause failures on the redundant sub-networks.

In the substitute transmission mechanism, in order to avoid the condition in which CNNs cannot receive the data of PD from the publisher CNN when it is failed, since the data with the same contents is transmitted normally from the partner CNN of the publisher CNN in failure, the data can be re-transmitted by the other CNNs as the substitution with using the data from the partner.

In the local links, the received data at the LPR are stored to update the content in the Traffic Store for the LPR, and then when the substitute transmission is executed, the data are taken out to transmit to the sub-network.

The substitute transmission shall be started in the events below:

a) When a CNN detects failure of a trunk link between the neighbouring CNN by means of periodical checking of the status of the trunk links,

b) When a CNN detects one or more of CNN(s) bypassed in the upward,

c) When a CNN receives the request contained in the CNN management information from the other CNN.

In such cases, the CNN transmits the data received from the CNN(s) in the other side sub-network by reading the data from the traffic store dedicated for the LPR, in addition to its own data.

NOTE For formal description of the substitute transmission in ladder topology, refer to Table D.45 and Table D.46 in D.4.8. For failure cases in the ladder topology with the substitute transmission, refer to Clause D.5.

D.2.7 Configuration parameters for ladder topology

D.2.7.1 General

This subclause describes configuration parameters for the ladder topology.

D.2.7.2 Configuration parameters for CNN

In the ladder topology, different individual IP addresses shall be assigned to respective End Devices with different subnet-IDs, which are attached to CNNs in the separate sub-networks of sub-network 1 and sub-network 2.

NOTE For IP address assignment, refer to D.3.3.

Table D.1 shows configuration parameter for CNN in the sub-network 1, and Table D.2 shows that for CNN in the sub-network 2 in the ladder topology.

Table D.1 – Configuration parameters for CNN in sub-network 1

Parameter	Type	Description
IndividualIpAddressIedS1	UNSIGNED32	Individual IP address for the CNN management in CNN in the sub-network 1
IndividualIpAddressLprS1	UNSIGNED32	Individual IP address for the local port for the other sub-network in CNN in the sub-network 1

Table D.2 – Configuration parameters for CNN in sub-network 2

Parameter	Type	Description
IndividualIpAddressIedS2	UNSIGNED32	Individual IP address for the CNN management in CNN in the sub-network 2
IndividualIpAddressLprS2	UNSIGNED32	Individual IP address for local port for the other sub-network in CNN in the sub-network 2

D.2.7.3 Configuration parameters for substitute transmission

Table D.3 shows configuration parameters for substitute transmission of PD. When substitute transmission function is applied in ladder topology, number of entries and its contents shall be same among all CNNs in the sub-network.

NOTE As to the function of the substitute transmission, refer to D.2.6.3.

Table D.3 – Configuration_Process_Data_Transmission_Substitute

Parameter	Type	Description
ConfigurationSubsCnnK	Type_Configuration_ Substitute	Configuration data for substitute transmission of CNN k
ConfigurationSubsCnnL	Type_Configuration_ Substitute	Configuration data for substitute transmission of CNN l
ConfigurationSubsCnnM	Type_Configuration_ Substitute	Configuration data for substitute transmission of CNN m
…	…	…

k, l, m: CNN number to be substituted to transmit

The data structure Type_Configuration_ Substitute shall contain the following elements, listed in Table D.4.

Table D.4 – Type_Configuration_Substitute

Parameter	Type	Description
OffsetPdSubs1	UNSIGNED16	Offset address of Process Data for producer packet 1 for substitute transmission
SizePdSubs1	UNSIGNED12	Size of Process Data for producer packet 1 for substitute transmission [0..1 464]
OffsetPdSubs2	UNSIGNED16	Offset address of Process Data for producer packet 2 for substitute transmission
SizePdSubs2	UNSIGNED12	Size of Process Data for producer packet 2 for substitute transmission [0..1 464]

D.2.8 Signal connection for trunk link

D.2.8.1 General

In order to reduce the weight and wiring cost of vehicles, it is desired to reduce the number of wires and pins of the connector, especially in case of applying ECN to existing vehicles using traditional electric couplers between them. By means of operation of the real time MAC in Link Layer, simultaneous transmission and reception of signals do not occur in the link, so that a single twisted pair cable may be used instead of two twisted pair cable with full duplex operation defined in this standard, in case of Physical Layer of the transmission bit rate of 10 Mbps with the amplifying transceiver for higher robustness.

NOTE The communication with single twisted pair cable and the transceiver with amplified signals are the exceptions which are not compliant to IEEE 802.3.

D.2.8.2 A single twisted pair connection (Option)

Figure D.7 shows the block diagram of the transceiver unit type A, defined in Annex C, with a single twisted pair connection. The differential transmission data signals TD+ and TD- from the IEEE 802.3 10BASE-T MAU are levelled up in the amplifier, which become signals TDRD+ and TDRD- and are led to the transformer. The transmission signals and the received signals are multiplexed at the point of the output of the amplifier, which are also the input of the level conditioner.

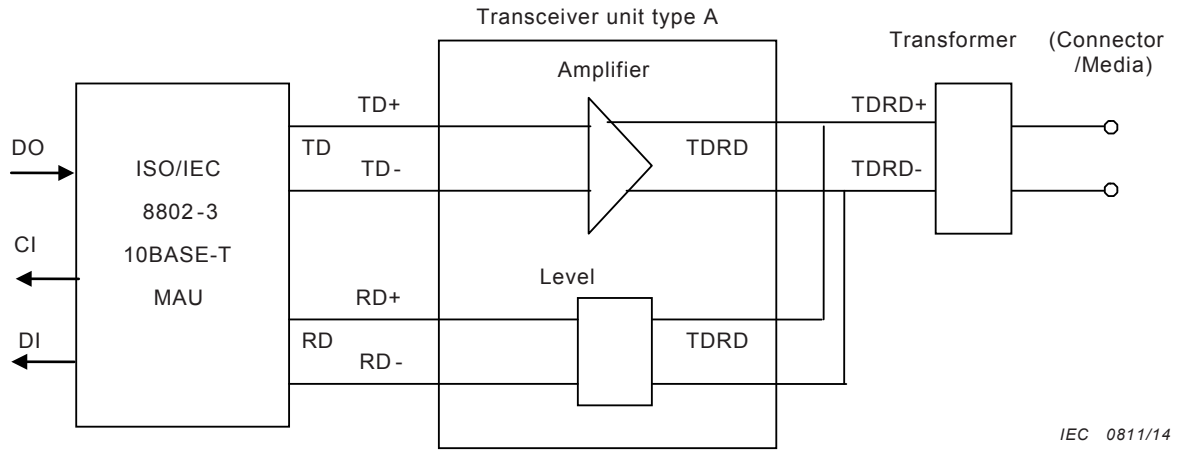


Figure D.7 – Block diagram of the transceiver unit for a single twisted pair connection

The signal connection for a single twisted pair cable is given in Table D.5, which shows the connection between the two transceivers. And Figure D.8 illustrates cable connection with a single shielded twisted pair cable.

Table D.5 – Signal connection between transceivers (single twisted pair)

Signal name	Symbol	Signal direction	Symbol	Signal name
Transmission/ reception	TDRD (+)	⟷	TDRD (+)	Transmission/ reception
	TDRD (-)		TDRD (-)	

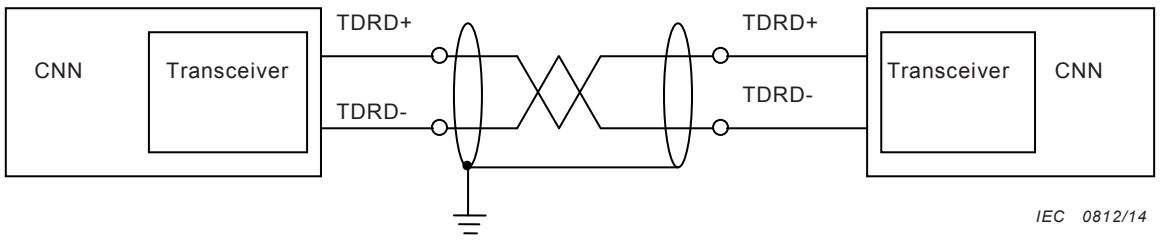


Figure D.8 – Cable connection for a single twisted pair

D.2.9 Local link connection

For the local link ports in ladder topology, the connector described below shall be used.

- M12 D-coded connector

This connector with the pinning conforms to 4.9.4.3 of this standard.

NOTE When a pair of CNNs is implemented in a same unit, any type of connection can be used, e.g. connection through back plane, which is outside the scope of this standard.

D.3 Link Layer

D.3.1 General

This clause defines the Link Layer of the CNN for ladder topology.

In order to implement ladder topology, the real time MAC is adopted to the dedicated trunk link between the CNNs in addition to the function of the MAC of Consist Switch defined in this standard.

NOTE The protocol of the real time MAC is the exception which is not compliant to IEEE 802.1D.

D.3.2 MAC – Media Access Control

D.3.2.1 General

This subclause defines the protocol of the real time MAC, which performs real time control to guarantee deterministic responsibility with shorter cycle time.

The command frames for real time MAC are also used for failure detection and recovery for ladder topology.

By means of the real time MAC protocol defined in this subclause, alternative transmission is performed on trunk links, because the real time MAC protocol controls the traffic so that only one CNN can transmit its frame on the sub-network at a time.

Flow control defined as MAC Control PAUSE operation in IEEE 802.3 shall be supported in interfaces at the InP and at the ExP in real time MAC, which are shown in Figure D.4. The items not defined in this subclause shall be compliant with IEEE 802.3, Clause 2 (Media Access Control service specification).

D.3.2.2 CNN number

D.3.2.2.1 General

Individual CNN numbers are assigned to CNNs, which indicate the sequence of the CNNs in the network. Format of CNN number is shown in Table D.6.

Table D.6 – CNN number

Parameter	Type	Description
CnnNumber	UNSIGNED5	CNN number, initially set by application and not changed during operation. [1..31]

D.3.2.2.2 Assignment of CNN number

CNN number of each CNN shall be initially set by application, which shall be incremental by one from the one end CNN to the other end CNN. CNN numbers are not allowed to be assigned in discontinuous, irregular or duplicated in the order.

The CNN at the one end which is assigned with the minimum number is named as the uppermost CNN and at the other end, as the lowermost CNN. The direction from the uppermost CNN to the lowermost CNN is named as the downward direction and the opposite direction is the upward direction.

In the ladder topology, as shown in Figure D.9 for example, in the sub-network 1, the number begins from the minimum number 1 at the one of the end CNNs and increases to the other end CNN in downward direction. In the sub-network 2, the number shall be assigned as the same to the paired CNN.

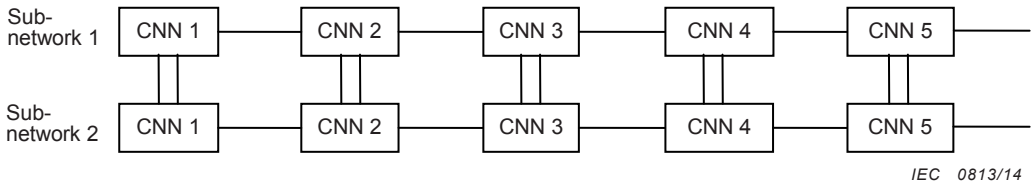


Figure D.9 – Example of CNN number assignment in ladder topology

D.3.2.3 Command frame definition

D.3.2.3.1 General

Five types of the dedicated command frames for the real time MAC are defined and shall be applied to the data link protocol. These command frames are only applied between two neighbouring CNNs at a time. That is, these command frames are not immediately passed to the next CNN, but received, interpreted and then re-transmitted to the next CNN if necessary.

a) Reset command

b) Token command

c) Return command

d) Link command

e) Link-ACK command

a) Reset command

Reset command is issued from the uppermost CNN to the lower CNNs to synchronize the start of cyclic transmission. When the next CNN receives the Reset command from the upper CNN, the CNN becomes an initial state having no token, and then re-transmits the Reset command to the next lower CNN and so forth.

b) Token command

Token command is applied to transfer the transmission right to the next CNN. The CNN, which has received the Token command from the upper CNN, is permitted to transmit its own data frames to the sub-network. After the CNN transmits the data frames, it transmits the Token command to the next lower CNN.

c) Return command

Return command is issued from the lowermost CNN in the upward direction in order to return the transmission right to the uppermost CNN. When an intermediate CNN receives the Return command from the lower CNN, the CNN repeats it to the upper CNN respectively.

d) Link command

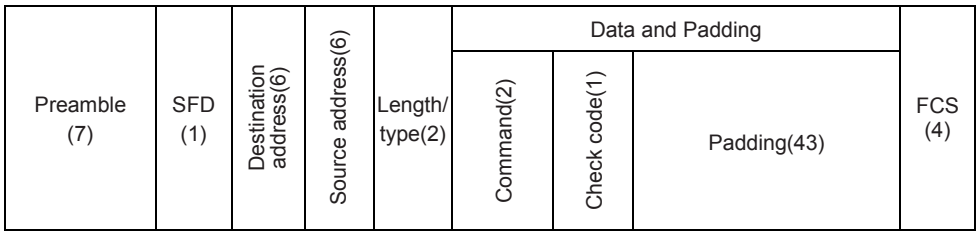
Link command is applied to solicit a new CNN to the sub-network at the lowermost CNN. If a new CNN requests to enter the sub-network, it sends Link-ACK command in return for the Link command.

e) Link-ACK command

Link-ACK command is the response against the Link command for joining the sub-network. Initially, a stand alone CNN is waiting the Link command from the upper CNN. When the CNN receives the Link command, the CNN sends the Link-ACK command to the upper CNN.

D.3.2.3.2 Command frame formats

The frame format for the command is shown in Figure D.10, which is formed in the minimum size of the data link frame.



NOTE The numbers in parenthesis mean size of the field in octet.

Figure D.10 – Frame format for the commands

NOTE 1 Hereinafter in this subclause, octets represented in the field are transmitted from left to right.

a) Destination address field

A particular multicast-group address shall be assigned to the destination address field. The specified number of the destination address field is given in Table D.7.

Table D.7 – Contents of the Destination Address field

Field	Octets in hexadecimal number
Destination Address	01 80 C2 00 00 01

NOTE 2 The address is based on the globally assigned multicast address for MAC control PAUSE operation defined in IEEE 802.3 Annex 31B.

b) Source address field

A particular address shall be assigned to the source address field. The specified number of the source address field is given in Table D.8.

Table D.8 – Contents of the Source Address field

Field	Octets in hexadecimal number
Source Address	00 00 00 00 00 00

NOTE 3 The Source Address field is not interpreted by the Link Layer in this operation.

c) Length/Type field

A particular number shall be assigned to the Length/Type field. The specified number of the Length/Type field is given in Table D.9.

Table D.9 – Contents of the Length/Type field

Field	Octets in hexadecimal number
Length/Type	22 DF

NOTE 4 The Ethernet Type number is assigned for this type of Ethernet frame by IEEE.

d) Command and Check Code fields

Two octets of command field are applied to the data link protocol and an octet of check code is to make the command reliable. The arithmetic for the check code is in the following.

Add the numbers from the first octet of the destination address field to the last octet of the command field, and take 2’s complement of the sum.

Command and check code fields shall be set with the numbers specified in Table D.10 respectively.

Table D.10 – Contents of command and check code fields

Command frames	Fields	Octets in hexadecimal number	Remarks
Reset command	Command	80 nn	nn: '00'h for default, other values are reserved.
	Check code	kk	(See NOTE2)
Token command	Command	10 nn	(See NOTE1)
	Check code	kk	(See NOTE2)
Return command	Command	20 00	
	Check code	0C	
Link command	Command	08 nn	(See NOTE1)
	Check code	kk	(See NOTE2)
Link-ACK command	Command	04 nn	(See NOTE1)
	Check code	kk	(See NOTE2)

NOTE 1 nn: CNN number of the CNN which transmits the command.

NOTE 2 kk: Value which varies depending on the calculation result.

e) Padding field

Forty three octets of padding field shall be set with the specified numbers given in Table D.11.

Table D.11 – Contents of the Padding field

Field	Octets in hexadecimal number
Padding	00 ---------- 00 (all 00 for 43 octets)

f) Frame Check Sequence (FCS) field

Four octets of frame check sequence shall be based on IEEE 802.3, Clause 3 (Media access control frame structure).

D.3.2.4 Network reconfiguration

D.3.2.4.1 General

This subclause describes link establishment for network reconfiguration.

In this subclause, the term of acknowledged link means not just physical link but link with handshake by Link and Link-ACK command frames.

D.3.2.4.2 Initial configuration

In installation of the network, the rules of the initial configuration below shall be applied.

a) Two trunk ports in a CNN are previously configured as the one for the up link port and the other for the down link port. Physical connections between the neighbouring CNNs are determined accordingly.

b) Two neighbouring CNNs are connected with a trunk link between the down link port of one CNN and the up link port of the other CNN.

c) At one end CNN to which the least CNN number is assigned in the network, the up link port in the CNN shall be set to forced link off mode, but not for the down link port.

d) At the other end CNN to which the most CNN number is assigned in the network, the down link port in the CNN shall be set to forced link off mode, but not for the up link port.

e) At other intermediate CNNs, neither their up link ports nor down link ports shall be set to forced link off mode.

At the CNN in which the up link port is set to forced link off mode, transmission of data frames are inhibited at the up link port except Link-ACK command frame responding to Link command frame, if it is received at the port. On the other hand, at the CNN in which the down link port is set to forced link off mode, transmission of data frames are inhibited except Link command frame sending every 20 ms.

D.3.2.4.3 Sequence of link establishment

a) Trunk links

Establishment of acknowledged link between two CNNs is shown in Figure D.11.

In Figure D.11, the upper CNN, or CNN J, after powered up, transmits a Link command frame to downward CNN, or CNN K, through its down link port to the up link port of the next CNN, which is repeated until the sender receives a Link-ACK command frame from the next CNN.

On the other hand, at the lower CNN, or CNN K, after powered up, when the CNN receives a Link command frame, it sends a Link-ACK command frame to the upper CNN, or CNN J, through its up link port.

This handshaking results that an acknowledged link between the two CNNs has been established.

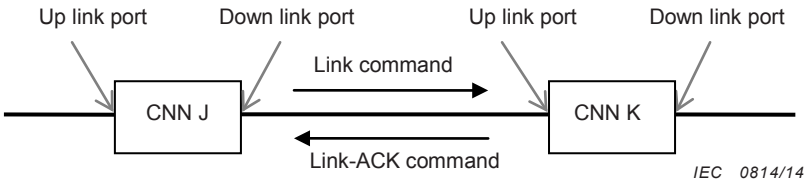


Figure D.11 – Link establishment between two CNNs

This procedure is performed at every trunk link between two neighbouring CNNs in the sub-network respectively. Finally acknowledged links at all trunk ports in the sub-network are established.

If either of Link command frame or Link-ACK command frame is not received normally in a trunk link, acknowledged link is not established at the trunk link. In this case, acknowledged links are established in separated ranges of consecutive CNNs.

In the ladder topology, the acknowledged link establishment is executed independently in the separated two sub-networks (see Figure D.12). After all acknowledged links between the CNNs are established in each sub-network, the network forms a broadcast domain in the range between both end CNNs in the respective sub-network.

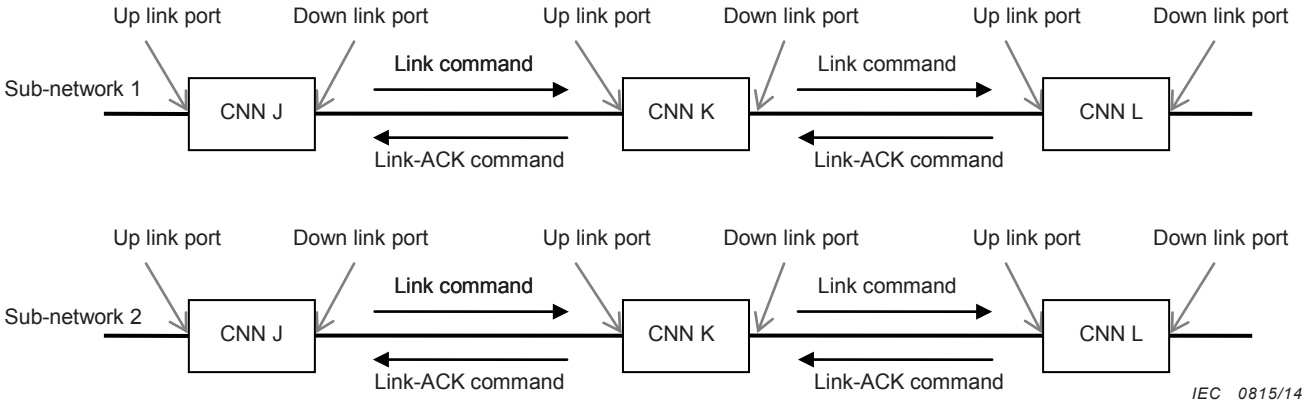


Figure D.12 – Link establishment in ladder topology

b) Local link

Redundant CNNs in a pair connect each other with two full-duplex links (see Figure D.13). Normal physical layer links which are not acknowledged links shall be established in the respective local links.

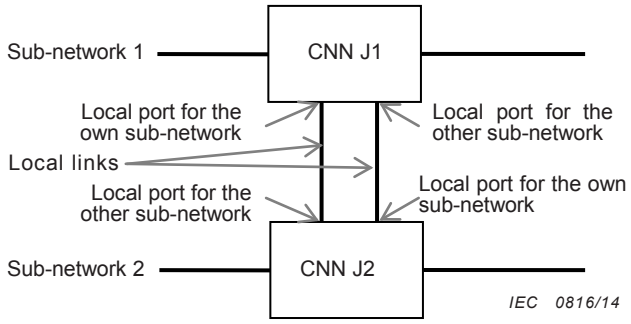


Figure D.13 – Local links between redundant CNNs

D.3.2.4.4 Determination of CNN mode

If a CNN receives no Link command frame at its up link port, the CNN comes to be in the uppermost CNN mode. On the contrary, if a CNN receives no Link-ACK command frame at its down link port, the CNN comes to be in the lowermost CNN mode.

A CNN in which acknowledged links both at the up link port and at the down link port have been established, it comes to be in the intermediate CNN mode. When a CNN has no established trunk port link, it comes to be in the stand-alone CNN mode (see Figure D.14).

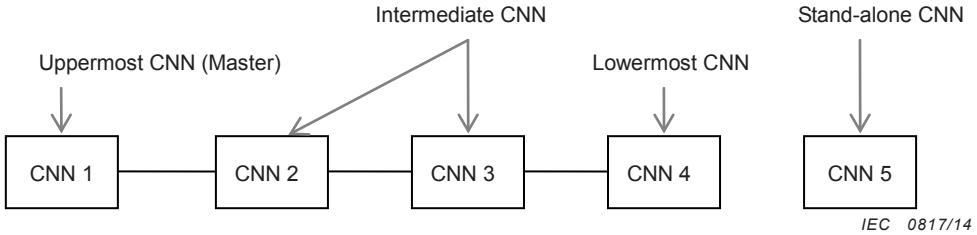


Figure D.14 – Example of CNN modes

In the stand-alone CNN mode, the CNN becomes off-line state in which the CNN waits Link command frame at the up link port and continues to sending Link command frame every 2 ms at the down link port until receiving Link-ACK command frame.

In both sub-networks of the ladder topology, the CNN mode is determined in the same manner. This decision is made by the CNNs respectively as summarized in Table D.12. The uppermost CNN becomes also the master of the network.

At the start up of the networks in the ladder topology, the modes of two CNNs in a pair should be identical.

Table D.12 – CNN mode for CNN in ladder topology

Sub-network	CNN mode	Acknowledged link established at up link port	Acknowledged link established at down link port	Remarks
Sub-network 1	Uppermost CNN (Master)	No (Forced link off)	Yes	Preconfigured
	Lowermost CNN	Yes	No (Forced link off)	Preconfigured
	Intermediate CNN	Yes	Yes	
	Stand-alone CNN	No	No	
Sub-network 2	Uppermost CNN (Master)	No (Forced link off)	Yes	Preconfigured
	Lowermost CNN	Yes	No (Forced link off)	Preconfigured
	Intermediate CNN	Yes	Yes	
	Stand-alone CNN	No	No	

D.3.2.4.5 End of link establishment

The CNN which completes the link establish process of its trunk port for the down link as the master on first-come, first-served basis sends Reset command frame to the downward CNN in order to start cyclic transmission.

Although the CNN sends Reset command early, when the CNN receives any command frame at its up link port, the CNN changes its mode from the uppermost CNN mode to the intermediate CNN mode. Finally, the actual uppermost CNN becomes the master which starts cyclic transmission with token passing on the sub-network. Cyclic transmission is executed on the respective sub-network in the ladder topology independently.

The state diagrams of the network reconfiguration in relation to the token are described in D.3.2.5.

D.3.2.5 Real time MAC protocol

D.3.2.5.1 Real time MAC structure

D.3.2.5.1.1 General

In Figure D.15, boxes inside Link Layer mean blocks of functions which compose MAC sub-layer of real time MAC. Arrows with solid lines mean direction of primitives passed between the boxes. Names of the primitives are indicated near by the arrows.

ACM (Access Control Machine) takes charge of media access control of the network. After acknowledged link has been established, ACM controls token passing and repeating of received frames at one trunk port to the other trunk port.

TPCM (Trunk Port Control Machine) controls trunk port acknowledged links. TPCM sends Link command frame to its down link port, after Link-ACK command frame has been received, establishes acknowledged link between the downward CNN. When Link command frame has been received at up link port, TPCM sends Link-ACK command frame back at the up link port to establish acknowledged link between the upward CNN.

TRRC (Transmission, Reception and Repeat Control) issues physical layer data request primitive at adequate trunk port with requested data from ACM to TRRC. The primitive received at trunk port is de-serialized, and then sent to ACM, TPCM and the other trunk port with the corresponding primitive.

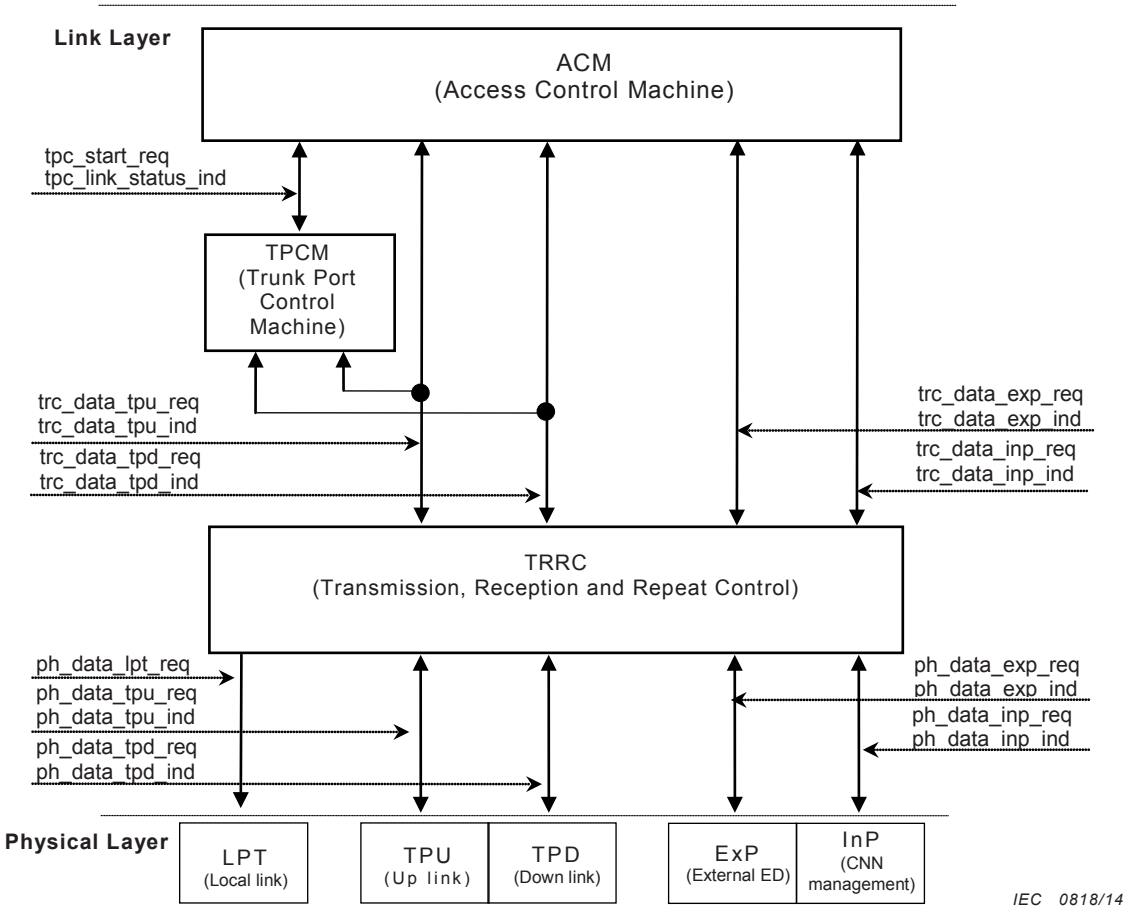


Figure D.15 – Structure and primitives of Real Time MAC sub-layer

D.3.2.5.1.2 Primitives

Primitives provide services to respective state machines.

Physical layer primitives defined in IEEE 802.3, Clause 6 are also used in this standard, which are listed in Table D.13.

Table D.13 – Physical layer primitives

Name	Description
ph_data_tpu_req()	Request primitive to TPU port, corresponding to PLS_DATA.request primitive
ph_data_tpu_ind()	Indication primitive from TPU port, corresponding to PLS_DATA.indication primitive
ph_data_tpd_req()	Request primitive to TPD port, corresponding to PLS_DATA.request primitive
ph_data_tpd_ind()	Indication primitive from TPD port, corresponding to PLS_DATA.indication primitive
ph_data_inp_req()	Request primitive to InP port, corresponding to PLS_DATA.request primitive
ph_data_inp_ind()	Indication primitive from InP port, corresponding to PLS_DATA.indication primitive
ph_data_exp_req()	Request primitive to ExP port, corresponding to PLS_DATA.request primitive
ph_data_exp_ind()	Indication primitive from ExP port, corresponding to PLS_DATA.indication primitive
ph_data_lpt_req()	Request primitive to LPT port, corresponding to PLS_DATA.request primitive

D.3.2.5.1.3 Variables and parameters

Variables and parameters used in the description of real time MAC protocol are defined in Table D.14.

Table D.14 – Variables and parameters for real time MAC protocol

Variable and parameters	Description
CnnMode	One of the CNN modes determined in the topology; Uppermost, Lowermost, Intermediate or Standalone
forceOffTPU	True when trunk port for upper link is in forced link off, otherwise false (See NOTE.)
forceOffTPD	True when trunk port for down link is in forced link off, otherwise false (See NOTE.)
ENInp	Acceptable number of frames from internal port, when CNN has held Token and TTRT2 has not expired.
ENExp	Acceptable number of frames from external port, when CNN has held Token and TTRT2 has not expired.
frame	Delivered frame with primitive, specific values of which are listed in Table D.15.
linkTPU	True when trunk port link is established between upward CNN with coupling of Link command and Link-ACK command, otherwise False.
linkTPD	True when trunk port link is established between downward CNN with coupling of Link command and Link-ACK command, otherwise False.
receivingTPU	True when linkTPU is true and Rest command or Token command is received. False when TNORU timer is expired, started after linkTPU become true.
receivingTPD	True when linkTPD is true and Return command is received. False when TNORD timer is expired, started after linkTPD become true.
VTL1	Value set to the timer for the cycle; 2 ms as default for lowermost CNN mode and stand-alone mode.
VTL2	Time value set into TL2 timer for delay sending Link-ACK command frame after reception of Link command frame; 0,5 ms as default
VTLT	Time value set into TLT timer for monitoring re-configuration; 15 ms as default
VTNORU	Time value set into TNORU timer for monitoring reception status at the trunk port for up link; twice VTLT as default
VTNORD	Time value set into TNORD timer for monitoring reception status at the trunk port for down link; twice VTLT as default
VTTRT1	Time value set into TTRT1 timer; 8 ms as default
VTTRT2	Time value set into TTRT2 timer; 9 ms as default
VTREQ	Time value for monitoring transmit request of a frame after sending PAUSE0 frame at the port; 50 μs as default
PortDirection	True when the TPU corresponds to the primitives of trc_data_tpu_req and trc_data_tpu_ind, and the TPD to trc_data_tpd_req and trc_data_tpd_ind. False when, on the contrary, the TPU corresponds to the primitives of trc_data_tpd_req and trc_data_tpd_ind, and the TPD to trc_data_tpu_req and trc_data_tpu_ind.
NOTE Forced link off means the state in which data frames received at the trunk port are prohibited to be passed to both the next CNN and the End Devices.	

Table D.15 – Frame name

Frame name	Description
LINK	Link command frame
LINKACK	Link-ACK command frame
PAUSE0	PAUSE frame with pause time 0 (See NOTE)
PAUSEX	PAUSE frame with pause time x; twice TLT as defalt (See NOTE)
RESET	Reset command frame
TOKEN	Token command frame
RETURN	Return command frame
NOTE The operations of frames PAUSE0 and PAUSEX accord with MAC Control PAUSE operation in IEEE 802.3.	

D.3.2.5.1.4 Timers

Timers used in the description of real time MAC protocol are defined in Table D.16.

Table D.16 – Timers for real time MAC protocol

Timers	Description
TL1	Period to try to establish trunk port link cyclically or time out to receive
TL2	Delay time after reception of Link command frame to send Link-ACK command frame
TLT	Limit timer for time out for Return command frame reception, which shall be greater than T_{TTRT2}
TNORU	Timer to detect no signal reception at TPU
TNORD	Timer to detect no signal reception at TPD
TTRT1	Target-Token-Rotation-Timer-1; starts at sending or receiving Reset command frame, when expired, token holding CNN re-sends Token to the next CNN, in case of the lowermost CNN, sends Return command frame, with permission to send data frame for internal port but prohibition for external port. (T_{TTRT1} <= T_{TTRT2})
TTRT2	Target-Token-Rotation-Timer-2; starts at sending or receiving Reset command frame, when expired, token holding CNN shall send Token to the next CNN immediately, in case of the lowermost CNN, it sends Return command frame, with prohibition to send data frame both for internal port and for external port. (T_{TTRT1} <= T_{TTRT2})
TREQ	Timer to detect no data frame requested from the port which is permitted to send after send PAUSE frame with pause time 0.

D.3.2.5.1.5 Procedures

Procedures which are common to the real time MAC protocol are defined in Table D.17.

Table D.17 – Procedures for real time MAC protocol

Procedures	Description
delay(timer)	Delay with specified in (timer)
detectCNNLocation	Determine initial state of trunk ports according to preset CNN mode. For the uppermost CNN mode, make up link port off and down link port on. For the lowermost CNN mode, make up link port on and down link port off. For intermediate CNN mode, make both up link port and down link port on.
initReconfiguration	Execute the following initialization, necessary for reconfiguration a) Set linkTPD False b) Send PAUSE frames with time TPAUSE to both internal port and external port. TPAUSE shall be greater than TCYCLE, default of which is three times of TCYCLE.
startTimer(timer)	Start the timer specified in (timer). If the specified timer is operating, it is reset and re-started.
stopTimer(timer)	Stop the timer specified in (timer).

D.3.2.5.1.6 Events

Events which are common to the real time MAC protocol are defined in Table D.18.

Table D.18 – Events for real time MAC protocol

Events	Description
request primitive	Request is issued.
indication primitive	Indication of data or status
expiredTimer(timer)	Timer started by startTimer procedure expired.

D.3.2.5.2 TRRC operation

D.3.2.5.2.1 TRRC primitives

Primitives defined for TRRC operation are listed in Table D.19.

Table D.19 – TRRC primitives

Name	Meaning
trc_data_tpu_req(frame)	Request primitive to TPU
trc_data_tpu_ind(frame)	Indication primitive from TPU
trc_data_tpd_req(frame)	Request primitive to TPD
trc_data_tpd_ind(frame)	Indication primitive from TPD
trc_data_inp_req(frame)	Request primitive to InP port
trc_data_inp_ind(frame)	Indication primitive from InP port
trc_data_exp_req(frame)	Request primitive to ExP port
trc_data_exp_ind(frame)	Indication primitive from ExP port

D.3.2.5.2.2 TRRC request primitive and operation

TRRC operation on acceptance of request primitives is defined in Table D.20.

After TRRC has accepted a request primitive issued from ACM or TPCM, TRRC packs received data in frame and serialize it as defined in IEEE 802.3, and issues physical request primitive corresponding to the TRRC request primitive.

Table D.20 – TRRC operation on acceptance of request primitives

Accepted request primitive	TRRC operation
trc_data_tpu_req	packs received data in frame and serialize it, and issues ph_data_tpu_req primitive.
trc_data_tpd_req	packs received data in frame and serialize it, and issues ph_data_tpd_req primitive.
trc_data_inp_req	packs received data in frame and serialize it, and issues ph_data_inp_req primitive.
trc_data_exp_req	packs received data in frame and serialize it, and issues ph_data_exp_req primitive.

D.3.2.5.2.3 Physical indication primitive and TRRC operation

TRRC makes frame in IEEE 802.3 format out of signals received at port of TPU, TPD, InP or ExP with physical indication primitive, and issues corresponding physical indication primitive from TRRC to TPCM and ACM.

Further, in case that destination address of received frame does not match that of MAC Control frame, TRRC forwards the frame to all other ports.

TRRC operation on acceptance of physical indication primitives is defined in Table D.21.

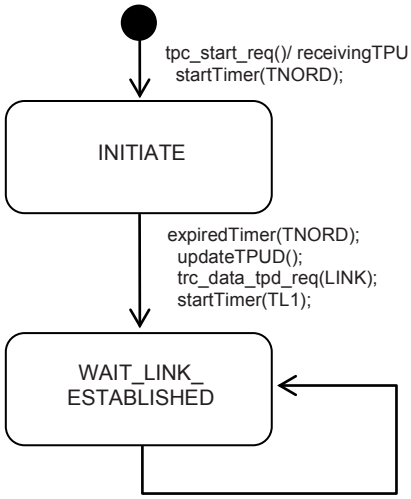
Table D.21 – TRRC operation on acceptance of physical indication primitives

Accepted physical indication primitive	TRRC operation
ph_data_tpu_ind	IF destination address (DA) does not match that of Real Time MAC control frame; THEN Transfer the DA and following signals to all other ports of LPT, TPD, InP, ExP. ENDIF Make frame out of received signals, and issue trc_data_tpu_ind and trc_data_tpud_ind primitives.
ph_data_tpd_ind	IF destination address (DA) does not match that of Real Time MAC control frame; THEN Transfer the DA and following signals to all other ports of LPT, TPU, InP, ExP. ENDIF Make frame out of received signals, and issue trc_data_tpd_ind and trc_data_tpud_ind primitives.
ph_data_inp_ind	IF destination address (DA) does not match that of Real Time MAC control frame; THEN Transfer the DA and following signals to all other ports of LPT, TPU, TPD, ExP. ENDIF Make frame out of received signals, and issue trc_data_inp _ind primitive
ph_data_exp_ind	IF destination address (DA) does not match that of Real Time MAC control frame; THEN Transfer the DA and following signals to all other ports of LPT, TPU, TPD, InP. ENDIF Make frame out of received signals, and issue trc_data_exp _ind primitive

D.3.2.5.3 TPCM operation

D.3.2.5.3.1 State machine of TPCM

Figure D.16 shows protocol state machine of TPCM. Table D.22 shows state transition table for TPCM. Procedures in TPCM state machine are liste in Table D.23.



trc_data_tpu_ind(frame); [frame == LINK]/
delay(TL2); trc_data_tpu_req(LINKACK); receivingTPU = True; updateTPUD(); startTimer(TNORU);

trc_data_tpd_ind(frame)[frame == LINKACK]/
receivingTPU = True; updateTPUD(); startTimer(TNORD); startTimer(TL1);

trc_data_tpu_ind(frame)[(frame == RESET || frame == TOKEN) && linkTPU == True && forceOffTPU == False]/
receivingTPU = True; updateTPUD(); startTimer(TNORU);

trc_data_tpd_ind(frame[frame == RETURN) && linkTPD == True && forceOffTPD == False]/
receivingTPD = True; updateTPUD(); startTimer(TNORD);

expiredTimer(TNORU); /
receivingTPU = False; updateTPUD();

expiredTimer(TNORD); /
receivingTPD = False; updateTPUD(); startTimer(TL1);

expiredTimer(TL1)/ if (linkTPD != True || forceOffTPD) trc_data_tpd_req(LINK); startTimer(TL1);

IEC 0819/14

Figure D.16 – TPCM state machine

Table D.22 – State transition table for TPCM

Current state	Event[condition]	Actions	Next State

Initial state	tpc_start_req()	// Start state machine, initialize variables and start TNORD timer
		receivingTPU = False; receivingTPD = False;
		startTimer(TNORD);
			INITIATE

INITIATE	expiredTimer(TNORD);	// TNORD timer expires, indicate link status and send the first Link command
		updateTPUD();
		trc_data_tpd_req(LINK);
		startTimer(TL1);
			WAIT_LINK_
			ESTABLISHED

WAIT_LINK_
ESTABLISHED
	trc_data_tpu_ind(frame)
	[frame == LINK]
		// Receive Link command from TPU
		delay(TL2);
		trc_data_tpu_req(LINKACK);
		receivingTPD = True;
		updateTPUD();
		startTimer(TNORU);
			WAIT_LINK_
			ESTABLISHED

	trc_data_tpd_ind(frame)
	[frame == LINKACK]
		// Receive Link command from TPD
		receivingTPD = True
		updateTPUD();
		startTimer(TNORD);
		stopTimer(TL1);	

	trc_data_tpu_ind(frame);
	[(frame == RESET ||
	frame == TOKEN) &&
	linkTPU == True &&
	forceOffTPU == False]
		// Receive from TPU
		receivingTPU = True;
		updateTPUD();
		startTimer(TNORU);	

	trc_data_tpd_ind(frame);
	[frame == RETURN &&
	linkTPD == True &&
	forceOffTPD == False]
		// Receive from TPD
		receivingTPD = True;
		updateTPUD();
		startTimer(TNORD);	

	expiredTimer(TNORU);	// TNORU timer expires, change Link status
		receivingTPU = False;
		updateTPUD();	

	expiredTimer(TNORD);	// TNORD timer expires, change Link status
		receivingTPD = False;
		updateTPUD();
		startTimer(TL1);	

	expiredTImer(TL1)	// Timer for link establish expires
		if (linkTPD != True) {
		trc_data_tpd_req(LINK);
		}
		startTimer(TL1);	

Table D.23 – Procedures in TPCM state machine

Procedure	Description

updateTPUD()	// Update the status of link establishment of TPU and TPD. On detecting change, issue the primitive tpc_link_status_ind.
	if (receivingTPU != linkTPU || receivingTPD != linkTPD) {
	linkTPU = receivingTPU; linkTPD = receivingTPD;
	tpc_link_status_ind(linkTPU, linkTPD);
	}

D.3.2.5.3.2 TPCM primitives

Primitives defined for TPCM are listed in Table D.24.

Table D.24 – TPCM primitives

Name	Meaning
tpc_start_req()	start TLC state machine
tpc_link_status_ind(stsTPU, stsTPD)	indication of trunk port states stsTPU: state of trunk port for up link stsTPD: state of trunk port for down link

D.3.2.5.4 ACM operation

D.3.2.5.4.1 ACM state machine

Figure D.17 shows ACM state machine and Figure D.18 shows state diagram of USE_TOKEN. Table D.25 shows state transition table for ACM. And Table D.26 shows state transition table for USE_TOKEN.

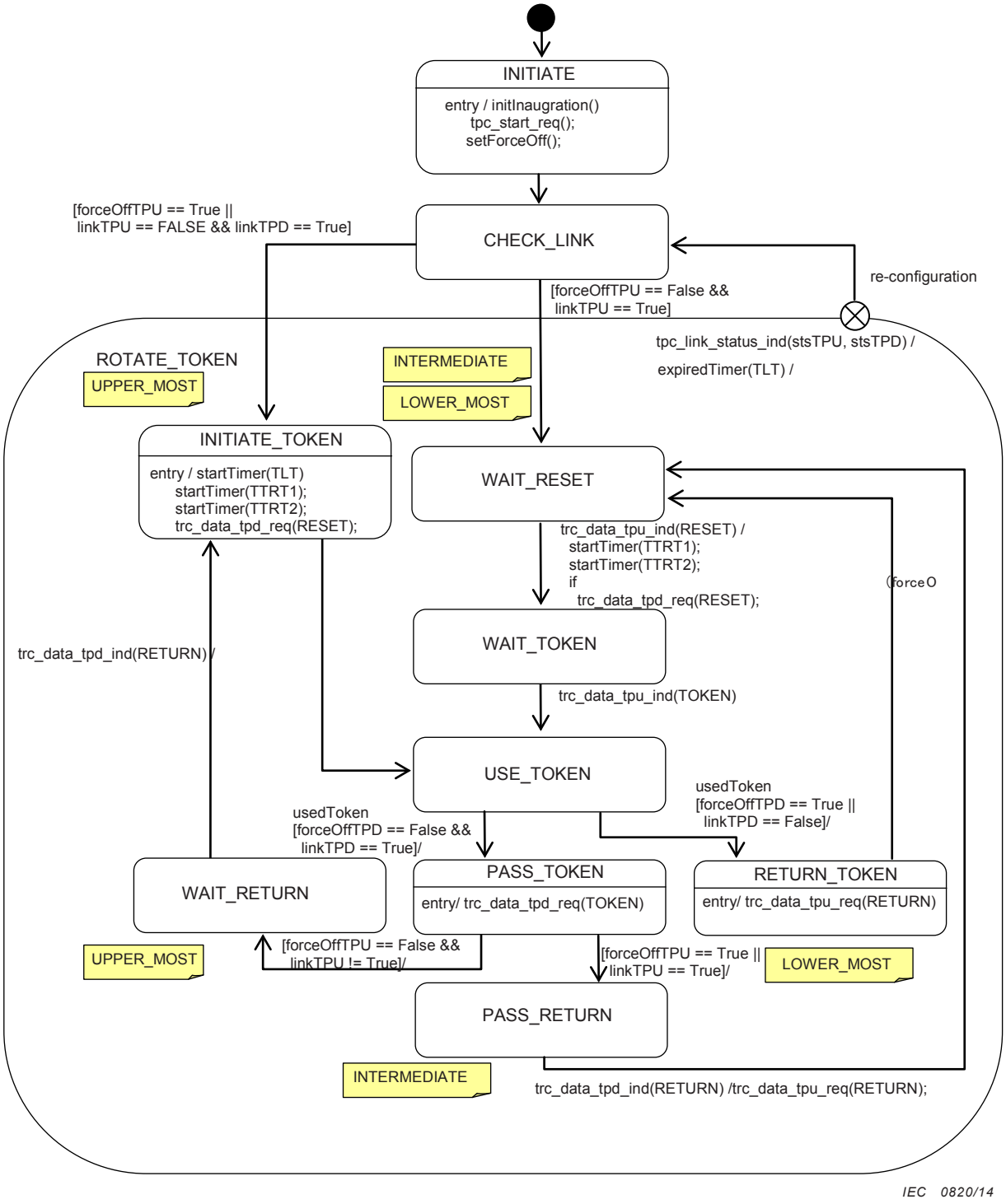


Figure D.17 – ACM state machine

Table D.25 – State transition table for ACM

Current state	Event[condition]	Actions	Next State

INITIATE	entry	// Start initialization
		initReconfiguration();
		tpc_start_req();
		setForceOff();
			CHECK_LINK

CHECK_LINK	[forceOffTPU == True || linkTPU == False && linkTPD == True]	-	INITIATE_TOKEN
	[forceOffTPU == False && linkTPD == True]	-	WAIT_RESET

INITIATE_TOKEN	entry	// Start Token rotation at Uppermost CNN
		startTimer(TLT);
		startTimer(TTRT1);
		startTimer(TTRT2);
		trc_data_tpd_req(RESET);
			USE_TOKEN

WAIT_RESET	trc_data_tpd_ind(RESET)	// Receive RESET command at Intermediate CNN or Lowermost CNN
		startTImer(TTRT1);
		startTimer(TTRT2);
		// If link for downward established, repeat RESET command
		if (forceOffTPD == False && linkTPD == True) {
		trc_data_tpd_req(RESET);
		}
			WAIT_TOKEN

WAIT_TOKEN	trc_data_tpu_ind(TOKEN)	// Receive TOKEN	USE_TOKEN
USE_TOKEN	usedToken [forceOffTPD == False && linkTPD == True]	// Finish Use Token, downward link established	PASS_TOKEN
	usedToken [forceOffTPD == True || linkTPD == False]	// Finish Use Token, downward link not established	RETURN_TOKEN

PASS_TOKEN	entry
	[forceOffTPU ==False && linkTPU == True]
		// Send TOKEN downward, repeat RETURN
		trc_data_tpd_req(TOKEN);
			PASS_RETURN

	entry
	[forceOffTPU == True || linkTPU != True]
		// Send TOKEN downward, wait RETURN
		trc_data_tpd_req(TOKEN);
			WAIT_RETURN

RETURN_TOKEN	entry	// In Lowermost CNN, Send RETURN upward
		trc_data_tpu_req(RETURN);
			WAIT_RESET

PASS_RETURN	trc_data_tpd_ind(RETURN)	// In Intermediate CNN, forward RETURN upward after it received from the lower
		trc_data_tpu_req(RETURN);
			WAIT_RESET

WAIT_RETURN	trc_data_tpd_int(RETURN)	// In Uppermost CNN, re-start TOKEN circulation after reception of RETURN	INITIATE_TOKEN

Current state	Event[condition]	Actions	Next State
Except INITIATE and CHECK_LINK state	tpc_link_status_ind(stsTPU, stsTPD)	// Network re-configuration generated	CHECK_LINK
	expiredTimer(TLT);	// Network re-configuration generated	

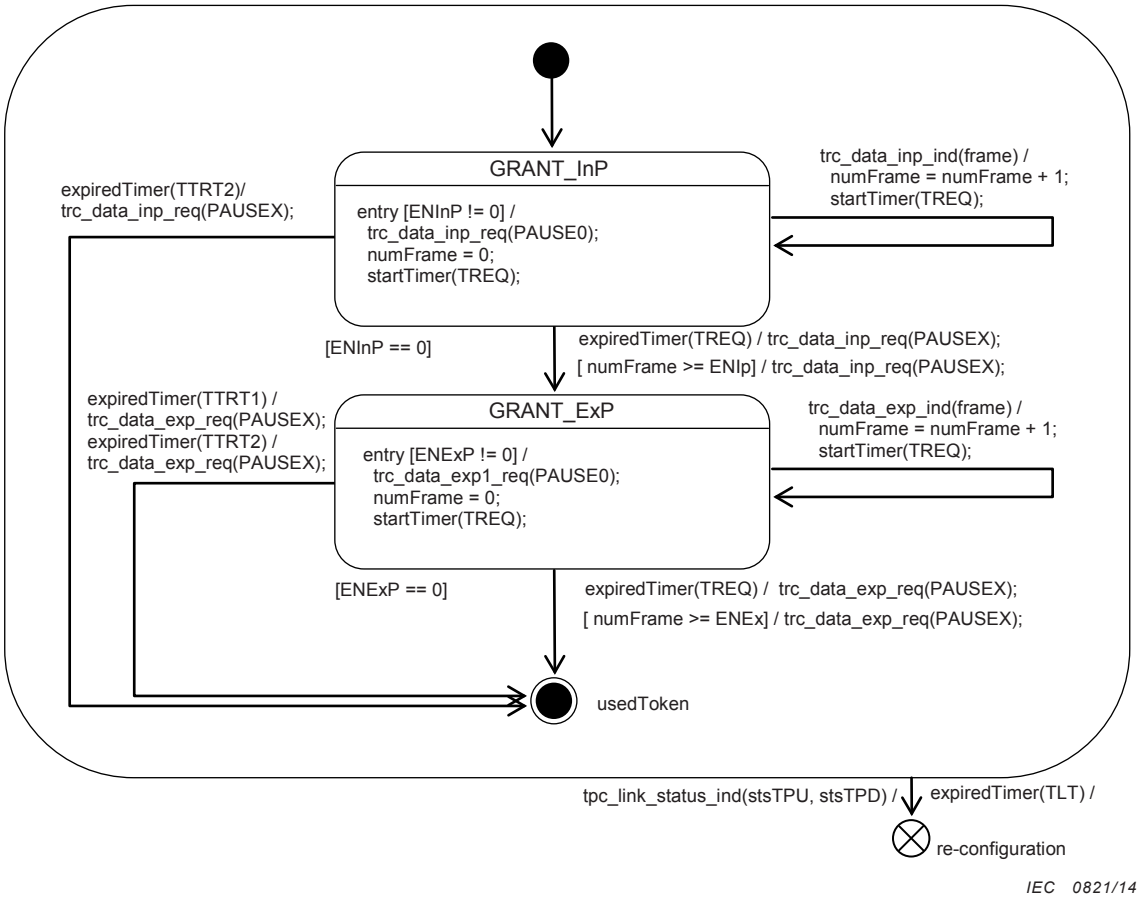


Figure D.18 – State diagram of USE_TOKEN

Table D.26 – State transition table for USE_TOKEN

Current state	Event	Actions	Next State

GRANT_InP	entry[ENInP != 0]	// transmission from InP is granted.
		trc_data_inp_req(PAUSE0);
		numFrame = 0;
		startTImer(TREQ);
			GRANT_InP

	entry[ENInP == 0]	// transmission from InP is not granted.	GRANT_ExP

	trc_data_inp_ind(frame);	// frame from InP received
		numFrame++;
		startTimer(TREQ);
			GRANT_InP

	expiredTimer(TREQ);	// Pause frame because of no frame transmitted from InP
		trc_data_inp_req(PAUSEX);
			GRANT_ExP

	numFrame >= ENIp;	// Pause frame because number of transmitted frames from InP reaches to limit
		trc_data_inp_req(PAUSEX);
			GRANT_ExP

	expired(TTRT2);	// Timer TTRT2 expires, pause frame from InP
		trc_data_inp_req(PAUSEX);
			Final state

GRANT_ExP	entry[ENExP != 0]	// Transmission from ExP is granted.
		trc_data_exp1_req(PAUSE0);
		numFrame = 0;
		startTImer(TREQ);
			GRANT_ExP

	entry[ENExP == 0]	// Transmission from ExP is not granted.	Final state

	trc_data_inp_ind(frame);	// Receive frame from ExP
		numFrame++;
		startTimer(TREQ);
			GRANT_ExP

	expiredTimer(TREQ);	// Pause frame because of no frame transmitted from ExP
		trc_data_exp_req(PAUSEX);
			Final state

	numFrame >= ENEx;	// Pause frame because number of transmitted frames from ExP reaches to limit
		trc_data_exp_req(PAUSEX);
			Final state

	expired(TTRT2); ||
	expired(TTRT1);
		// Timer TTR1 or TTR2 expirers, pause frame from ExP
		trc_data_exp_req(PAUSEX);
			Final state

Any state	tpc_link_status_ind()	// Initiate re-configuration	FInal state
	expiredTimer(TLT)	// Initiate re-configuration	

D.3.2.5.4.2 Variable

ACM uses local variable defined in Table D.27.

Table D.27 – Variable for ACM

Variable	Description
numFrame	number of received frames from internal port or external port during CNN holds Token

D.3.2.5.5 Configuration for real time MAC

Configuration parameters for real time MAC are defined in Table D.28. Configuration parameters shall be given by application and passed to real time MAC through CNN management.

Table D.28 – Configuration parameters for real time MAC

Parameter	Type	Meaning
NetworkTopology	ENUM2	Network topology [0]: Linear [1]: Reserved [2]: Ladder [3]: N/A
ForceSetCnnMode	BOOLEAN1	Force to set CNN mode FALSE: No TRUE: Yes
ForcedCnnMode	ENUM2	When ForceSetCnnMode is TRUE, set CNN mode; [0]: Stand alone CNN mode [1]: Uppermost CNN mode [2]: Lowermost CNN mode [3]: Intermediate CNN mode
DisableTrunkTxrx	ENUM2	Disable to transmit and receive for trunk ports [0]: not disable either port [1]: disable down link port [2]: disable up link port [3]: disable both down link and up link ports
DirectionSwitch	BOOLEAN1	Switch direction of trunk ports FALSE: Set up link port to Direction_1 and down link port to Direction_2 TRUE: Set them to reverse combination of the above.
PermitedPacketCountInp	UNSIGNED4	Permitted packet count to send for internal port during Token holding [0]: no permission to send [1..15]: number of permitted packets to send
PermitedPacketCountExp	UNSIGNED4	Permitted packet count to send for external port during Token holding [0]: no permission to send [1..15]: number of permitted packets to send
CnnNumber	UNSIGNED5	CNN number: [1..31]
TotalNumberOfCnns	UNSIGNED6	Total number of CNNs: [1..31]
TransmissionLinkSubnetworkId	ENUM1	Identification of the sub-network for trunk link in which the CNN is placed [0]: sub-network 1 [1]: sub-network 2

Parameter	Type	Meaning
DataSizeProducerPacket1	UNSIGNED10	Data size for producer packet 1 (N-1): [0..1 023]
DataSizeProducerPacket2	UNSIGNED10	Data size for producer packet 2 (N-1): [0..1 023]
DataSizeCnnManagement	UNSIGNED10	Data size for CNN management (N-1): [0..1 023]
SubstituteTransmission	BOOLEAN1	Enable substitute transmission FALSE: No TRUE: Yes
PermitedPacketCountSubs	UNSIGNED4	Permitted packet count for substitute transmission: [1..15] Internally, permitted packet count for internal port is changed to; [PermitedPacketCountInp] + [PermitedPacketCountSubs]
EnableTargetTokenRotationTime1	BOOLEAN1	Enable Target Token Rotation Time 1 (TTRT1) FALSE: No TRUE: Yes
TargetTokenRotationTime1	UNSIGNED7	Target Token Rotation Time 1 (TTRT1) In order to keep token rotation time, when expired, transmission is restricted except for data frame from internal port. [1..127]: time value in unit of 0,1 ms
EnableTargetTokenRotationTime2	BOOLEAN1	Enable Target Token Rotation Time 2 (TTRT2) FALSE: No TRUE: Yes
TargetTokenRotationTime2	UNSIGNED7	Target Token Rotation Time 2 (TTRT2) In order to keep token rotation time, when expired, transmission is restricted except for Token frame. [1..127]: time value in unit of 0,1 ms TTRT2 > TTRT1

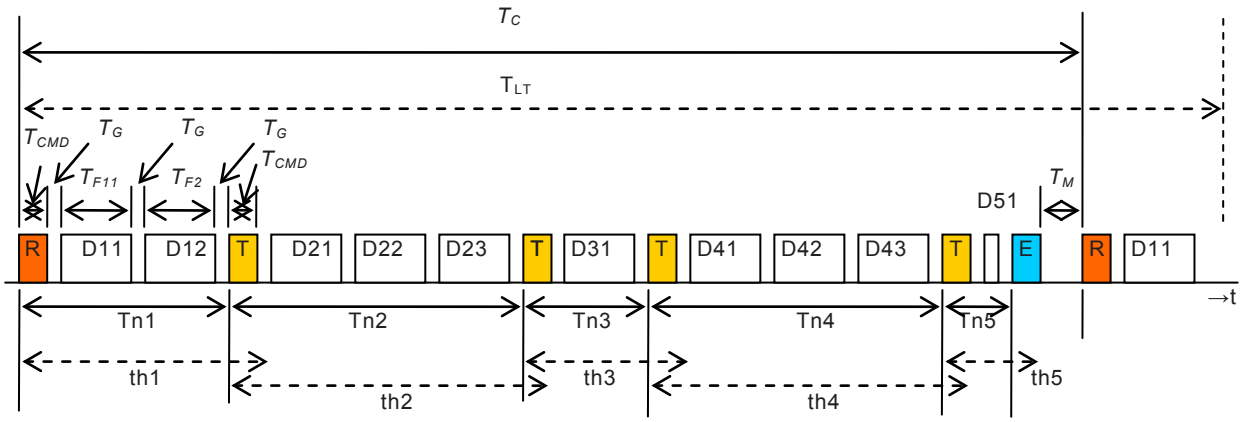
D.3.2.5.6 Real time control

In each sub-network of the ladder topology, a CNN can transmit its frames to the sub-network while holding the token and the token circulates among all CNNs in turn.

EXAMPLE: Figure D.19 illustrates an example of sequence of transmission on the sub-network with five CNNs and the explanation is described below. The time elements for the sequence of transmission are described in Table D.29.

First, the uppermost CNN, or CNN 1, issues Reset command on the sub-network, after that, transmits two data frames and the subsequent Token command. The next lower CNN, or CNN 2, transmits three data frames and the subsequent Token command. CNN 3 transmits a single data frame and the subsequent Token command. CNN 4 transmits three data frames and subsequent Token command. Finally, the lowermost CNN, or CNN 5, transmits a data frame and the Return command.

After the end of cycle margin time (T_M) from reception of the Return command, CNN 1 issues Reset command for the next cycle. When CNN 1 does not receive the Return command within the limit time (T_{LT}), it issues Reset command compulsorily.



R Reset command frame
T Token command frame
E Return command frame
Dij No.j Data frame from CNN i

IEC 0822/14

Figure D.19 – Example of sequence of transmission

Table D.29 – Time elements for sequence of transmission

Time elements	Description
T_C	Cycle time at the cycle; varies every cycle.
T_{C_MAX}	Maximum cycle time; can be calculated.
T_{LT}	Limit time for Return time out; pre-determined for waiting Return is sent back.
T_{CMD}	Command frame time; constant depending on the command frame length.
T_G	Inter frame gap time; defined in IEEE 802.3 with the minimum and depends on the implementation.
T_{Fi}	Data frame time; varies depending on the application data size.
T_M	End of cycle margin time; pre-determined by configuration, including the all latency of passing CNNs and all latencies of links between CNNs.
Tni	Time for CNN i data transmission; varies depending on the amount of the data in the application.
thi	Maximum token hold time for CNN i; pre-determined for each CNN depending on the application

D.3.2.5.7 Data class service parameters

Data class service parameters of the CNN with the real time MAC are described in Table D.30, in which, in order to guarantee deterministic responsibility, the maximum cycle time can be calculated with the equations for T_{C_MAX}.

Table D.30 – Data class service parameters

Data class	Parameter	Value	Comments
Process Data	Cycle time	$T_{C\_MAX} = T_{CMD} \times N + T_G(N+F) + \sum_{i=1}^{F} T_{Fi} + T_M$ $T_{Fi} = (L_{Hi} + L_{Di}) \times 8 / BR$ where T_{C_MAX}: Maximum cycle time T_{CMD}: Command frame time (72 × 8 / BR) N: Number of CNNs in the network, T_G: Inter frame gap time including flow control frame time F: Number of data frames transmitted on the network, T_{Fi}: Time for transmission of data frame i L_{Hi}: Length of preamble and headers for MAC, IP and UDP or TCP of data frame i in octets L_{Di}: Length of service data of data frame i in octets. BR: Bit rate (10 Mbps or 100 Mbps) T_M: Margin time at the end of cycle	Typically, T_{C_MAX} is less than 10 ms for 16 CNNs with the service data size of PD below; 128 octets/CNN for 10 Mbps, 1 280 octets/CNN for 100 Mbps.
	Latency	$T_X + T_{BL} \times N + \sum_{i=1}^{N-1} LL_i + Tcj + T_X$ where N : number of CNNs between sender and taget EDs, T_X : time for frame to send out depending on the length, T_{BL} : Latency of passing a CNN; 128 bit time, LLi : Latencies of links between (i)th and (i+1)th CNNs from sender ED adding latency between sender ED and the CNN and latency between target ED and the CNN Tcj : Jitter caused by the cycle time; 0 to T_{C_MAX}	N=2..31 A bit time depends on transmission bit rate; 0,1 μs for 10 Mbps, 0,01 μs for 100 Mbps.
	Jitter	0 to T_{C_MAX}	
Message Data	Latency	(Same as that of Process Data)	
	Jitter	(Same as that of Process Data)	
Stream data	Latency	(Same as that of Process Data)	
	Jitter	(Same as that of Process Data)	
Best effort data	Latency	(Same as that of Process Data)	
	Jitter	(Same as that of Process Data)	
Supervisory data	Latency	(Same as that of Process Data)	
	Jitter	(Same as that of Process Data)	

D.3.2.5.8 Bandwidth control

The bandwidth of the network is distributed as the token holding periods of the respective CNNs except the margin of the cycle time, in which only the CNN holding the token can transmit its data frame to the network in turn.

During token holding time in a CNN, End devices connected to the CNN share the time to transmit their data frames.

This is controlled by the permitted maximum frame count and by the target token rotation time at each CNN, which are pre-configured by the application.

QoS shall be supported with the switch function of CNN according to 4.6.

D.3.3 IP address and IP address management

D.3.3.1 General

General format of IP address for ECN is defined in this standard. This subclause defines the host field of the IP address for the network in ladder topology. Assignment to other fields than the host field shall follow the definition of this standard.

D.3.3.2 Individual IP address assignment

The IP address format in this network shall accord with the following.

00001010.xxxxxxxx.xx**innnnn**.**dddddddd** /18

The notation for the IP address fields in the above is described in Table D.31.

Table D.31 – Notation for IP address fields

Notation	Description
[x]	(According to IP address in this standard.)
[i]	Subnet-id extension inside the ECN [0-1] (See NOTE 1)
[n]	Default number of the CNN [1-31] for inside CNN ports (See NOTE 2), or Upper 5 bit extension of [d] field for external End Devices (See NOTE 3)
[d]	a) Default numbers for inside CNN ports; [1]: Port for CNN management of the CNN in the sub-network 1, [2]: Port for CNN management of the CNN in the sub-network 2, [3]: Port for the local link to the other side sub-network in the sub-network 1, [4]: Port for the local link to the other side sub-network in the sub-network 2 [5-15]: Reserved b) For external End Devices (See NOTE 3); [0]: Not used [1-254]: Device numbers for external End Devices [255]: Not used

NOTE 1 Different subnet-IDs are used for each sub-network 1 and 2.

NOTE 2 CNN number is defined in D.3.2.2 in this standard, which is assigned statically.

NOTE 3 IP addresses for external End Devices may be assigned dynamically with the ranges of [n] and [d] by avoiding the default numbers used for the inside CNN ports and all '1' and all '0'.

D.4 Consist Network Node management protocol

D.4.1 General

This clause describes the CNN management protocol in the ladder topology.

D.4.2 Architecture of CNN management

Figure D.20 shows the architecture of CNN management.

The CNN management periodically updates the CNN management database with the link status of the up link, down link and local links in the CNN and sends the link status as CNN management information to other CNNs with multicast communication.

When a CNN receives the CNN management information from the other CNN, the CNN management updates the CNN management database with the link status corresponding to the source CNN.

By executing the above periodically and also in every change of the link status, each CNN is possible to recognize the all link status of CNNs and all CNN healthiness on the network.

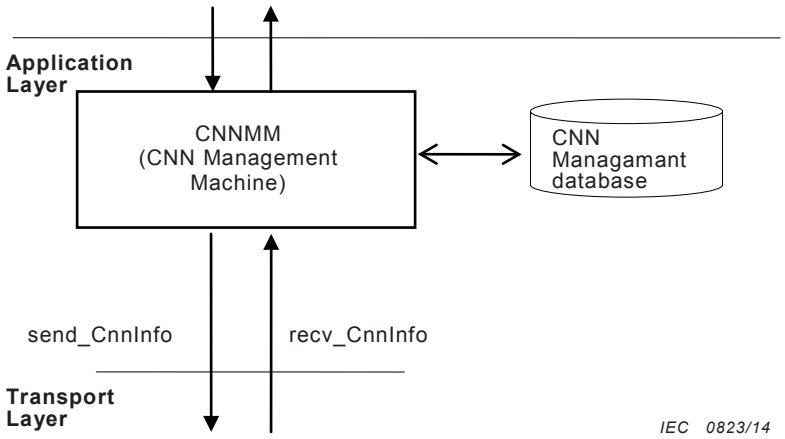


Figure D.20 – Architecture of CNN management

D.4.3 Individual CNN management information

After cyclic transmission starts over the sub-networks, each CNN shall send its individual CNN management information to the sub-networks by cyclic transmission mechanism with CNN management protocol, so that all CNNs can obtain all the individual CNN management information of other CNNs.

Individual CNN management information is contained in service data unit of UDP packet. Transmission frequency of individual CNN management information with priority as same as PD data class should be restricted to less than that for PD in order to keep bandwidth for real time control data.

Data format of the individual CNN management information is shown in Table D.32, and the parameters in Table D.33.

Table D.32 – Format of individual CNN management information

Bit->	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0	CateVer															
2	ServiceDataSize															
4	reserved															
6	reserved												null		ConnectionSts	
8	Null				CnnSts				null							
10 12	BypassedCnnDetect															
14 16	SubsCnnExec															
18	Null				ConnectionStsOth (*)				null						CnnStsOth (*)	
20 22	BypassedCnnDetectOth (*)															
24 26	SubsCnnExecOth (*)															
28	CnnHltyCountOth (*)												null			
30	CnnIpAddr3Oth (*)												CnnIpAddr4Oth (*)			
32	reserved												ForcLinkOffSts			
34	UpDwHead												reserved			
36 132	reserved (96 octests)															
132	CnnHealthyCount												null			
134	CnnNr															
136	SubsReqFlag1												SubsDstCnnNr1			
138	SubsSrcCnnNr1												reserved			
140 142	SubsCnnExecNr1															
144	SubsReqFlag2												SubsDstCnnNr2			
146	SubsSrcCnnNr2												reserved			
148 150	SubsCnnExecNr2															
152	reserved												null			
154 200	reserved (48 octets)															

(*) Parameters which have suffixed names with Oth are used for ladder topology, the fields for these parameters remain reserved if the network is not ladder topology.

Table D.33 – Description of parameters for individual CNN management information

Parameter	Type	Description
CateVer	UNSIGNED16	Category and version of transmission data; MSB octet indicates CNN Management Information: ‘10’H, LSB octet indicates the version of the format starting from: ‘00’H.
ServiceDataSize	UNSIGNED16	Size of service data
ConnectionSts	Type_Connection_Status	Connection status of CNN
CnnSts	UNSIGNED4	CNN status ‘0100’B: off line ‘0010’B: standby ‘0001’B: on line other : n/a
BypassedCnnDetect	Type_CNN_Flags	Bypassed CNN detection flags, for each entry; ‘1’: bypass detected, ‘0’: none
SubsCnnExec	Type_CNN_Flags	Flags for CNNs for which the substitute transmission are executed by other CNNs ‘1’:executed, ‘0’: none
ConnectionStsOth	BITSET4	Connection status of CNN in the other sub-network in ladder topology cn_u_oth(0): up link port (‘0’:normal, ‘1’:abnormal) cn_d_oth(1): down link port (‘0’:normal, ‘1’:abnormal) cn_l_oth (2): local port for the other sub-network (‘0’:normal, ‘1’:abnormal) reserved (3): n/a
CnnStsOth	UNSIGNED4	CNN status of CNN in the other sub-network in ladder topology ‘0100’B: off line ‘0010’B: standby ‘0001’B: on line Other : n/a
BypassedCnnDetectOth	Type_CNN_Flags	Flags for CNNs which are detected to be bypassed in the other sub-network in ladder topology 1st 16 bits: (MSB) CNN 15 – CNN 1 (‘1’: bypass detected, ‘0’: none) 2nd 16 bits: CNN 31 – (LSB) CNN 16 (‘1’: bypass detected, ‘0’: none)
SubsCnnExecOth	Type_CNN_Flags	Flags for CNNs for which the substitute transmission are executed by other CNNs on the other sub-network in ladder topology ‘1’:executed, ‘0’: none
CnnHltyCountOth	UNSIGNED8	CNN healthy count of CNN in the other sub-network in ladder topology (modulo 256)
CnnIpAddrOth	Type_Ip_Addr_3_4	The 3rd and the 4th octets of IP address of CNN in the other sub-network in ladder topology (*1)
ForcLinkOffSts	BITSET8	Forced link off status of CNN not used (0)-(5): null ulp_f_off (6): up link port forced link off (‘1’: forced off, ‘0’: none) dlp_f_off (7): down link port forced link off (‘1’: forced off, ‘0’: none)
UpDwHead	UNSIGNED8	Up or down head flag of CNN placement (0: Intermediate, 1: Up head, 2: Down head, 3-255: n/a)
CnnHltyCount	UNSIGNED8	CNN healthy count (modulo 256)

Parameter	Type	Description
CnnNr	UNSIGNED8	CNN number (1 – 31: valid, 0 and 32 – 255: n/a)
SubsCnnFlag	UNSIGNED8	Substitute transmission request flag (0: none, 1: requested, 2 -255: n/a)
SubsDstCnnNr	UNSIGNED8	Substitute transmission destination CNN number (1 – 31: valid, 0 and 32 – 255: n/a)
SubsSrcCnnNr	UNSIGNED8	Substitute transmission source CNN number (1 – 31: valid, 0 and 32 – 255: n/a)
SubsCnnExecNr	Type_CNN_Flags	Flags for CNNs for which the substitute transmission are executed by other CNNs in the requested CNNs ‘1’:requested, ‘0’: none
NOTE IP address of CNN means the default IP address for the CNN management.		

Table D.34 – Type_Connection_Status

Type name	Type	Description
Type_Connection_Status	UNSIGNED4	Connection status of ports in CNN cn_u (0): up link port (‘0’:normal, ‘1’:abnormal) cn_d (1): down link port (‘0’:normal, ‘1’:abnormal) cn_l (2): local port for the other sub-network (‘0’:normal, ‘1’:abnormal) reserved (3): n/a

Table D.35 – Type_CNN_Flags

Bit->	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	-
2	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16

NOTE1 Number in each entry means corresponding CNN number.

NOTE2 “-“ means “not used”.

Table D.36 – Type_Ip_Addr_3_4

Type name	Type	Description
ip_ad_3_4	UNSINED16	The 3rd and the 4th octets of IP address of CNN (the least significant octets)

D.4.4 CNN management database

After more than one cycle time of the individual CNN management information has past, each CNN shall calculate a CNN management database in it with the individual CNN management information received from other CNNs. The contents of the database become identical among all CNNs on the network.

The parameters with flags in the CNN management database are calculated in logical ORed of the identical parts in all of the individual CNN management information. The parameters with numerical values are packed into one parameter for all CNNs.

Table D.37 lists parameters of the CNN management database.

Table D.37 – Parameters of CNN management database

Parameter	Type	Description
BypassedCnnDetectAll1	Type_CNN_Flags	Bypassed CNN detection flags of all CNNs in sub-network 1, for each entry; ‘1’: bypass detected, ‘0’: none
BypassedCnnDetectAll2 (*)	Type_CNN_Flags	Bypassed CNN detection flags of all CNNs in sub-network 2, for each entry; ‘1’: bypass detected, ‘0’: none
SubsCnnExecAll1	Type_CNN_Flags	Flags for CNNs for which substitute transmission are executed by other CNNs in sub-network 1; ‘1’:executed, ‘0’: none
SubsCnnExecAll2 (*)	Type_CNN_Flags	Flags for CNNs for which substitute transmission are executed by other CNNs in sub-network 2; ‘1’:executed, ‘0’: none
ConnectionStsAll1	Type_Connection_Status_All	Connection status flags of trunk links and local links for all CNNs in sub-network 1
ConnectionStsAll2 (*)	Type_Connection_Status_All	Connection status flags of trunk links and local links for all CNNs in sub-network 2
IpAddrAll1	Type_Ip_Addr_3_4_All	Individual IP addresses for all CNNs in sub-network 1
IpAddrAll2 (*)	Type_Ip_Addr_3_4_All	Individual IP addresses for all CNNs in sub-network 2
OnlStsAll1	Type_CNN_Flags	On-line status flags for all CNNs in sub-network 1; ‘1’: On-line, ‘0’: None
OnlStsAll2 (*)	Type_CNN_Flags	On-line status flags for all CNNs in sub-network 2; ‘1’: On-line, ‘0’: None
StbyStsAll1	Type_CNN_Flags	Standby status flags for all CNNs in sub-network 1; ‘1’:Standby, ‘0’: None
StbyStsAll2 (*)	Type_CNN_Flags	Standby status flags for all CNNs in sub-network 2; ‘1’:Standby, ‘0’: None
HltyCountAll1	Type_Healthy_Count_All	Healthy counts for all CNNs in sub-network 1
HltyCountAll2 (*)	Type_Healthy_Count_All	Healthy counts for all CNNs in sub-network 2
(*) If the network topology is not ladder topology, parameters for the sub-network 2 are not used.		

Table D.38 – Type_Connection_Status_All

Bit->	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
	ARRAY [32] Type_Connection_Status															
0	CNN 3				CNN 2				CNN 1				Not used			
2	CNN 7				CNN 6				CNN 5				CNN 4			
	---				---				---				---			
14	CNN 31				CNN 30				CNN 29				CNN 28			

NOTE In case that no corresponding CNN exits, content of the entry is null.

Table D.39 – Type_Ip_ Addr_3_4_All

Bit->	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
	ARRAY [32] Type_Ip_Addr_3_4															
0	Not used															
2	CNN 1															

62	CNN 31															

NOTE In case that no corresponding CNN exits, content of the entry is null.

Table D.40 – Type_Healthy_Count_All

Bit->	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
	ARRAY [32] UNSIGNED8															
0	CNN 1								Not used							
2	CNN 3								CNN 2							

30	CNN 31								CNN 30							

NOTE In case that no corresponding CNN exits, content of the entry is null.

D.4.5 Primitives for CNN management protocol

CNN management uses the primitives to the lower protocol layer listed in Table D.41.

Table D.41 – Primitives to the lower protocol layer for CNN management

Primitives	Description
send_CnnInfo	Send CNN management information to the transport layer
recv_CnnInfo	Receive CNN management information from the transport layer

D.4.6 Parameters for CNN management protocol

The parameters for CNN management are listed in Table D.42, which are used in D.4.8.

Table D.42 – Parameters for CNN management

Parameters	Type	Description
Topology	ENUM2	Network topology; LINEAR (linear topology) or LADDER (ladder topology)
CnnMode	ENUM2	A mode of the CNN; UpperMost (Uppermost CNN mode), LowerMost (Lowermost CNN mode), InterMediate (Intermediate CNN mode) or Standalone (Stand alone CNN mode).
MyCnn	UNSIGNED5	Own CNN number of the CNN; [1..31]
MaxCnn	UNSIGNED5	The maximum CNN number of the network
TokenCnn	UNSIGNED5	The number of the CNN which is included in the Token command frame received from the upper CNN.
StatTpu	ENUM1	Status of the trunk port for up link; Normal: when link on state of the port (linkTPU == True) lasts more than the limit of the timer TRTPU, Failure: when link off state of the port (linkTPU == False) lasts more than the limit of the timer TFTPU.
StatTpd	ENUM1	Status of the trunk port for down link; Normal: when link on state of the port (linkTPD == True) lasts more than the limit of the timer TRTPD, Failure: when link off state of the port (linkTPD == False) lasts more than the limit of the timer TFTPD.
StatLpr	ENUM1	Status of the local port for the other sub-network; Normal: when link on state of the port lasts more than the limit of the timer TRLPR, Failure: when link off state of the local-link lasts more than the limit of the timer TFLPR.
ForceOffTpu	BOOLEAN1	Status of TPU forced off True: Forced off False: Not forced off
ForceOffTpd	BOOLEAN1	Status of TPD forced off True: Forced off False: Not forced off
SubsCnnFlags	Type_CNN_Flags	Flags for CNNs substituted by this CNN. A bit position in SubsCnnFlags corresponds to the one of CNNs: “1”: the CNN is substituted by this CNN, “0”: the CNN is not substituted by this CNN.
TempSubsCnnFlags	Type_CNN_Flags	Temporal flags for CNNs substituted by this CNN, which is stored temporally to send afterwards in the subusXmit() procedure. The content and the form of TempSubsCnnFlags are the same as SubsCnnFlags.

D.4.7 Timers for CNN management protocol

The timers for the CNN management are listed in Table D.43.

Table D.43 – Timers for CNN management

Timers	Description
TNMS	Timer for sending CNN management information periodically; default value is 100 ms.
TFTPU	Timer for the trunk port for up link to be failed when expired; default value is 30 ms.
TRTPU	Timer for the trunk port for up link to be recovered when expired; default value is 0 ms.
TFTPD	Timer for the trunk port for down link to be failed when expired; default value is 30 ms.
TRTPD	Timer for the trunk port for down link to be recovered when expired; default value is 0 ms.
TFLPR	Timer for the local port for the other sub-network to be failed when expired; default value is 30 ms.
TRLPR	Timer for the local port for the other sub-network to be recovered when expired; default value is 0 ms.

D.4.8 Procedures for CNN management protocol

D.4.8.1 Procedures and functions

The procedures for CNN management are listed in Table D.44 and the related functions are described in Table D.45 and Table D.46.

Table D.44 – Procedures for CNN management

Procedures	Description
initNDB()	Initialize CNN management database. All data are cleared to 0.
buildCnnInfo(frame)	Build CNN management information frame for this CNN to send. Refer to Table D.32 for the frame format.
sourceCnn(frame)	Extract the CNN number from the frame designated in (frame).
startTimer(timer)	Start the timer designated in (timer). If the timer has already started, the timer is reset to restart.
updateNDB(cnn, value1, ...)	Update the value of variables enumerated in the area for the CNN designated in (cnn) in CNN management database in this CNN.
updateMyNDB(value1, ...)	Update the value of variables enumerated in the area of the MyCnn in CNN management database in this CNN.
genSubsXRqBNStat()	Generate the information for the request frame for substitute transmission. (SubsReqFlag1, SubsDstCnnNr1, SubsCnnExecNr1 and SubsSrcCnnNr1) Table D.45 shows functions for substitute transmission with the related activities which generate the frame by detecting CNN bypassed. (See NOTE.)
genSubsXRqTPStat(statTPU, statTPD)	Generate the information for the request frame for substitute transmission according to status of the trunk port in the CNN. (SubsReqFlag2, SUbsDstCnnNr2, SubsCnnExecNr2 and SubsSrcCnnNr2)Table D.46 shows functions for generating the request frame with the related activities when detecting trunk port failure. (See NOTE.)
subsXmit()	subsXmit() finds the CNN(s) which, because of bypassed or link failure, shall be substituted by this CNN by means of calculating the data in the individual CNN management information from CNN 1 to MaxCnn, and then executes periodical transmission of the PD. subsXmit() also finds the CNN(s) for which the substitute transmission shall be stopped because of no need to be substituted by this CNN any more. Start or termination of substitute transmission of the PD for the CNN(s) with using PD service in Application Layer is executed in the following steps.

Procedures	Description
	a) For the case of bypassed CNN(s), find the CNN(s) to be substituted by means of calculating logical OR of all SubsCnnExecNr1 with the condition of both SubsReqFlag1 equals “1” and SubsDstCnnNr1 equals MyCnn in all the individual CNN management information from CNN 1 to MaxCnn. b) For the case of link failures, find the CNN(s) to be substituted by means of calculating logical OR of all SubsCnnExecNr2 with the condition of both SubsReqFlag2 equals “1” and SubsDstCnnNr2 equals MyCnn in all the individual CNN management information from CNN 1 to MaxCnn. c) Because the CNN(s) for which both the logical OR of a) SubsCnnExecNr1 and b) SubsCnnExecNr2 in the above are “1” shall be substituted by this CNN, request to transmit the PD of the CNN(s) periodically by using the data in the traffic store for the other side sub-network. The result in this step is stored as TempSubsCnnFlags. d) Calculates exclusive OR of TempSubsCnnFlags, the result of c) in the above, and SubsCnnFlags, and then calculates logical AND of this result and SubsCnnFlags. Because the CNN(s) for which the corresponding bits are “1” in this result are the previous substitution CNN(s), the substitute transmission shall be stopped at this time. e) Request to stop transmitting the PD of the CNN(s) to which the original producer ED(s) belongs. In order to detect the condition to stop the substitute transmission by this CNN in the next time calling, save TempSubsCnnFlags, the result of c) in the above, as new SubsCnnFlags.
NOTE The CNN which executes substitute transmission is named as substitution CNN, while the CNN for which substitute transmission is executed by other CNN is named as substituted CNN.	

Table D.45 – Functions for substitution transmission by detecting bypassed CNN

Function name	Operations

genSubsXRqBNStat()	Calculate difference between TokenCnn and MyCnn.
	If the difference is greater than 1, then, since the previous CNN is bypassed, create the information for substitute transmission in the individual CNN management information of this CNN. (SubsReqFlag1, SubsDstCnnNr1, SubsSrcCnnNr1 and SubsCnnExecNr1)
	If the difference is 1, then, since no CNN is bypassed, clear the information for substitute transmission to 0.
	prevSubsDstCnnNr1 = SubsDstCnnNr1;
	prevSubsCnnExecNr1 = SubsCnnExecNr1;
	if ((MyCnn – TokenCnn) > 1) {
	// On detecting one or more bypassed CNN(s) in upward
	if (isOthCnnTPD(myCnn – 1) == Normal) {
	if (isOthCnnHealty(MyCnn, MaxCnn)) {
	SubsDstCnnNr1 = getMinCnnHealtyOthCnn(MyCnn, MaxCnn);
	SubsCnnExecNr1 = setBits(TokenCnn + 1, MyCnn – 1);
	} else if (isOthCnnHealty (1, TokenCnn)) {
	SubsDstCnnNr1 = getMaxCnnHealtyOthCnn(1, TokenCnn);
	SubsCnnExecNr1 = setBits(TokenCnn + 1, MyCnn – 1));
	} else {

Function name	Operations

	SubsDstCnnNr1 = 0; SubsCnnExecNr1 = 0;
	}
	else if (isOthCnnTPU(TokenCnn + 1) == Normal) {
	if (isOthCnnHealty (1, TokenCnn)) {
	SubsDstCnnNr1 = getMaxCnnHealtyOthCnn(1, TokenCnn);
	SubsCnnExecNr1 = setBits(TokenCnn + 1, MyCnn – 1);
	} else {
	SubsDstCnnNr1 = 0; SubsCnnExecNr1 = 0;
	}
	} else {
	SubsDstCnnNr1 = 0; SubsCnnExecNr1 = 0;
	}
	} else {
	SubsDstCnnNr1 = 0; SubsCnnExecNr1 = 0;
	}
	if (SubsDstCnnNr1 != 0) {
	SubsReqFlag1 = 1; SubsSrcCnnNr1 = MyCnn;
	} else {
	SubsReqFlag1 = 0; SubsSrcCnnNr1 = 0;
	}
	if (prevSubsDstNr1 != SubsDstNr1 || prevSubsCnnExecNr1 != SubsCnnExecNr1)
	return TRUE;
	return FALSE;

isOthCnnTPD(n)	Return the status of the down link of the CNN designated with (n) which is paired on the other side sub-network; Normal state: when the CNN is normal, or in case of the lowermost CNN force state is returned, Failure state: when the CNN in failure.
isOthCnnTPU(n)	Return the status of the up link of the CNN designated with (n) which is paired on the other side sub-network; Normal state: when the CNN is normal, or in case of the lowermost CNN force state is returned, Failure state when the CNN in failure.
isOthCnnHealthy(n1, n2)	If local ports of CNNs designated with from n1 to n2 in the same sub-network are normal and the corresponding CNNs in the other side sub-network are healthy, then return normal state. Else, return failure state.
getMinCnnHealthyOthCnn (n1, n2)	If local ports of CNNs designated with from n1 to n2 on the same sub-network are normal and the corresponding CNNs on the other side sub-network are healthy, then return the least CNN number.
getMaxCnnHealthyOthCnn (n1, n2)	If local ports of CNNs designated with from n1 to n2 on the same sub-network are normal and the corresponding CNNs on the other side sub-network are healthy, then return the most CNN number
setBits(n1, n2);	Set “1” for bits from 2^(n1) to 2^(n2).

Table D.46 – Functions for substitution transmission by detecting link failure

Function name	Operations

genSubsXRqTPStat(statTPU, statTPD)	Generate the information for the request frame for substitute transmission according to status of the trunk ports of TPU and TPD in the individual CNN management information in the CNN. (SubsReqFlag2, SUbsDstCnnNr2, SubsCnnExecNr2 and SubsSrcCnnNr2)
	if ((StatTpu == Failure) && (StatTpd == Normal)) {
	// in case of failure at trunk port for up link
	if (isOthCnnHealty (MyCnn, MaxCnn)) {
	SubsDstCnnNr2 = getMinCnnHealtyOthCnn(MyCnn, MaxCnn);
	SubsCnnExecNr2 = setBits(1, MyCnn – 1);
	} else
	SubsDstCnnNr2 = 0;
	} else if ((StatTpu == Normal) && (StatTpd == Failure)) {
	// in case of failure at trunk port for down link
	if (isOthCnnHealthy (1, MyCnn-1)) {
	SubsDstCnnNr2 = getMaxCnnHealthyOthCnn(1, MyCnn-1);
	SubsCnnExecNr2 = setBits(MyCnn + 1, MaxCnn);
	} else
	SubsDstCnnNr2 = 0;
	} else
	SubsDstCnnNr2 = 0;
	if (SubsDstCnnNr2 != 0) {
	SubsReqFlag2 = 1; SubsSrcCnnNr2 = MyCnn;
	} else
	SubsReqFlag2 = 0; SubsSrcCnnNr2 = 0;

D.4.8.2 Events

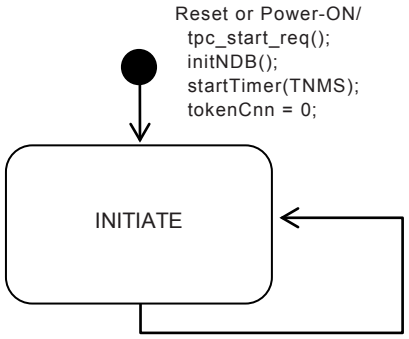
Events for CNN management are listed in Table D.47.

Table D.47 – Events for CNN management

Events	Description
Reset or Power ON	Hardware reset or power on.
receivedToken(Cnn)	Receive token with CNN number which sent the token.
changeTPUD (statTPU, statTPD)	Change occurs in the status of trunk port for up link or trunk port for down link, which indicates failure or normal.
changeLPR(statLPR)	Change occurs in the status of local port for the other sub-network, which indicates failure or normal.
expiredTimer(timer)	Expires the timer started by startTimer activity.

D.4.9 Operation of CNN management machine

Figure D.21 shows the state diagram for CNN management machine and the state transition table is described in Table D.48.




```
changeTPUD(statTPU, statTPD) /
  updateMyNDB(statTPU, statTPD);
  if (Topology == LADDER) {
    genSubsXRqTPStat(statTPU, statTPD);
  }
  buildCnnInfo(cnnInfo);
  send_CnnInfo(cnnInfo);
  subsXmit();

receivedToken(cnn)[ Topology == LADDER]/
  tokenCnn = cnn;
  if (genSubsXRqBNStat() == TRUE) {
    buildNodeInfo(cnnInfo);
    send_NodeInfo(cnnInfo);
  }
  subsXmit();

recv_CnnInfo(cnnInfo)/
  cnn = sourceCnn(cnnInfo);
  updateNDB(cnn, cnnInfo);
  subsXmit();

changeLPR(statLPR)/
  updateMyNDB(statLPR);
  buildCnnInfo(cnnInfo);
  send_CnnInfo(cnnInfo);

expiredTimer(TNMS)/
  updateMyNDB(healthyCounter);
  buildCnnInfo(cnnInfo);
  send_CnnInfo(cnnInfo);
  startTimer(TNMS);
```

IEC 0824/14

Figure D.21 – State diagram for CNNMM

Table D.48 – State transition table for CNNMM

Current state	Event[condition]	Actions	Next State

Initial state	Reset or Power ON	// Reset or power on
		tpc_start_req();
		initNDB();
		startTimer(TNMS);
		tokenCnn = 0;
			INITIATE

INITIATE	changeTPUD(statTPU, statTPD)	// Change in link status of trunk ports
		updateMyNDB(statTPU, statTPD);
		if (topology == LADDER) {
		genSubsXRqTPStat(statTPU, statTPD);
		}
		buildCnnInfo(cnnInfo);
		send_CnnInfo(cnnInfo);
		subsXmit();
			INITIATE

INITIATE	receivedToken(Cnn)
	[Topology == LADDER]
		// Receive token
		tokenCnn = cnn;
		if (genSubsXRqBNStat() == TRUE) {
		buildCnnInfo(cnnInfo);
		send_CnnInfo(cnnInfo);
		}
		subsXmit();
			INITIATE

INITIATE	recv_CnnInfo(CnnInfo)	// Receive individual CNN management information from other CNN
		cnn = sourceCnn(cnnInfo);
		updateNDB(cnn, cnnInfo);
		subsXmit();
			INITIATE

INITIATE	changeLPR(statLPR)	// Change in link state of local port for the other sub-network
		updateMyNDB(statLPR);
		buildCnnInfo(cnnInfo);
		send_CnnInfo(cnnInfo);
			INITIATE

INITIATE	expiredTimer(TNMS)	// TNMS timer expire to send individual CNN management information periodically.
		updateMyNDB(healthyCounter);
		buildCnnInfo(cnnInfo);
		send_CnnInfo(cnnInfo);
		startTimer(TNMS);
			INITIATE

D.4.10 Port number assignment for CNN management protocol

For interoperable data communication, the port assignments in Transport Layer for CNN management protocol listed in Table D.49 should be used as default, which shall not be duplicated with the port numbers for PD, MD or other application protocols:

Table D.49 – Default port number for CNN management protocol

Protocol	Destination Port	Source Port
CNN Management Data (UDP)	49 154	49 154
NOTE Using different port number is allowed for project specific purposes.		

D.5 Failure cases in ladder topology

D.5.1 General

This clause describes various failure cases in the ladder topology, in which re-configuration of the transmission paths for PD is performed by the substitute transmission function.

D.5.2 Failure cases

Hereinafter, various failure cases are shown with examples of five pair CNN sub-networks in the ladder topology.

NOTE In figures in this clause, henceforth, the examples assume five pair CNN sub-network in the ladder topology. Not all End Devices attached to the paired CNNs in dual homing are illustrated for simplification. The thick arrows mean the data frames transmitted over the sub-network 1, and thin arrows those over the sub-network 2. The CNN indicated by shading box means that the CNN executes the substitute transmission. The CNN numbers are not actual but abstract for explanation.

a) Normal operation

In Figure D.22, the data originated from an attached End Device is transmitted to both the sub-network 1 and 2 simultaneously, and also delivered to the CNNs in the other side sub-network mutually through the local links at each of the CNNs.

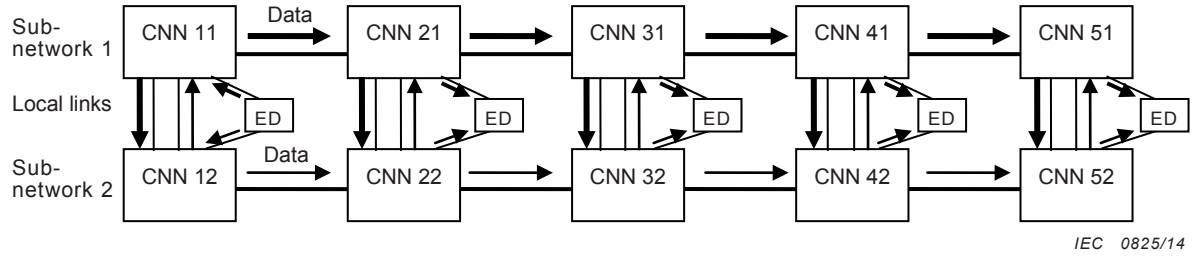


Figure D.22 – Normal configuration of transmission paths in ladder topology

b) A single link failure in a sub-network

In Figure D.23, in case of a link failure in the sub-network 1, CNN 41 utilizes the data received from CNN 12, CNN 22 and CNN 32 via the local link between CNN 42, to re-transmit the data to the one intact part of the sub-network 1, in which the data are the same that should be received from CNN 11, 21 and 31 respectively.

On the other hand, CNN 31 utilizes the data received from CNN 42 and CNN 52 via the local link between CNN 32, to re-transmit the data to the other intact part of the sub-network 1, in which the data are the same that should be received from CNN 41 and CNN 51 respectively.

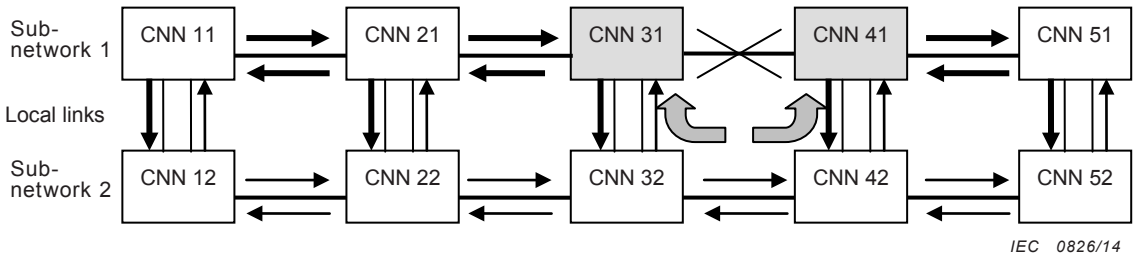


Figure D.23 – Re-configuration of transmission paths with a single link failure in a sub-network

c) A single CNN failure in a sub-network

In Figure D.24, in case of a CNN failure in the sub-network 1, the link of the CNN is bypassed with the relay circuit. CNN 32 works for backup of the failed CNN 31.

CNN 41 utilizes the data received from CNN 32 at the local link via CNN 42, which is the same that should be received from CNN 31, to re-transmit the data to the sub-network 1 as the substitute transmission.

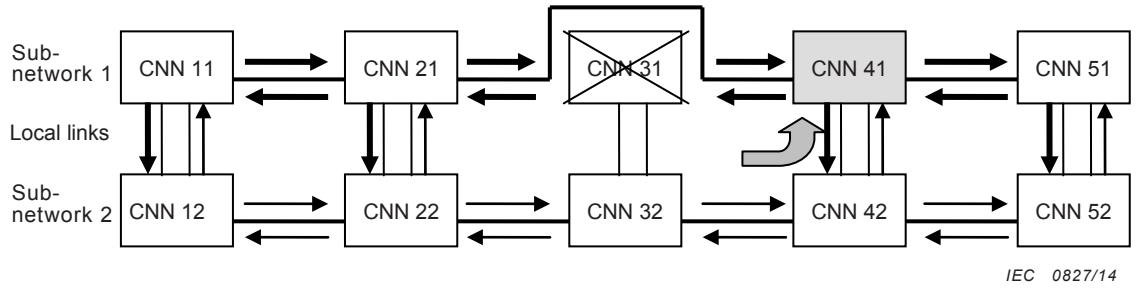


Figure D.24 – Re-configuration of transmission paths with a single CNN failure in a sub-network

d) Double failures of links in a sub-network

In Figure D.25, in case of double failures of different links in the sub-network 1;

CNN 21 executes the substitute transmission of CNN 31, 41 and 51,

CNN 31 executes the substitute transmission of CNN 11 and 21,

CNN 41 executes the substitute transmission of CNN 51,

CNN 51 executes the substitute transmission of CNN 11, 21, 31 and 41.

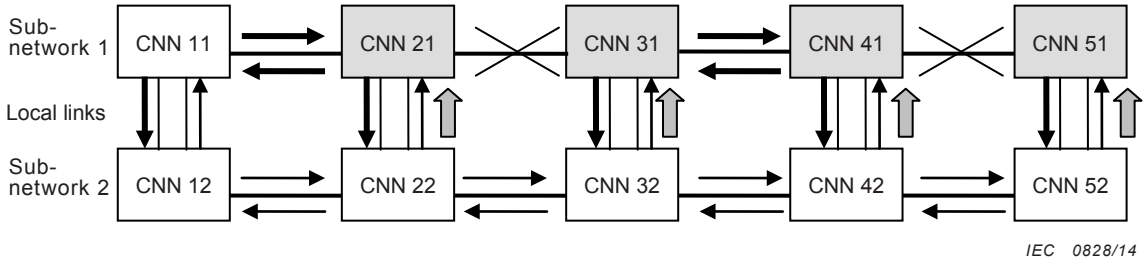


Figure D.25 – Re-configuration of transmission paths with double failures of links in a sub-network

e) Double failures of different links over both sub-networks

In Figure D.26, in case of double failures of different links over both sub-network 1 and sub-network 2;

CNN 21 executes the substitute transmission of CNN 31, 41 and 51,

CNN 31 executes the substitute transmission of CNN 11 and 21,

CNN 32 executes the substitute transmission of CNN 42 and 52,

CNN 42 executes the substitute transmission of CNN 12, 22 and 32.

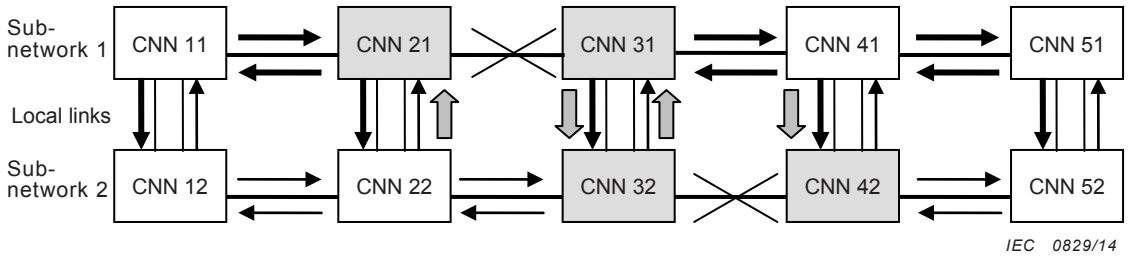


Figure D.26 – Re-configuration of transmission paths with double failures of links over both sub-networks

f) Double CNN failures over both sub-networks

In Figure D.27, in case of a CNN failure in the sub-network 1 and another failure of the CNN in the sub-network 2;

CNN 31 executes the substitute transmission of CNN 21 in the sub-network 1, by using the data from CNN 22,

CNN 52 executes the substitute transmission of CNN 42 in the sub-network 2, by using the data from CNN 41.

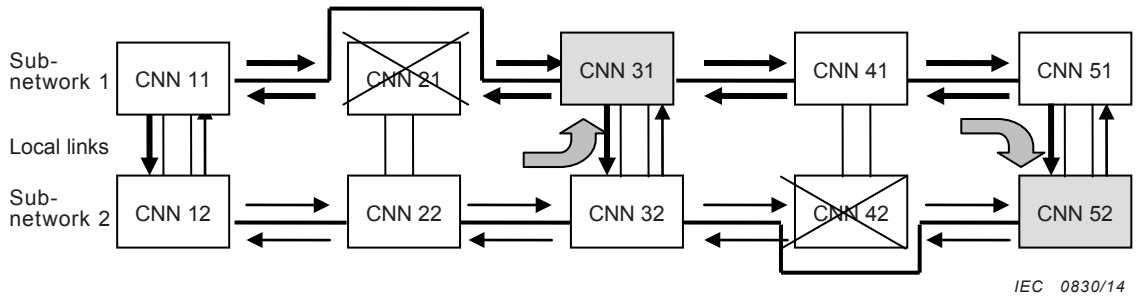


Figure D.27 – Re-configuration of transmission paths with double failures of CNNs over both sub-networks

g) Double failures of a CNN and a link over both sub-networks

In Figure D.28, in case of a CNN failure in the sub-network 1 and another failure of a link in the sub-network 2;

CNN 31 executes the substitute transmission of CNN 21 in the sub-network 1, by using the data from CNN 22,

CNN 32 executes the substitute transmission of CNN 42 and 52 in the sub-network 2, by using the data from CNN 41 and 51,

CNN 42 executes the substitute transmission of CNN 12, 22 and 32 in the sub-network 2, by using the data from CNN 11, 22 and 31.

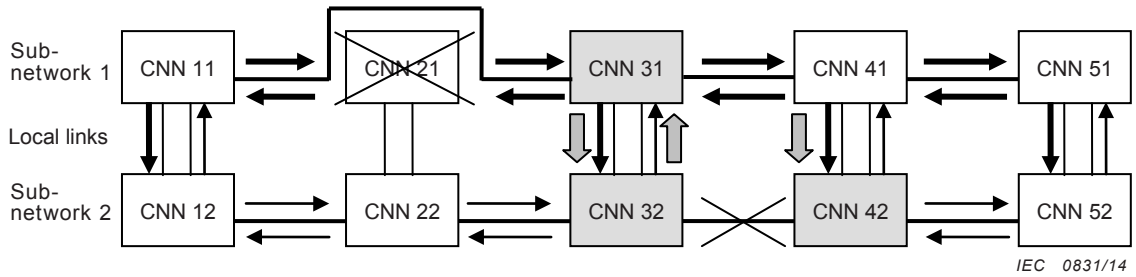


Figure D.28 – Re-configuration of transmission paths with double failures of a link and a CNN over both sub-networks

h) Double failures of a CNN and a link over both sub-networks

In Figure D.29, in case of a CNN failure in the sub-network 1 and another failure of the a link in the sub-network 2;

CNN 32 executes the substitute transmission of CNN 22 in the sub-network 2, by using the data from CNN 21,

CNN 41 executes the substitute transmission of CNN 51 in the sub-network 1, by using the data from CNN 52,

CNN 51 executes the substitute transmission of CNN 11, 21, 31 and 41 in the sub-network 1, by using the data from CNN 12, 21, 32 and 42.

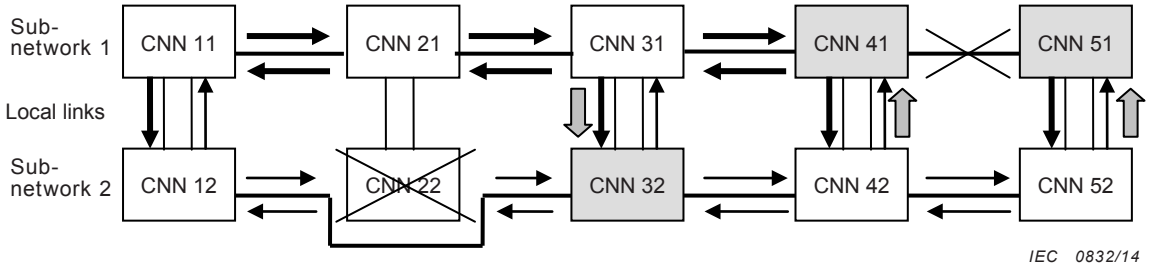


Figure D.29 – Re-configuration of transmission paths with double failures of a link and a CNN over both sub-networks

D.5.3 Restore of the network

In case that the failures of links or CNNs are restored, when CNNs at both sides of the failure points find the points to be normal condition, they remove the control of the detour route from the failure points, then re-start normal operation in both of the sub-networks.

Bibliography

IETF RFC 768, *User Datagram Protocol,*
available at <http://www.ietf.org/rfc/rfc768.txt>

IETF RFC 791, *Internet Protocol,*
available at <http://www.ietf.org/rfc/rfc769.txt>

IETF RFC 792, *Internet Control Message Protocol,*
available at <http://www.ietf.org/rfc/rfc792.txt>

IETF RFC 793, *Transmission Control Protocol,*
available at <http://www.ietf.org/rfc/rfc793.txt>

IETF RFC 826, An *Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware,*
available at <http://www.ietf.org/rfc/rfc826.txt>

IETF RFC 854, *TELNET Protocol specification, available at <http://www.ietf.org/rfc/rfc854.txt>*

IETF RFC 959, *File Transfer Protocol (FTP), available at <http://www.ietf.org/rfc/rfc959.txt>*

IETF RFC 1034, *Domain Names – Concepts and Facilities,*
available at <http://www.ietf.org/rfc/rfc1034.txt>

IETF RFC 1035, *Domain Names – Implementation and Specification,*
available at <http://www.ietf.org/rfc/rfc1035.txt>

IETF RFC 1112, *Host Extensions for IP Multicasting,*
available at <http://www.ietf.org/rfc/rfc1112.txt>

IETF RFC 1122, *Requirements for Internet Hosts -- Communication Layers,*
available at <http://www.ietf.org/rfc/rfc1122.txt>

IETF RFC 1166, *Internet Numbers,*
available at <http://www.ietf.org/rfc/rfc1166.txt>

IETF RFC 1213, *Management Information Base for Network Management of TCP/IP-based internets: MIB-II,*
available at <http://www.ietf.org/rfc/rfc1213.txt>

IETF RFC 1305, *Network Time Protocol (Version 3) Specification, Implementation and Analysis*,
available at <http://www.ietf.org/rfc/rfc1305.txt>

IETF RFC 1350, *THE TFTP Protocol (REVISION 2),*

available at <http://www.ietf.org/rfc/rfc1350.txt>

IETF RFC 1361, *Simple Network Time Protocol (SNTP),*
available at <http://www.ietf.org/rfc/rfc1361.txt>

IETF RFC 1901, *Introduction to Community-based SNMPv2*
available at <http://www.ietf.org/rfc/rfc1901.txt>

IETF RFC 1905, *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2),*
available at <http://www.ietf.org/rfc/rfc1905.txt>

IETF RFC 1906, *Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2),*
available at <http://www.ietf.org/rfc/rfc1906.txt>

IETF RFC 1918, *Address Allocation for Private Internets,*
available at <http://www.ietf.org/rfc/rfc1918.txt>

IETF RFC 2131, *Dynamic Host Configuration Protocol,*
available at <http://www.ietf.org/rfc/rfc2131.txt>

IETF RFC 2132, *DHCP Options and BOOTP Vendor Extensions,*
available at <http://www.ietf.org/rfc/rfc2132.txt>

IETF RFC 2236, *Internet Group Management Protocol, Version 2,*
available at <http://www.ietf.org/rfc/rfc2236.txt>

IETF RFC 2365, *Administratively Scoped IP Multicast,*
available at <http://www.ietf.org/rfc/rfc2365.txt>

IETF RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers,*
available at <http://www.ietf.org/rfc/rfc2474.txt>

IETF RFC 2544, *Benchmarking Methodology for Network Interconnect Devices,*
available at <http://www.ietf.org/rfc/rfc2544.txt>

IETF RFC 2616, *Hypertext Transfer Protocol -- HTTP/1.1,*

available at <http://www.ietf.org/rfc/rfc2616.txt>

IETF RFC 3022, *Traditional IP Network Address Translator (Traditional NAT),*
available at <http://www.ietf.org/rfc/rfc3022.txt>

IETF RFC 3046, *DHCP Relay Agent Information Option,*
available at <http://www.ietf.org/rfc/rfc3046.txt>

IETF RFC 3203, *DHCP reconfigure extension,*

available at <http://www.ietf.org/rfc/rfc3203.txt>

IETF RFC 3376, *Internet Group Management Protocol, Version 3,*
available at <http://www.ietf.org/rfc/rfc3376.txt>

IETF RFC 3768, *Virtual Router Redundancy Protocol (VRRP),*
available at <http://www.ietf.org/rfc/rfc3768.txt>

IETF RFC 4251, *The Secure Shell (SSH) Protocol Architecture,*

available at <http://www.ietf.org/rfc/rfc4251.txt>

IETF RFC 4541, *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches, available at <http://www.ietf.org/rfc/rfc4541.txt>*

———————

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™