DIN EN 13757-5

ICS 33.200; 35.100.10; 35.100.20

Kommunikationssysteme für Zähler und deren Fernablesung – Teil 5: Weitervermittlung; Englische Fassung EN 13757-5:2008

Communication systems for meters and remote reading of meters – Part 5: Wireless relaying; English version EN 13757-5:2008

Systèmes de communication et de télérelevé des compteurs – Partie 5: Relais sans fil; Version anglaise EN 13757-5:2008

Gesamtumfang 76 Seiten

Normenausschuss Heiz- und Raumlufttechnik (NHRS) im DIN
DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE

Nationales Vorwort

Dieses Dokument (EN 13757-5:2008) wurde vom Technischen Komitee CEN/TC 294 „Kommunikationssysteme für Zähler und deren Fernablesung“ erarbeitet, dessen Sekretariat vom DS (Dänemark) gehalten wird.

Das zuständige deutsche Gremium ist NA 041-03-66 AA im Normenausschuss Heiz- und Raumlufttechnik (NHRS).

Das Dokument (EN 13757-5:2008) wurde unverändert vom englischen Originaltext übernommen. Der Normenausschuss Heiz- und Raumlufttechnik (NHRS) war für das DIN Deutsches Institut e.V. an der Erstellung dieser Norm beteiligt. Da davon auszugehen ist, dass die Fachleute der Kommunikationstechnik sich bereits mit der englischen Urfassung befasst haben, wurde von einer Übersetzung ins Deutsche abgesehen. Nach dem DIN Präsidiumsbeschluss 13/1983 ist auf dem Gebiet der Informatik die Veröffentlichung in Englisch zulässig, insbesondere wenn dadurch Fehler bei der Übersetzung bzw. dem Verständnis der Norm vermieden werden können.

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 13757-5

October 2008

ICS 33.200; 35.100.10; 35.100.20

English Version

Communication systems for meters and remote reading of meters — Part 5: Wireless relaying

Systèmes de communication et de télérelevé des compteurs — Partie 5: Relais sans fil

Kommunikationssysteme für Zähler und deren Fernablesung — Teil 5: Weitervermittlung

This European Standard was approved by CEN on 16 August 2008.

CEN 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 Management Centre or to any CEN 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 CEN member into its own language and notified to the CEN Management Centre has the same status as the official versions.

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

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: rue de Stassart, 36 B-1050 Brussels

Ref. No. EN 13757-5:2008: E

Contents

Page

Foreword

This document (EN 13757-5) has been prepared by Technical Committee CEN/TC 294 “Communication systems for meters and remote reading of meters”, the secretariat of which is held by DS.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by April 2009, and conflicting national standards shall be withdrawn at the latest by April 2009.

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

EN 13757 consists of the following parts, under the general title *Communication systems for meters and remote reading of meters:*

— *Part 1: Data exchange*

— *Part 2: Physical and link layer*

— *Part 3: Dedicated application layer*

— *Part 4: Wireless meter readout (Radio meter reading for operation in the 868 MHz to 870 MHz SRD band)*

— *Part 5: Wireless relaying*

— *Part 6: Local Bus*

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

1 Scope

This standard defines the requirements for the protocols to use when performing relaying in wireless meter readout networks. This document is an extension to Part 4 of EN 13757, *Wireless meter readout (Radio meter reading for operation in the 868 MHz to 870 MHz SRD band)*. It supports the routing of mode R2, but the routing of mode S and T is not supported.

The main use of this standard is to support routed wireless networks for the readout of meters.

NOTE Electricity meters are not covered by this standard, as the standardisation of remote readout of electricity meters is a task for IEC/CENELEC.

2 Normative references

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

EN 13757-1:2002, *Communication system for meters and remote reading of meters – Part 1: Data exchange*

EN 13757-3:2004, *Communication systems for and remote reading of meters – Part 3: Dedicated application layer*

EN 13757-4:2005, *Communication systems for meters and remote reading of meters – Part 4: Wireless meter readout (Radio meter readout for operation in the 868 MHz to 870 MHz SRD band)*

EN 60870-5-1:1993, *Telecontrol equipment and systems – Part 5: Transmission protocols – Section 1: Transmission frame formats (IEC 60870-5-1:1990)*

EN 60870-5-2:1993, *Telecontrol equipment and systems – Part 5: Transmission protocols – Section 2: Link transmission procedures (IEC 60870-5-2:1992)*

EN 62054-21, *Electricity metering (a.c.) – Tariff and load control – Part 21: Particular requirements for time switches (IEC 62054-21:2004)*

ETSI EN 300 220-1:2000, *ElectroMagnetic Compatibility and Radio Spectrum Matters (ERM); Short Range Devices (SRD); Radio equipment to be used in the 25 MHz to 1 000 MHz frequency range with power levels ranging up to 500 mW; Part 1: Technical characteristics and test methods*

ETSI EN 300 220-2:2000, *ElectroMagnetic Compatibility and Radio Spectrum Matters (ERM); Short Range Devices (SRD); Radio equipment to be used in the 25 MHz to 1 000 MHz frequency range with power levels ranging up to 500 mW; Part 2: Supplementary parameters not intended for conformity purposes*

ETSI EN 301 489-1:2008, *Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements*

ETSI EN 301 489-3:2002, *Electromagnetic compatibility and Radio spectrum Matters (ERM);ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 3: Specific conditions for Short-Range Devices (SRD) operating on frequencies between 9 kHz and 40 GHz*

RFC 1662 July 1994, *HDLC-like Framing, Appendix C. Fast Frame Check Sequence (FCS) Implementation*

3 Terms and definitions

For the purpose of this European Standard, the following terms and definitions apply.

3.1
primary station
network node that controls all of the data exchange in a simple network with one central node, unbalanced data transfer and multiple remote nodes

NOTE All data transfer will (normally) be controlled by the primary station. A data collecting unit will be a primary station.

3.2
secondary station
node in a hierarchical network that is able to receive commands and requests from a central node, the primary station, and to send a response back to the central node

NOTE A meter will be a secondary station.

3.3
upstream
transmission of data in the direction from the meter to the data collecting unit

3.4
downstream
transmission of data in the direction from the data collecting unit to the meter

3.5
relaying
forwarding of information from one logical network to another

NOTE A function performed by an intermediate node connected to two logical networks.

3.6
gateway
intermediate node in a data communications network, connected to two or more logical networks, where the protocols or modes used on the logical networks are different

3.7
router
intermediate node in a data communications network, connected to two or more logical networks with identical protocols and modes

3.8
node
unit in a network that is able to send and receive data

3.9
end node
meter or data collecting unit

3.10
intermediate node
node in a network sitting in between a data collecting unit and a meter

3.11
hop
transfer of a set of data from one node to an adjacent node, as one of the steps in the transfer of data between end nodes

3.12
frame
set of user data encapsulated by a header and optionally a trailer

NOTE For an EN 60870-5-1 based protocol, this will be a start character followed by up to 16 blocks of data.

3.13
block
sub-element of a frame

NOTE For an EN 60870-5-1 based protocol, this will be up to 16 bytes of user data completed by a CRC check.

4 Explanation

4.1 General

This clause is an explanatory clause. The specific requirements are to be found in the latter clauses of this European Standard.

4.2 Introduction

The availability of low cost radio modules has made it feasible to use radio communication for the readout of meter data. Many meters are battery operated and have a very strict power budget and regulatory requirements are imposed as well. This limits the transmitting power levels and thereby the useful distance between transmitters and receivers. The use of reinforced concrete, conductive surface coatings and placement of meters in the basement of the buildings aggravates the problem of directly communicating between a data collecting unit and a meter. This limits the useful size radio networks unless relaying or forwarding is used. By letting some of the nodes forward or relay data, the effective size of the network can be increased. This makes the radio based networks a more cost effective solution.

A relaying or forwarding concept will still have a number of constraints. The cost of adding this capability to the meters must be low, since meters are cost sensitive high volume products. The limited energy and computing power available in the individual nodes, mandates a limited complexity of the software handling the communications protocol and the forwarding.

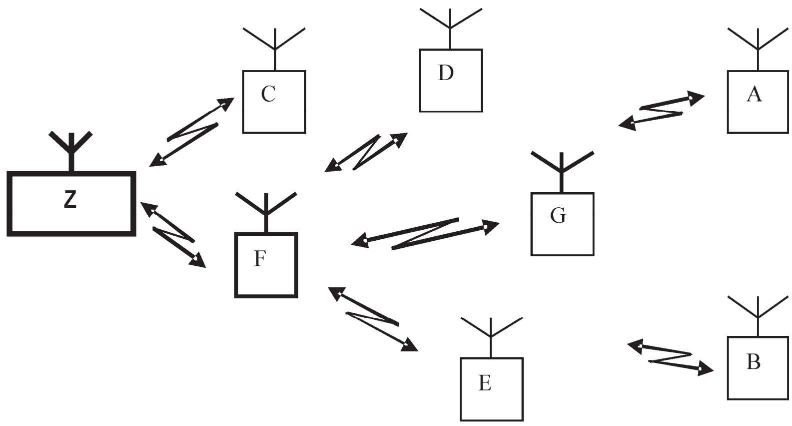
Operating and installation costs are important factors when planning for meter networks. The reconfiguration of the network when adding, replacing or removing meters must be automated to limit the operating cost.

The overhead due to relaying of data transmitted must be low to keep the transmission duty cycle within the limitations imposed by the authorities.

Radio networks for remote readout of meters are basically hierarchical networks. There is basically only one single data collecting node. All the meters send their data to this node, some directly, and some through forwarding nodes. There is basically no requirement for communication between meters as peer nodes.

4.3 Relaying

A radio network may have a structure like the one shown in Figure 1 below. The nodes A, B, C, D, E, F and G are simple meters. They all need to communicate with node Z, the data collecting unit/the primary station. In the current setup only nodes C and F are able to reach node Z. The other nodes cannot reach node Z. The useful size of this network is thereby limited to only 2 nodes, nodes C and F.



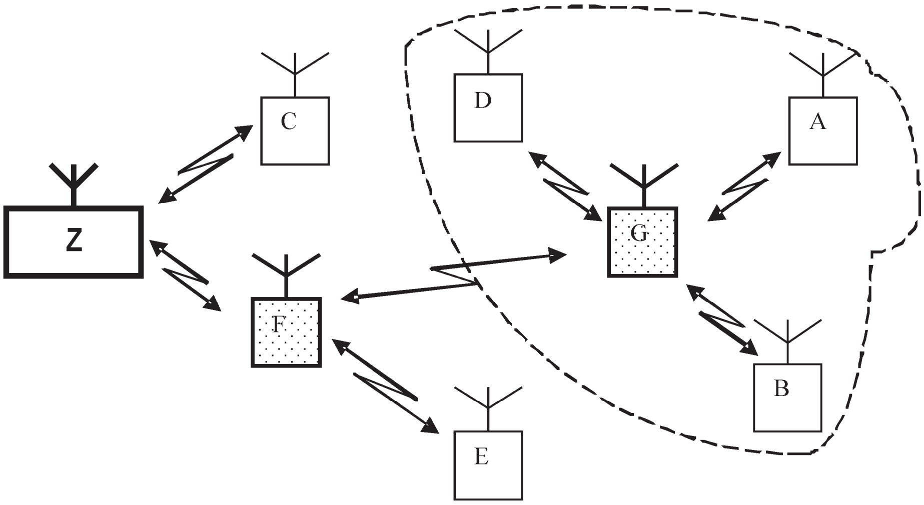
Key

A – G simple meters

Z data collecting unit/primary station

Figure 1 — Network with simple nodes, without relaying

Extending the network by adding some nodes with relaying capability will give a structure as shown in Figure 2. Nodes F and G have now been extended to include relaying capability. Communication between nodes A, B and D and the primary station is achieved by relaying the data through nodes G and F. Node A sends data to node G, node G relays data to node F and node F relays data to node Z, the data collecting unit. The size of the network can now be extended to include all of the nodes shown. Nodes F and G may be dedicated relaying nodes or meters with extended capabilities. Transmission from one node to another is called a hop. The transmission from node A to the data collecting unit/primary station consists of three hops.

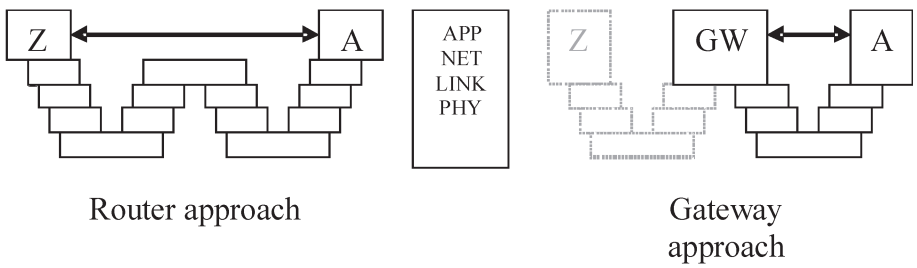


Key

A – E simple meters
F, G nodes with relaying capability
Z data collecting unit/primary station

Figure 2 — Network with relaying nodes

Note that the network still has a hierarchical structure at the application level, despite the relaying nodes. All end-to-end data transfer is performed between the data collecting unit and the meters. The meters do not communicate with one another at the application level, nor do the relays.



Key

A meter
GW node with relaying capability
Z data collecting unit/primary station

Figure 3 — Router vs. gateway solution

The relaying can be performed in two different ways as shown in Figure 3, using either a gateway or a router approach.

In the router approach all nodes in the network are aware of the other nodes in the network and they all use the same protocol in both directions. The nodes are aware of the routing capability of certain nodes as well. Node B, as shown in Figure 2, will know that it for instance has to send data through the relaying nodes G and F to reach the data collecting unit.

In the gateway approach only the locally reachable nodes are known. Nodes beyond the gateway are hidden. For nodes A, B and D in Figure 2, the network is limited to the area inside the dashed line, and node E is to all subordinate units the 'data collecting unit'. The gateways are organised in a hierarchy of networks as well, as shown in Figure 2, where node E is at the bottom of the hierarchy, node F is one level above it and node Z, the real data collecting unit, is at the top level.

The generic details of the gateway and the router approach are specified in the following subclauses.

4.4 Use of routers

In a routed network the nodes all behave like peer entities at the network level. Transfer between nodes is based on pairs of addresses, the sender node address and the receiver node address. This allows for a non-hierarchical structure of the nodes in a network with parallel paths.

The fact that a pair of addresses is needed makes the routed approach incompatible with the data link layer used in EN 13757-4. There is thus a need of being able to distinguish between native EN 13757-4 data and routed data at the data link layer. This to ensure that simple nodes don't try to decode and handle routed data by mistake.

The way of selecting the path to use when sending a package through a network can be determined in two ways. The first is the hop-by-hop method. Here the full path is set up prior to the first transmission, and it includes all the nodes to connect through. The second method uses network generated paths. Here the first node sends the data to a suitable neighbour router, and this router then determines the next hop for the data, based on its routing information. This latter method is the one used by the IP protocol on the Internet. The approach selected for this application is the hop-by-hop addressing method, as this is less complex to implement and requires less network traffic overhead and less intelligence in the nodes in the network.

4.5 Use of gateways

4.5.1 General

A simple node has only a single address field. It is only able to work in a network with a single primary station controlling the network and one or more secondary stations/meters. A simple node will, when receiving data, look for its own address in the address field. It will assume that all data sent to it originates from the primary station. A simple node will, when responding, include its own address in the header. It will assume that all data will be received by the primary station.

The gateway hides the network and network complexity from the simple nodes. To the nodes the gateway appears as the primary station. If the network shown in Figure 2 is using the gateways approach, then node G will appear as the primary station to node A, B and D. Node E will assume that node F is the primary station, and only node C will actually connect directly to node Z, the data collecting unit.

EN 13757-4 uses the approach of simple nodes. This makes the gateway approach backward compatible to EN 13757-4 units.

A gateway node may be a dedicated node or a meter with extended functionality.

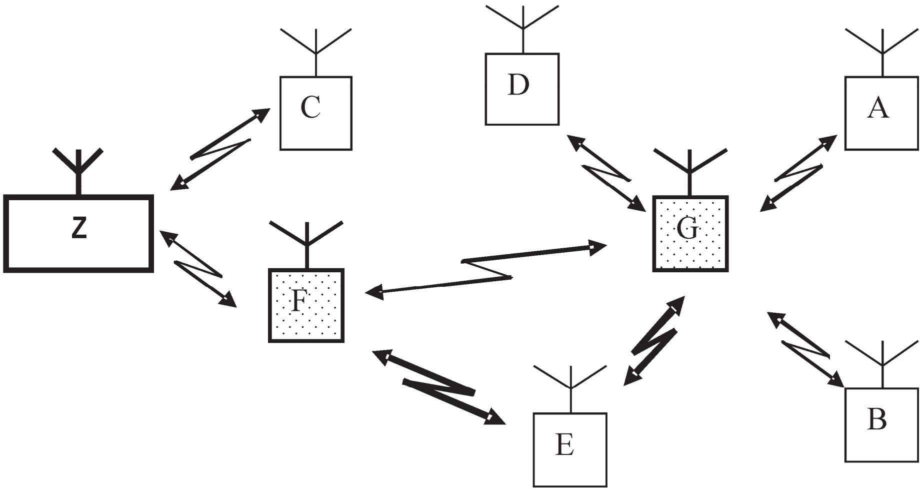
The gateway will, when sending data downstream to the simple node(s), appear like the primary station. It will send data to the simple nodes in the format specified in EN 13757-4 for the R2 mode. It will, when receiving data sent upstream from a simple node, appear like a primary station. It will accept data in the format as specified in EN 13757-4 for the R2 mode.

The gateway does not have any prior knowledge of the overall network configuration. Relaying of data must then either be based on fixed rules, or on information provided in the header of the data. Both of these approaches are used in this gateway protocol.

The gateway may, when data are sent upstream, use the generic rule that the network is hierarchical. The gateway will, when it has received data from a simple node to be sent upstream, forward them further upstream. Data will then be received by another gateway or the primary station. There is no need for destination addressing of data sent upstream.

4.5.2 Data duplication

Not all data sent upstream should be forwarded, as this may cause data duplication. This is can be seen in Figure 4 below.



Key
A – E simple meters
F, G nodes with relaying capability
Z data collecting unit /primary station

Figure 4 — Data duplication

Data sent by node E can be received by gateway G as well as by gateway F. When node E sends a set of data, it will be received by both gateways. One set of data will be sent along the path E – G – F to node Z, the data collecting unit, and another set of data will be sent along the path E – F to node Z. The use of unconditional relaying will cause duplication of the data received by the data collecting unit and cause unnecessary traffic on the network as well. Methods and rules need to be implemented to ensure that data duplication is avoided.

Two issues should be handled when looking into avoidance of data duplication:

a) whether to use enabling or disabling lists;

b) whether to use a list of local or global nodes.

The nature of radio communication is that the actual transmitting distance may vary a lot over time. It is thus not feasible to generate a list of nodes not allowed to relay for. Special transmitting conditions, due to for instance special metrological conditions, may make it possible to hear nodes located far away. It is as well possible that a new operator, also following this European Standard, could set up new nodes that weren't known when the initial network was set up. Data from the new nodes is not to be performed by default, but there is no possibility of knowing the coming of these nodes in advance. These are examples of situations that cannot be handled orderly by a disabling list. An enabling list is therefore to be used.

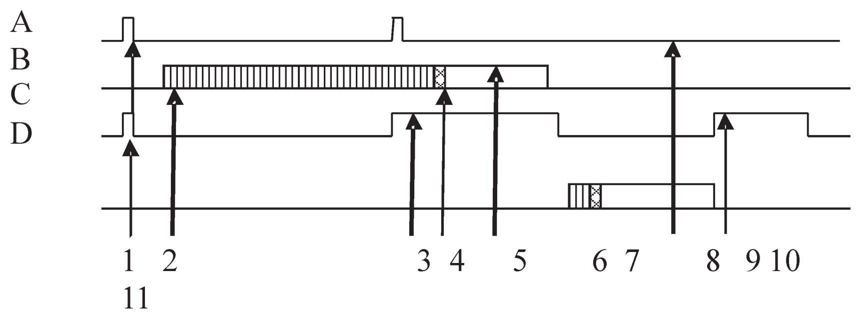
The use of a global list of nodes would require that nodes at the higher levels of the hierarchy must contain very large lists holding the address of all subordinate units it is to receive data from. All possible intermediate nodes have to contain information about all their subordinate nodes as well. This would require a lot of data memory in the gateways and cause a lot of network traffic when the lists are to be updated. The use of a local list has therefore been evaluated as superior, and selected. The use of a local list has the minor drawback that data sent upstream must contain the (local) address of the sending node, as well as the address of the originator, the meter.

More specific requirements will be explained in detail in the subclauses on gateways.

The gateway will need further address information when it receives data to be sent downstream. It must know what node(s) to forward the data to. This information, network control information, is to be available as a part of the header of the data.

4.6 Use of power strobed units

Many meters and intermediate nodes are battery operated and have to operate from a single battery for several years. This makes it necessary to conserve power by switching off part of the circuits in the node when not in use. One such part is the radio. This is further described in Figure 5. The control program in a node may, when the node isn't communicating, only switch on the receiver briefly with fixed intervals (1, 3). This listening will be disabled when the node is transmitting (8). Another node wanting to communicate with the power strobed node must then send a wake-up signal (2). The power-strobed receiver will, during its listening interval, look for data transfer of the expected type (a wake-up signal), and will switch off again if no data transfer is detected (1). The receiver shall, once wake-up is detected (3), look for a synchronisation pattern (4) and start to collect data (5). The receiver may, if the destination address of the information doesn't match that of the node, switch off to conserve power. A node should, after the transmitter in the node has been active (6, 7, 9), switch on the receiver for a period (10, 11) in anticipation of a response to the transmitted message. Such behaviour will improve the processing of the data and limit the duty cycle, as no wake-up sequence is needed.



Key

A receiver 'listening' window
B wake-up and data signal
C receiver active
D data transmitted

Figure 5 — Power strobed receiver

The duration of the wake-up sequence shall be long enough so that it is detected by the node during the first listening interval to ensure an effective data transfer, i.e. it must be longer than the listening interval of the receiver.

To prevent unnecessary wake-up of meters, the wake-up signal uses a different data rate than normal data transfers. On-going data transfers between nodes will not awake sleeping nodes, thus saving power.

The parameters specifying power wake-up behaviour should be standardised to ensure energy efficient data transfer in the radio network.

4.7 Error handling

The data error rate will be higher in a radio based network than in a wired network. Some of the reasons for this are:

— the units are operating in a license free band, where a lot of other units may be operating at the same time. Such units may garble or block the transmission between a pair of nodes in the metering network;

— noise from other sources may impair the signals;

— the radio transmission conditions may change due to changes in the environment (new building erected, container placed in front of the meters) or changes in weather conditions;

— the transmission of information from a meter to the data collecting unit may traverse multiple links. The overall transmission is only successful if all of the individual hops, forth and back, are successful.

All this makes it necessary to use efficient error handling algorithms in a radio based relayed network. To alleviate the error handling, the following concepts are implemented in the protocols used:

— data transmission is acknowledged for each hop;

— there is a fast acknowledge at the link layer;

— a negative acknowledge is returned if the message that should have been acknowledged is garbled and the sender can be identified;

— a standardised retry algorithm is used;

— if the retry algorithm fails, then the originating node is informed about the failure and about the hop where the failure occurred. This information is provided to higher layer protocols that may attempt to reroute the traffic through other nodes in the network. The protocols for such rerouting are outside the scope of this European Standard.

4.8 Time synchronisation

New regulations in the energy market [COM (2003) 739 Final] demand improved energy efficiency. This requires reporting of actual time of use and thereby precise time information from the meters. Standards for energy meters, like EN 62054-21, already quantify these requirements. This imposes capabilities of precision timing in the meters, and thereby for a communications system that allows for a precision time synchronisation through the network.

This need is to some extent in conflict with the use of power strobed meters and routers as shown in Figure 6 below.

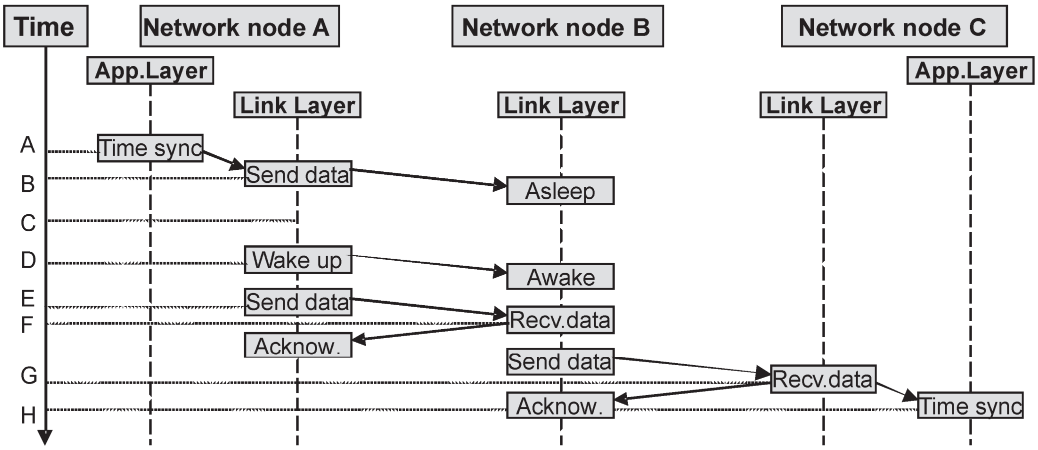


Figure 6 — Time synchronization propagation

The scenario is that a network node A distributes a time synchronization signal to some other nodes in the network, nodes B and C. One of the receiving nodes B is asleep and will need a wake-up signal before data can be transferred to it.

The management application in node A retrieves the time information at t_A. The information is processed by the lower protocol layers in the node, and sent to the network at t_B. The information isn't detected by the receiving node that is asleep. This will at t_C cause a timeout condition in the sending node A, as no acknowledge signal is received. The time-out condition will cause the link layer in node A to send a 'wake-up' signal at t_D, followed by a retransmission of the packet at t_E. The receiving node, B, is now awake and will receive the data at t_F, acknowledge the packet, and send the packet on to node C. Node C receives the data at t_G and passes the information on to the application layer at t_H.

The synchronization time in the application data is t_{BA}, whereas the actual time is t_H. This time difference t_H - t_A will be in the (multiple) seconds range if one or more of the intermediate nodes were asleep prior to the transfer. This is not acceptable according the requirements for modern meters in EN 62054-21.

A transmission protocol must be devised, that ensures that precise timing information can be transferred. Such a protocol must take into account the delay introduced during the end-to-end transmission. This information shall be updated for each hop in the transmission. This processing of the data must be performed at the link layer of the nodes. Experience from other precision timing protocols like IEEE 1588-2002 shows that this requires a special handling at the lower protocol layers. A special set of lower layer protocols will be specified for this purpose. The protocol shall contain a synchronisation time t_A as well as delay information t_H - t_{BA}. The synchronization time shall be a part of the application data. The delay information shall be a part of the link layer information. The delay information shall be updated for each hop/retransmission of the data. This protocol may be used if requirement for precision timing exists.

NOTE Interconnection to meters using an EN 13757-4 interface can be achieved using an application layer gateway.

4.9 Protocol possibilities

Based on the general needs expressed in this clause, three different protocols for relaying in a radio network are defined. They have the following general characteristics:

— A gateway based protocol: this protocol is intended for the extension of networks using the R2 mode as specified in EN 13757-4. Nodes using the gateway protocol may be meters as well as dedicated gateway nodes. They will interoperate seamlessly with R2 nodes. The gateway protocol can be used to extend the size of R2 networks. This is the protocol to use, if one wants to extend an existing network of R2 nodes. Networks using such gateways will anyway still have the constraint of a master/slave structure and a single address link layer.

- A router based protocol: this protocol, named mode P, extends the addressing to a dual address /balanced protocol as used by all modern data link layer protocols. This is done using the EN 60870-5-1 physical layer and EN 60870-5-2 link layer. Nodes using the mode P protocol cannot communicate directly with R2 nodes but the nodes can coexists in the same frequency band. The P and the R2 protocols are by structure very similar and dual-mode nodes supporting mode R2 as well as mode P may be foreseen. This is the protocol to use when one wants to use a true routed network with full addressing, but at the same time wants to keep the general structure of the R2 protocol.

- A contemporary protocol supporting precision timing: this protocol, named mode Q, is intended where one hasn't the need of following the EN 60870-5 series of standards. These EN 60870-5 series of standards were developed around 15 years ago and do not fulfil all the needs of a modern protocol. Mode Q takes into account the possibility of energy saving using power strobing of the nodes, the needs for transfer of precision timing information and the possibility of using NRZ coding based on digital signal processors. The protocol is applicable as the transport service for a modern object oriented high level application layer service like the DLMS protocol specified in EN 13757-1.

5 Mode P, protocol using routers

5.1 General

This protocol is applicable to communication between nodes with routing capability. The protocol shall use mode P at the physical layer and the data link layer to ensure that nodes without routing capability don't try to handle such messages.

The protocol is optimised for battery operated units with power strobed radio unit.

5.2 Physical layer protocol

5.2.1 General

All the parameters shall, at the minimum, conform to ETSI EN 300 220-1 and -2, even if some applications may require extended temperature or voltage range. The channel and frequency band shall be as specified in Table 1.

Table 1 — Mode P, general

Characteristic	Min.	Typ	Max.	Unit
Frequency band [a]	868.0		868.6	MHz
Channel spacing		60		kHz
Transmitter duty cycle [b]			1	%

NOTE The characteristics are, for the SRD band, identical to the characteristics for the S and R2 modes in EN 13757-4.

[a] The standard is optimised for the 868 - 870 MHz band, but with local radio approval it may allow for operation in other frequency bands.

[b] Duty cycle shall be as defined by ETSI EN 300 220-1 in the SRD bands. It may with local radio approval allow for other duty cycles in other frequency bands.

5.2.2 Transmitter

The parameters for the transmitters shall be as specified in Table 2.

Table 2 — Mode P, transmitter

Characteristic	Sym	Min.	Typ	Max.	Unit	Remark
Centre frequency [a] (other)			868.330		MHz	
Centre frequency [a] (meter)			868.030 + n × 0.06 [h]		MHz	
Frequency tolerance (meter / other)			0	± 17	kHz	~ 20 ppm
FSK Deviation		± 4.8	± 6	± 7.2	kHz	
Chip rate, wake-up [b]			3,12		kcps	
Chip rate tolerance, wake-up			0	± 2,5	%	
Wake-up signal duration	t_{WD}	5 200		6 000	µs	
Chip rate, communications [b]			4.8		kcps	
Chip rate tolerance, communications			0	± 1,5	%	
Digital bit jitter [c]				± 5	µs	
Data rate (Manchester encoding) [d]			f_{chip} × 1/2		bps	
Preamble (leader) length including bit / byte-sync	L_{PR}	96			chips	
Postamble (trailer) length [e]	L_{PO}	2		16	chips	
Acknowledge window [f]	t_{Aw}	3		50	ms	
Response delay [g]	t_{RD}	5		10 000	ms	

NOTE The wake-up chip rate has been selected in such a way that it may be possible to derive it from the same master clock as the communications chip rate.

[a] The standard is optimised for the 868 – 870 MHz band, but with local radio approval, it may allow for operation in other frequency bands.

[b] The chip rate during communication deviates from the chip rate during wake-up. This ensures that an ongoing transmission to another node isn't detected as a wake-up signal by a power-strobed unit.

[c] The bit jitter shall be measured at the output of the micro-controller or encoder circuit.

[d] Each bit shall be coded as 2 chips (Manchester coding).

[e] The postamble (trailer) shall consists of n = 1 to 8 'ones' i.e. the chip sequence shall be n × (01).

[f] Acknowledge window: after transmitting a message, the node shall be ready for the reception of an acknowledge message in less than the minimum acknowledge window. After transmitting a message, the node shall at least continue receiving for the duration of the maximum acknowledge window.

[g] Response delay: after receiving a request message, the node shall not start sending the response back in less than the minimum response delay and shall start sending the response back in less than the maximum response delay.

[h] n shall be in the range 0 to 9.

5.2.3 Receiver

The parameters for the receivers shall be as specified in Table 3.

Table 3 — Mode P, receiver

Characteristic	Class	Sym	Min.	Typ	Max.	Unit	Remark
Sensitivity [b]	H_R	P_o	- 105	- 110		dBm	
Blocking performance	L_R		3			Class [a]	
Blocking performance [c]	M_R		2			Class [a]	
Blocking performance [c, d]	H_R		2			Class [a]	
Acceptable chip rate range		f_{chip}	4,7	4,8	4,9	kcps	~ 2 %
Acceptable chip rate variation during header and frame		Df_{chip}		0	± 0,2	%	
Wake-up period		t_{WUP}			5 000	ms	
Acknowledge delay [e]		t_{AD}	5		48	ms	
Response wait [f]		t_{RW}			21 000	ms	

NOTE The characteristics with respect to frequencies and performance are the same as for mode R2 in EN 13757-4.

[a] Receiver class according to ETSI EN 300 220-1:2000, 9.3.

[b] The sensitivity shall either be measured at (BER < 10^{-2}) in conducted mode as specified in ETSI EN 300 220-2:2000, 4.1, or if this isn't possible then it shall be measured at (block acceptance rate > 80 %) as specified in ETSI EN 300 220-2:2000, 4.2.

[c] Additional requirement for M_R and H_R receiver class: the receiver shall meet the performance criteria as specified in ETSI EN 301 489-1:2008, 9.2 and ETSI EN 301 489-3:2002, 6.

[d] Additional requirement for the H_R receiver class: adjacent band selectivity shall be > 40 dB and adjacent channel selectivity shall be > 40 dB minimum, as specified in ETSI EN 300 220-1 V1-3-1:2000, 9.1 and 9.2 respectively.

[e] Acknowledge delay: after receiving a message, the node shall not start sending the acknowledge in less than the minimum acknowledge delay. After receiving a message, the node shall start sending the acknowledge in less than the maximum acknowledge delay.

[f] Response wait: after sending a message and expecting a response, a node shall, at the application layer, not time out the connection in less than the maximum response wait time. The maximum value takes into account that a wake-up signal must be sent to some of the units. The maximum value may be extended after agreement with the operator.

5.3 Data encoding

5.3.1 Manchester encoding

Manchester encoding shall be used for this mode. It allows for a simple coding/decoding. Each bit shall either be encoded as "10", chip sequence representing a data value of 0; or as 01, chip sequence representing a data value of 1. The lower frequency shall correspond to a chip value of 0.

5.3.2 Order of transmission of the encoded data

Each data byte shall always be transmitted with the most significant bit (MSB) first. The byte sequence of the CRC shall be transmitted with the high byte first. The byte sequence of all other multi-byte fields shall be transmitted with the low byte first.

5.3.3 Wake up and preamble chip sequences

This protocol is designed for use with long lifetime battery powered meters. It is important not to activate such meters at the wrong moment. The communications part of the meter is normally asleep/unpowered. The meter shall with regular intervals listen for a dedicated wake-up signal for a short time. It may, if no wake-up signal is detected, go asleep again.

The chip-rate for the wake-up signals shall deviate from the chip-rate for normal communication. This ensures that normal data traffic isn't detected as a wake-up signal.

A wake-up signal shall be sent before the preamble, when the sender expects the receiver to be asleep. The wake-up signal shall be immediately followed by the preamble. The total preamble (header + synchronisation) chip sequence for this mode is n × (01) 000111 0101 1010 0101 with n ≥ 39.

NOTE 1 In Manchester coding, the chip sequence 000111 is invalid, but it is used near the end of the header to allow a receiver to detect the start of a new or a stronger transmission. This applies even during reception of a weaker transmission. The capture effect allows efficient communication even in a channel where many weak transmitters from a large area might otherwise effectively block the reception of a nearer (stronger) transmitter. In addition, it allows receivers with power strobing to distinguish safely between the start of a valid frame and an accidental 'sync' sequence within an ongoing transmission.

NOTE 2 The synchronisation pattern differs from that of mode S and mode R2 of EN 13757-4.

All chips of each frame, including pre- and postamble shall form an uninterrupted chip sequence.

5.4 Data link layer protocol

5.4.1 General

The protocol used shall be symmetrical, i.e. the same formatting of the data is used independent of whether it is an upstream or a downstream data transfer.

The link layer as described in EN 60870-5-2:1993, 3.4 with the format class FT3 with the below mentioned exceptions shall be used:

— the two start characters as specified in EN 60870-5-1:1993, 6.2.4.4.2 are not used, as there is a preamble instead;

— some of the header information, the address of the source node, extends into the second block to allow for sufficient size address fields.

5.4.2 Frame format

A frame shall consist of at least two and optionally more blocks.

The format of the first block shall be as specified in Figure 7.

NOTE 1 The size of the first block is less than 16 bytes to avoid breaking an address into two parts.

L-field	C-field	M1-field	A1-field	CRC-field
1 byte	1 byte	2 bytes	6 bytes	2 bytes

Key

L-field the total number of data in block 2 and onward as specified in EN 60870-5-1
C-field the control field as specified in EN 60870-5-2:1993, 6.1.2 (balanced transmission)
M1-field the manufacturer ID field for the destination node, as specified in EN 13757-4:2005, 6.5.2.3
A1-field the address of the destination node
CRC-field the check field as specified in EN 60870-5-1:1993, Table 1, Format Class FT3

Figure 7 — First block format

NOTE 2 The size of the two A-fields has been set to 6 bytes to make it compatible with the meter address format used in EN 13757-4, to be able to uniquely identify the meter by the link layer address. This makes it necessary to split the total address information across two blocks, inserting a part of the address information in the second block.

The format of the second block shall be as specified in Figure 8.

M2-field	A2-field	CI-field	Data	CRC-field
2 bytes	6 bytes	1 byte	7 or if it is the last block (L - 9) bytes	2 bytes

Key
M2-field the manufacturer ID field for the source node, as specified in EN 13757-4:2005, 6.5.2.3
A2-field: the address of the source node
CI-field the control information field
Data network control and application data
CRC-field the check field as specified in EN 60870-5-1:1993, Table 1, format class FT3

Figure 8 — Second block format

The format of the other optional blocks shall be as specified in Figure 9:

Data	CRC-field
16 or if it is the last block ((L - 1) modulo 16) + 1 bytes	2 bytes

Key
Data network control and application data
CRC-field the check field as specified in EN 60870-5-1:1993, Table 1

Figure 9 — Optional blocks format

NOTE 3 The total number of blocks in a frame is limited to 16 by the size of the L-field.

5.4.3 C-field

5.4.3.1 General

For relays using the router approach, the requirements for the coding of the C-field, as specified in EN 60870-5-2:1993, 6.1.2 shall apply. This is balanced transmission.

NOTE The definitions from EN 60870-5-2 are used in the subsections that follow.

The format of the C-field, bit by bit, shall be as specified in Figure 10.

MSB LSB

<table>
<tr><td rowspan="2">DIR</td><td rowspan="2">PRM</td><td>FCB</td><td>FCV</td><td rowspan="2">Function code</td><td>Initiating node</td></tr>
<tr><td>RES</td><td>DFC</td><td>Acknowledging node</td></tr>
</table>

Figure 10 — C-field data format

In addition to this, the following shall apply.

5.4.3.2 When initiating a data exchange

When initiating a data exchange, the following shall apply:

- DIR bit shall be 1 as the direction is from the initiating node;
- PRM bit shall be 1 if the direction is downstream and 0 if the direction is upstream;
- FCB and FCV bit coding shall be as specified in EN 60870-5-2.

The function code shall have one of the values listed in Table 4.

Table 4 — Initiating function codes

Function code [a]	Symbolic name	Function	Acknowledge
0_h	LRESET	Link reset, shall be used when the FCB bit for this link shall be reset	No
3_h	SEND	Send data, shall be used when the node sends normal data	Yes
4_h	BCAST [b]	Broadcast data, shall be used when the node sends broadcast data	No
6_h	INSTALL	Install information, shall be used when the node sends data and it itself is in installation mode	Yes

NOTE There is no need for a REQUEST function code at link layer level as requests and responses are handled at the application layer level.

[a] The value of the 4 bit function code is specified in hexadecimal format as denoted by the trailing subscript 'h'.
[b] Broadcast data shall not be relayed through routers.

5.4.3.3 During acknowledge of a data exchange

When responding to a data exchange the following shall apply:

- DIR bit shall be 0 if the direction is from the responding node;
- PRM bit shall be 1 if the direction is downstream and 0 if the direction is upstream;
- RES bit shall be 0;
- DFC bit shall be 1.

The function code shall have one of the values listed in Table 5.

Table 5 — Acknowledging function codes

Function code	Symbolic name	Function
0_h	ACK	Acknowledge, shall be used when the node confirms a message with a function code of SEND or INSTALL
1_h	NACK	Not acknowledge, shall be used when the node rejects a message with a function code of SEND or INSTALL

5.4.4 M- and A-fields

The size of the first block is by EN 60870-5-1 limited to 16 bytes. This block shall according to EN 60870-5-2 include all of the address fields. This does not allow for a full 8 byte address field. The address has been extended into the second block to allow for the use of full 8 byte address fields. This is not fully compliant to EN 60870-5-2:1993, 3.4.

The M1 and M2 field shall contain a unique user/manufacturer identification of a node. The 15 least significant bits of these two bytes shall be formed from a three letter code, as specified in EN 13757-3. If the most significant bit of the M-field is 0, then the corresponding A-field shall be a unique (hard coded) manufacturer specified node address of 6 bytes. If the most significant bit of the M-field is 1, then the corresponding A-field may be a soft coded address. This address shall be unique within the maximum range of the network. Such an address is normally assigned to the node at installation time.

A node may be multi-homed, i.e. it may respond to multiple destination addresses.

NOTE The order of the M- and A-fields ensures that the receiving node is able to distinguish the destination address of the frame as early as possible. This improves the possibility of limiting the on time and thereby the power consumption.

EN 60870-5-2 specifies that the broadcast address is an address field with all bits set to 1. This shall, in the current context, be interpreted in the following way: the concatenated destination M- and A-field shall have all bits set to 1 in a broadcast message. The source M-field and A-field shall be that of the sending node of the broadcast message.

5.4.5 The CI-field

The CI-field is the header of the upper layers. The use of this byte is explained in the subsequent subclauses on the network layer and on the application layer.

5.4.6 Message handling

5.4.6.1 General

The message handling requirements specified here are all at the data link layer level.

5.4.6.2 Sending from an initiating node

The transmitter should, before initiating a transmission, receive on the selected channel and ensure that a transmission isn't blocking another ongoing transmission.

The initiating node shall initially send the message without a leading wake-up signal.

The initiating node shall the first time and second time a message is retransmitted due to a NACK prepend the message with a link reset message. It shall not send a leading wake-up signal.

The initiating node shall, the first time a message is retransmitted due to timeout, resend it with a leading wake-up signal.

The initiating node shall, the second time a message is retransmitted due to timeout, resend it without a leading wake-up signal.

The initiating node shall, if the transmission hasn't succeeded after 3 attempts, pass a 'not success' flag to the network layer.

5.4.6.3 Sending from an acknowledging node

The acknowledging node shall send the acknowledge message without a leading wake-up signal.

NOTE This is a reply to a node that recently sent a message, and it should still be powered and active.

5.4.6.4 Receiving from an initiating node

When receiving from an initiating node, the following shall apply:

- the receiving node shall drop the frame if the destination address, i.e. the M1- or the A1-field, is incorrect;
- the node shall drop the frame if the CRC check of the first block fails;
- the node shall not acknowledge a message if the function code doesn't request acknowledge (Table 4);
- the node shall reply with a NACK if the DIR bit is 0;
- the node shall reply with a NACK if the FCV/FCB control of the frame fails;
- the node shall reply with a NACK if the function code isn't in the set specified in Table 4;
- the node shall reply with a NACK if any of the subsequent CRC checks of the blocks fail;
- the node shall, if all of the above tests are passed, reply with an ACK and forward the data to the network layer.

5.4.6.5 Receiving from an acknowledging node

When receiving from an acknowledging node the following shall apply:

- the node shall drop the frame if the destination address, i.e. the M1- or the A1-field, is incorrect;
- the node shall initiate retransmission if the CRC check of the first block fails;
- the node shall initiate retransmission if the DIR bit is 1;
- the node shall reset the link and start a retransmission if a NACK is received;
- the node shall, if all of the above tests are passed, pass an 'accepted' flag to the network layer.

5.4.7 Timing requirements

The timing requirements specified here are all at the data link layer level.

The timing parameters referenced in this subclause are specified in Table 2 and Table 3.

A node shall, when an ACK or a NACK shall be sent by the data link layer, not start the reply before the minimum value of t_{AW}.

NOTE This ensures that the receiver in the former transmitting node is able to settle before the message is received.

A node shall, when an ACK or a NACK shall be sent by the data link layer, start the reply within t_{AD} of the end of the received message.

A node expecting an ACK or a NACK shall timeout the transfer if no data is received before the maximum value of t_{Aw}.

NOTE Requests and responses are handled at the application layer.

5.5 Network layer protocol

5.5.1 General

This protocol shall only be used with the mode P data link layer

The presence of a CI-field specifies that higher layer data follows. The structure of higher layer protocols shall be as shown in Figure 11.

A CI-field ≠ 81_h shall be used when the network layer is empty. An empty network layer may only be used when there is a direct connection between two end nodes. In this case no network layer information is transferred and the first byte of the higher layers shall be the application layer CI-field.

A CI-field = 81_h shall be used when there is a network layer. The network layer information shall then be followed by a secondary CI-field, the application layer CI-field.

CI	Hop info	Address 1	…..	Address n	App-CI	Application data
81_h	2 bytes	8 bytes		8 bytes	1 byte	x bytes
Network layer information					Application layer information	

Figure 11 — Higher layer format

5.5.2 Network layer format

The format of the network layer information is mainly a list of intermediate routers to hop via. The format shall be as shown in Figure 12.

CI	Hop count	Current hop	Source Addr.	Interm. Addr. 1	…	Interm. Addr. n	Destin. Addr.
81_h	1 byte	1 byte	8 bytes	8 bytes		8 bytes	8 byte

Key

CI 1 byte shall be 81_h, specifying that network layer information follows

Hop count 1 byte the total number of hops to perform, range 1 to 10

NOTE 1 This field will be 1 if it is an end-to-end transfer without any intermediate nodes. The total number of address elements in the network layer information is 'Hop count' + 1 as the source address is transmitted as well.

Current hop 1 byte the number of the next intermediate node to use as destination, range 1 to 10

NOTE 2 This field will have the value 1 during the first hop, i.e. when sent from the end node. It will have the value 'Hop count' during the last hop, i.e. when received by the end node.

Source Addr. 8 byte the data link layer address of the initiating end node. It shall as well be in the network layer data to ensure that a response can be sent back. The field is the concatenation of the M-field and the A-field from the data link layer

Interm. Addr.1 8 byte optional, the data link layer address of the first intermediate node (router) to use in this transfer, it shall be empty if it is an end-to-end connection

Interm. Addr.n 8 bytes optional, the data link layer address of the last intermediate node (router) to use in this transfer. It is the 'Interm. Addr.1' field if there is only 1 router. It shall be empty if it is an end-to-end connection. There may be up to 9 intermediate addresses

Destin. Addr. 8 bytes,the data link layer address of the receiving end node for the data transfer

Figure 12 — Network layer format

Data in the network layer protocol shall not be moved as data are transferred through the network. The only parameter that shall change for each hop is the 'Current hop' field. It shall be incremented. The order of the network layer address elements shall be reversed at the end node before a response may be sent back to the initiating node.

5.5.3 Relaying rules

These are the rules that shall be used for handling of information at the network layer and the rules that shall be used for passing of control information from the network layer to the data link layer:

a) the 'Current hop' shall be 1 at the initiating end node;

b) the 'Hop count' value shall be in the range 1 to 10. If the 'Hop count' value is outside this range then the frame shall be rejected;

c) if the 'Current hop' value is outside the range 1 to 'Hop count' then the frame shall be rejected;

d) there shall be 'Hop count' + 1 address element in the network layer data, including the source address and the destination address;

e) the source address may be interpreted as 'Intermediate Address 0' and the destination address may be interpreted as 'Intermediate Address (Hop count)';

f) in an intermediate node (router), the data link layer addresses for the next hop shall be generated in the following way:

   1) move the information from 'Intermediate Address (Current hop - 1)' to the source address field in the data link layer,

   2) move the information from the 'Intermediate Address (Current hop)' into destination address field in the data link layer;

g) the intermediate (or initiating) node shall then pass the information on to the data link layer, i.e. send the data;

h) the receiving node shall, if 'Current hop' = 'Hop count' pass the data on to the application layer;

i) the receiving node shall, if 'Current hop' < 'Hop count' increment 'Current hop' and repeat from step f);

j) the sending node shall, if the data link layer returns a flag of 'not success' when trying to send data, perform error handling as follows:

   1) if the direction of transfer is downstream, then it shall return an error message back to the data collecting end node,

   2) if the direction of transfer is upstream, then it may optionally store the information about missing upstream connection in an error log, and shall flag that the upstream connection is faulty.

NOTE The protocol is balanced at the link and network level, but is master driven at the application level. The meter will only send data when so requested by the data collecting unit. An error in the upstream path will in the downstream path either cause a timeout on the acknowledge at data link level, or a timeout of the response at the application level. It is then up to the data collecting unit to determine what to do. The intermediate node should not queue the data at transmission errors in the upstream direction.

5.6 Application layer protocol

5.6.1 CI-field

The CI- or Control Information-field indicates the type of application data that follows. The format of this field is compatible with EN 13757-4. The values that may be used for the application layer CI-field are listed in Table 6. All other values shall be reserved for future use.

Table 6 — Application layer, control information field

CI value	Designation	Remarks
51_h	Data sent by the readout device to the meter without fixed header	For compatibility with EN 13757-4
70_h	Error reporting	Compatible with EN 13757-3
71_h	Alarm report	Compatible with EN 13757-3
72_h	EN 13757-3:2004, Application layer with full header	For compatibility with EN 13757-4
78_h	EN 13757-3:2004, Application layer without header (to be defined)	For compatibility with EN 13757-4
$7A_h$	EN 13757-3:2004, Application layer with short header	For compatibility with EN 13757-4
81_h	Network layer data	Not allowed as application layer data,
82_h	For future use	For compatibility with EN 13757-4
83_h	Network management application	For management of the network layer
$A0_h$-$B7_h$	Manufacturer specific application layer	

5.6.2 Error reporting services

5.6.2.1 General

A routing node shall contain an error reporting service. The node shall use the service to return error status information. Error information returned shall use a CI-field of 70_h. The first byte following the CI-field is a type field. The format of the data shall be as shown in Figure 13.

CI	Type	Application data
70_h	XX_h	Further error information
1 byte	1 byte	n bytes

Figure 13 — Error status data format

The type field may have the values as defined in Table 7.

Table 7 — Type field, error status information

Type value	Designation	Remarks
00_h	Unspecified	Compatible with EN 13757-3
01_h	No application	Unimplemented CI – field
02_h – 09_h	Application error	Compatible with EN 13757-3
$0A_h$ – 10_h	Reserved	
11_h	No function	Function in network management not implemented
12_h	Data error	Data incorrect
13_h	Relaying error	Cannot relay data further
14_h – $1F_h$	Reserved	Reserved for future use
20_h	Installation	Meter in installation mode
21_h - BF_h	Reserved	Reserved for future use
$C0_h$ – FF_h	Manuf.	Manufacturer specific error information

5.6.2.2 No application

This error status shall be returned by the application layer if the requested application CI-field isn't implemented in the node. The type field shall be followed by a copy of the incorrect CI-field.

5.6.2.3 Application error

These error codes may be used if an EN 13757-3 application layer is implemented.

5.6.2.4 No function

This error status shall be returned by the application layer if the requested function, that is a defined function, isn’t implemented in the actual application layer. The type field shall be followed by a copy of the not implemented function field.

5.6.2.5 Data error

This error status shall be returned by the application layer if the data provided to the application layer are incorrect.

5.6.2.6 Relaying error

This error status shall be returned by the application layer, if the node cannot forward data to the next node. The data returned shows the path the data had traversed before relaying failed. The format of the data returned shall be as shown in Figure 14.

Type value	Status	Destin. Addr.	Num. fields	Interm., Addr. n	…	Interm. Addr. 1	Initiating Addr.
13_h	1 byte	8 bytes	1 byte	8 bytes		8 bytes	8 bytes

Key

Type	13_h indication relaying error
Status	enumerated, showing status of attempt: 0 no response from node, timeout three times 1 node responds, but with NAK 2 node reacts, but with error in answer
Destin. Addr.	8 bytes, the destination address that cannot be reached
Num. fields	1 byte, the number of address fields that follows, including the initiating address. The list holds the addresses of the nodes that the frame passed on its way out, the range is 1 to 10
Interm. Addr. n	8 bytes, 'Intermediate Address n': the address of the current node, i.e. the node to handle the data when they 'got stuck', shall be 'Intermediate Address 1' if only one relay node has been active
Interm. Addr. 1	8 bytes, 'Intermediate Address 1': the address of the first node that relayed the message
Init. Addr	the address of the node that initiated the transfer, either the data collecting unit or a meter

Figure 14 — Relay error format

The minimal situation will be when an end node can only reach the first relay. Then the 'Num. Fields' shall be 1, all but 'Intermediate Address 1' shall be absent and the initiating address will be that of the end node.

5.6.2.7 Installation mode

This function shall be used by a node to signal that it is in installation mode, i.e. not yet configured. The procedures to use during installation mode are outside the scope of this standard.

5.6.3 Network management service

5.6.3.1 General

A routing node shall contain a network management application. Data shall be passed on to the network management application, whenever the CI-field is 83_h. The format of the data shall be as shown in Figure 15. The 1 byte field following the CI-field is the function field or F-field and it defines the way data shall be interpreted.

CI	Function	Application data
83_h	XX_h	Function specific information
1 byte	1 byte	x byte

Figure 15 — Network management data format

The functions listed in Table 8 below covers the following network management requirements:

- There will be a demand for precision time tagging information of the nodes as there is a drift of the real time clock in the nodes. It shall thus be possible to set the time in the nodes. This time setting may include corrections for the delay in intermediate nodes.

- It shall be possible to generate and retrieve a list of the nodes that a gateway is able to receive data from, in order to set up the proper transmission paths.

- It shall be possible to pass on information about failures in the relaying of information through gateways. Two situations exist: failure in transferring data downstream and failure in transferring data upstream. The purpose of such error messages is to be able to detect a failing link in order to maintain an efficient and robust data transfer network.

The F-field may have the values as defined in Table 8.

Table 8 — F-field, network management function list

F-field	Designation	Remarks
00_h	Time sync	Time synchronisation signal
01_h	Forward time sync	Forward time synchronisation one step downward
14_h	Known nodes list	List of network nodes know to routing node
15_h	Clear nodes list	Clear content of list of nodes know to the routing node
21_h	Relay error status	Request and return of message on previous failing relaying
NOTE Handling of relaying errors is performed by using the generic error reporting service with CI = 70_h and Type = 13_h.		

Values of the F-field in the range 00_h to $7F_h$ are for standardised use. Values in this range, not listed in the table above, are reserved for future use (RFU) and shall not be used. Values in the range 80_h to FF_h may be used for manufacturer specific functions.

For the F-fields listed above, the format for the application data following the F-field and the corresponding functionality is listed below.

5.6.3.2 Time sync

This function is used when the primary station, the data collection unit, or intermediate nodes want to synchronise the time in all of the nodes they send data directly to. The data format shall be as shown in Figure 16.

F-field	Delay	Year	Month	Day	Hour	Min	Sec	Time Zone
00_h	2 bytes	1 byte	1 byte	1 byte	1 byte	1 byte	1 byte	1 byte

Key

F-field 00_h, indicating time sync
Delay 2 bytes unsigned integer, transport delay in ms, range 0 to 64 000
Year 1 byte, unsigned integer, years since 2000, range 5 to 99
Month 1 byte, unsigned integer, range 1 to 12
Day 1 byte, unsigned integer range, 1 to 31
Hour 1 byte, unsigned integer, range 0 to 23
Min 1 byte, unsigned integer, range 0 to 59
Sec 1 byte, unsigned integer, range 0 to 59
Time Zone 1 byte signed, range - 12 to 12, offset relative to UTC

NOTE 1 This makes it possible to handle time zones and Daylight Saving Time.

Figure 16 — Time sync data format

The initiating node shall insert a value into the delay field that corresponds to the delay from the time the clock value was read from the clock source and until the sync sequence in the preamble is transmitted.

The destination node should take into account any delay introduced by intermediate nodes. This may be done using the hop count and precalculated values.

NOTE 2 The intermediate nodes cannot themselves insert a delay value as they don't analyse the content of the application layer data.

This command may be sent using the broadcast address as specified in EN 60870-5-2. Nodes receiving this command as a broadcast receiver shall not broadcast it further to avoid 'broadcast storms'.

NOTE 3 The use of broadcast prevents the use of acknowledge signals and thereby the confirmation of the command.

The manufacturer shall state the precision of the delay calculations in initiating as well as in intermediate nodes.

NOTE 4 Applications requiring a higher precision in the timing should select the mode Q protocol for their system.

5.6.3.3 Forward time sync

This function is used when the primary station, the data collection unit, wants an intermediate node to synchronise the time in all of the nodes it sends data directly to, based on the intermediate nodes own clock. The data format shall be as shown in Figure 17.

F-field	Destin. Address
14_h	8 bytes

Key

F-field 01_h, indicating forward time sync

Destin. Address 7 bytes, destination address to use when forwarding the time synchronisation

Figure 17 — Forward time sync data format

The receiving node shall send a time synchronisation message to the nodes one level further away from the data collecting unit. The destination address shall be as specified in the data field.

This command shall be sent using the broadcast address as specified in EN 60870-5-2 if the destination address field is 'all ones'.

NOTE The use of broadcast prevents the use of acknowledge signals and thereby the confirmation of the command.

5.6.3.4 Known nodes list

It must be possible to get information about which routers are able to receive from which other routers and end nodes in order to be able to maintain a list of hops to use in the primary station. This function requests a router to return information about the end-nodes and routers it is able to receive data from. The list contains the addresses of all the nodes known and may as well contain a quality indicator for each of them. The format of the request as well as the response is listed below.

The format of the request shall be as shown in Figure 18.

F-field	Modifier
14_h	1 byte

Key

F-field	14_h, indicating known nodes list

Modifier	1 byte, with bit fields

Bit 7	0 = return first block from list
1 = return subsequent block from list

Bit 6	0 = return only node address information
1 = return node address and quality information

Bit 5..0	reserved for future use, shall be 0 when not used

Figure 18 — Known nodes request format

The format of the response shall be as shown in Figure 19.

F-field	Count/ Modifier	Address 1	Quality indicator 1	…	Address n	Quality indicator n
14_h	1 byte	8 bytes	1 byte (opt)		8 byte	1 byte (opt)

Key

F-field	14_h	indicator of function type

Count/Modifier	1 byte, with bit fields

Bit 7	0 = first block from list
1 = subsequent block from list

Bit 6	0 = only node address information returned
1 = node address and quality information returned

Bit 5	0 = more data available
1 = last block from list

Bit 4..0	range 0 to 27 number of address element sets ('Address' and 'Quality indicator') returned in this frame

Address 1	8 bytes, the full address of the first address in this frame from the list of nodes known to this relay

Quality indicator 1	1 byte, range 0 to 255. Optional parameter only returned if bit 6 of the 'Count/Modifier' field is 1. It indicates the quality of the receive-connection from the node to the relay. A large value indicates a good connection, and a small value a bad connection. The algorithm to be used for generation is outside the scope for this European Standard

Address n	8 bytes, the full address of the last address in this frame from the list of nodes known by this relay node

Quality indicator n	1 byte, range 0 to 255. Optional parameter only returned if bit 6 of the 'Count/Modifier' field is 1. It indicates the quality of the receive-connection from the node to the relay. A large value indicates a good connection, and a small value a bad connection. The algorithm to be used for generation is outside the scope for this standard

NOTE	The frame size at the link layer is the limiting factor for the number of address element sets in a block.

Figure 19 — Known nodes response format

5.6.3.5 Clear nodes list

It must be possible to regenerate the information about which nodes a gateway is able to receive from in order to be able to maintain a list of hops to use in the primary station. This function requests a gateway to restart the collection of this information. This will clear the internal list of known nodes. The format of the command shall be as shown in Figure 20.

F-field
15_h

Key
F-field 15_h indicating clear nodes list

Figure 20 — Clear nodes list command format

5.6.3.6 Relaying error status

An error while transferring data upstream is at the same time a fault in the transmission path for error information. This inhibits the transfer of error information to the primary node. The router shall handle this error condition in two steps. It shall at first store the error status locally and await restoration of the transmission path. Upstream data transfer is the response to a request. The primary station will detect the missing response and shall retry the request. The primary station shall, if this fails, try to establish an alternate transmission path to the router.

The router may, if the error condition remains for a prolonged time, switch back to installation mode, and send an unsolicited installation request to establish an alternate path from the router to the primary station. This condition can be used to establish an alternate path from the router to the primary station.

NOTE The mechanism for storing the error status locally and for establishing alternate transmission paths is outside the scope of this standard.

Once the transmission path has been re-established, the information about the error condition may be retrieved by the primary station. The format of a relaying error status, the request as well as the response is listed below.

The format of a relaying error status request shall be as shown in Figure 21.

F-field	Modifier
21_h	1 byte

Key
F-field 21_h indicator of function type
Modifier 1 byte, with bit fields

Bit 7 0 = return first block from list
1 = return subsequent block from list
Bit 6 0 = don't return time tag for relaying error data
1 = return time tag for relaying error data
Bit 5 0 = don't return application data for relaying error data
1 = return application data for relaying error data
Bit 4..0 0, reserved for future use

Figure 21 — Relaying error status request format

The format of a relaying error status response shall be as shown in Figure 22.

F-field	Count/ Modifier	Time tag 1	Destin. Addr. 1	App. data 1	…	Time tag n	Destin. Addr. n	App. data n
21_h	1 byte	7 bytes	8 bytes	n bytes		7 bytes	8 bytes	n bytes

Key

F-field 21_h indicator of function type

Count/ Modifier 1 byte, with bit fields

- Bit 7: 1 = time tag is returned for data; 0 = no time tag is returned for data
- Bit 6: 0 = application data is returned; 1 = no application data is returned
- Bit 5: 1 = last block from list; 0 = more data available
- Bit 4..3: reserved for future use, shall be 0
- Bit 2..0: number of error data sets, range 0 to 7

Time tag 1 7 bytes, optional, the time when the first transmission error occurred. Format as used for the time sync function in 5.6.3.2

Destin. Addr. 1 8 bytes, the full address of the node that couldn't be reached, from the first error

App. Data 1 n bytes, optional, the application data that couldn't be transferred, from the first error

Time tag n 7 bytes, optional, the time when the last transmission error occurred. Format as used for the time sync function in 5.6.3.2

Destin. Addr. n 8 bytes, the full address of the node that couldn't be reached, from the last error

App. Data n n bytes, optional, the application data that couldn't be transferred, from the last (most recent) error

Figure 22 — Relaying error status response format

The capability of returning time tag for the relaying error is an optional capability that may be implemented.

The capability of returning a copy of the application data from the relaying error is an optional capability that may be implemented.

A 'Count/Modifier' of 00_h and no further data shall be returned if no error condition has occurred.

NOTE 1 The number and structure of error data stored in the node for later retrieval is outside the scope of this standard.

NOTE 2 The frame size at the link layer may be the limiting factor for the number of error data transmitted in a block.

6 Mode R2, protocol using gateways

6.1 General

This protocol is applicable to communication with nodes following the R2 mode as specified in EN 13757-4 and to the communication between gateways.

6.2 Physical layer protocols

Relays using the gateway approach shall follow the requirements in EN 13757-4 for mode R2 with respect to the following parameters:

— allowed frequency band;

— transmitter performance;

— receiver performance;

— data encoding.

With respect to data encoding and order of transmission, the following additional requirements shall apply:

— all data sent as part of the network layer function and all network management data to and from the application layer shall be sent with the low byte first;

— with respect to transmitter duty cycle, the requirements for EN 13757-4 mode R2 shall apply for the SRD frequency band, but it may, with local radio approval, allow for other power levels and duty cycles in other frequency bands.

6.3 Data link layer protocol

6.3.1 General

Relays using the gateway approach shall follow the requirements in EN 13757-4 for mode R2 with respect to:

— L-field;

— M-field;

— A-field;

— CRC-field.

NOTE This protocol is asymmetrical as different rules apply for upstream and downstream data transfer.

6.3.2 M- and A-field

For relays using the gateway approach, broadcast address may be used. This is specified in EN 60870-5-2:1993, 5.1.3 as a condition with all address bits set. This shall include the M-field, as well as the A-field.

6.3.3 C-field

6.3.3.1 General

For relays using the gateway approach, the requirements for the coding of the C-field, as specified in 5.1.2 of EN 60870-5-2:1993 shall apply. This is an unbalanced transmission.

NOTE The definitions from EN 60870-5-2 are used in the subsections following below.

The general format of the C-field, bit by bit, is as shown in Figure 23.

<table>
<tr><td>MSB</td><td></td><td></td><td></td><td>LSB</td><td></td></tr>
<tr><td rowspan="2">RES</td><td rowspan="2">PRM</td><td>FCB</td><td>FCV</td><td rowspan="2">Function code</td><td>Primary to secondary</td></tr>
<tr><td>ACD</td><td>DFC</td><td>Secondary to primary</td></tr>
</table>

Figure 23 — C-field data format

6.3.3.2 Transmitting downstream

When transmitting downstream from a gateway the following shall apply:

— RES bit shall always be 0;

— PRM bit shall always be 1;

— FCB and FCV bit coding shall be used according to the rules in EN 60870-5-2.

The function code shall have one of the values specified in Table 9.

Table 9 — Downstream function codes

Function code[c]	Symbolic name	Function	Confirmation [d]
0_h	LRESET	Link reset, shall be used when the FCB bit for this link shall be reset	No
3_h	SEND	Send data, shall be used when the gateway sends normal data downstream	Yes
4_h	BCAST	Broadcast data, shall be used when the gateway sends broadcast data to all nodes downstream	No
6_h	INSTALL	Install information, shall be used when the gateway sends data to a node in installation mode	Yes
7_h	RACK [a]	Response acknowledge, shall be used when the gateway acknowledges a response message received from downstream	No
8_h	S-REQUEST [b]	Status request, may be used by the gateway to interrogate whether or not the end node has any outstanding class 1 data (like alarms) pending. The gateway may expect a confirmation and shall expect a response to this message	Yes
A_h	P-REQUEST [b]	Priority request, may be used by the gateway to request class 1 (priority) data from the node. The gateway may expect a confirmation and shall expect a response to this message	Yes
B_h	REQUEST	Request, may be used by the gateway to request class 2 (normal) data from the node. The gateway may expect a confirmation and shall expect a response to this message	Yes

[a] This is, compared to EN 13757-4, an extension to ensure the possibility of handshake in both directions.

[b] The gateway shall be able to handle a confirmation of this message and shall expect a response to this message.

[c] The value of the 4 bit function code field is specified in hexadecimal format as denoted by the trailing subscript 'h'.

[d] This column specifies whether or not the receiving node may confirm the reception of the message with an acknowledge or a non-acknowledge.

NOTE x-REQUEST is a short form description used in the next subclauses for either REQUEST, P-REQUEST or S-REQUEST.

6.3.3.3 Transmitting upstream

When transmitting upstream from a gateway the following shall apply:

— RES bit shall always be 0;

— PRM bit shall always be 0;

— DFC bit shall be 0. There is no need for flow control, as only one device is interrogated at a time;

— ACD bit may be 1 if the gateway has class 1 (priority) data like alarms outstanding.

The function code shall have one of the values specified in Table 10.

Table 10 — Upstream function codes

Function code	Symbolic name	Function
0_h	ACK	Acknowledge, shall be used when the gateway confirms a message with a function code of SEND or INSTALL
0_h	ACK	Acknowledge, may be used by the gateway to confirm the reception of an x-REQUEST prior to sending the x-RESPONSE
1_h	NACK	Not acknowledge, shall be used when the gateway rejects a message with a function code of SEND, INSTALL or x-REQUEST
6_h	INSTALL	Install, used when the gateway transfers a message from a node in installation mode or in itself sends a message while in installation mode
8_h	RESPONSE	Response, used when the gateway transfers a response from a node received with function code RESPONSE or N-RESPONSE, or in itself replies with a response to a request with a function code of P-REQUEST or REQUEST
9_h	N-RESPONSE	NACK response, used when the gateway transfers a message from a node received with function code N-RESPONSE or in itself, in its application layer, cannot reply to a request with a function code of x-REQUEST
B_h	S-RESPONSE	Status response, used when the gateway transfers a message from a node received with function code S-REPONSE or it itself acknowledges a S-REQUEST message

NOTE x-RESPONSE is a short form description for RESPONSE or S-RESPONSE.

6.3.3.4 Receiving from downstream

When receiving from downstream at a gateway, the following shall apply:

- The gateway shall drop the frame if the PRM bit is set;
- The gateway shall drop the frame if the CRC check of any of the blocks fails;
- The gateway shall pass on the setting of the ACD bit when it is transferred upstream;
- The gateway shall neglect the DFC bit;
- The gateway shall, if it receives an ACK (function code 0_h) as the answer to an x-REQUEST (function code 8_h, A_h or B_h), set an internal flag to ensure that it sends reverse acknowledge, RACK, (function code 7_h) when the x-RESPONSE (function code of 8_h or B_h) is received. The ACK message shall not be transferred upstream;
- The gateway may, if it receives a NACK (function code 1_h), retransmit the rejected frame up to 2 times. The gateway may send a LRESET frame (function code 0_h) before retransmitting. The NACK message shall not be transferred upstream. The gateway shall, if the retransmissions fail, generate an error handling condition;
- The gateway shall, if it receives an x-RESPONSE, except during conditions as stated later in this subclause, transfer it upward. The original M- and A-fields shall be kept in the message. It shall, if an ACK was received prior to the x-RESPONSE, reply with a RACK (function code 7_h);
- The message shall **not** be transferred if the address of the sending node isn't on the lists of nodes to transfer data from. See the network management application for further details;
- The gateway shall, if it receives an INSTALL (function code of 6_h), i.e. data from a node in installation mode, transfer it upward. The original M- and A-fields shall be kept in the network information of the message.

6.3.3.5 Receiving from upstream

When receiving from upstream at a gateway, the following shall apply:

- the gateway shall drop the message if the PRM bit is 0;
- the gateway shall drop the message if the CRC check of the first blocks fails;
- the gateway shall, if the message isn't a broadcast message, drop the message if the M- and A-fields in the frame don't match the address of the gateway;
- the gateway shall reply with a NACK if the FCV/FCB control of the message fails;
- the gateway shall reply with a NACK if the CRC check of the blocks fails;
- the gateway shall forward the message if the function code is BCAST, i.e. 4_h;
- the gateway shall pass the message on to the application layer if the function code is 3_h, 4_h, 6_h, 8_h, A_h or B_h;
- the gateway shall **not** forward a message with a function code of 0_h or 7_h even if the CI-field indicates so.

6.3.4 Timing requirements

The error rate for radio networks may be high, compared to the error rate in cable based communication. This makes it important that loss of data is detected fast. This is achieved by the use of local confirmation for each hop. The timing requirement for gateways reflects that delays are accumulated when data is sent through a relayed network. Stringent requirements are imposed on relaying nodes, whereas more relaxed requirements are imposed on meters to ensure that compatibility with EN 13757-4 is preserved.

The response delay parameters from EN 13757-4, mode R2 shall be used.

The gateway shall, when an ACK or a NACK shall be sent upstream, start the reply within t_{RO} of the end of the received message.

The gateway shall, when a RACK shall be sent downstream, start the reply within t_{RO} of the end of the received message.

The gateway shall, when it receives an x-REQUEST that causes a locally generated x-RESPONSE, start the reply within t_{RM} of the end of the reception of the message.

The gateway shall, when it expects a confirmation of a message from another gateway not time out the connection before $1{,}5 \times t_{RO}$. The gateway shall, when a connection to another gateway times out, retry the transmission 2 times. The gateway shall generate an error handling condition if the retransmission fails.

If a message is sent to a gateway as the final destination, then the gateway shall be handled as a meter.

The gateway shall, when it expects a confirmation of a message from a meter not time out the connection before $1{,}1 \times t_{RM}$. The gateway shall, when a connection to a meter times out, retry the transmission 2 times. The gateway shall generate an error handling if the retransmission fails.

6.3.5 Error handling

The gateway shall, if upstream transmission fails, drop the message. The gateway may record an internal status of missing uplink transfer.

The gateway shall, if a downstream transmission fails, send an unsolicited RESPONSE message upstream. The M- and A-fields of the message shall be the values of the gateway. The application layer message shall include the M- and A-fields of the failing receiver. See the network management application for further details.

6.4 Network layer functionality

6.4.1 General

The gateway has no dedicated network layer. Network information is 'hidden' in the first part of the application data. The information is identified by a special header, CI-field = 81_h. The network information is prepended to the normal application layer data.

NOTE 1 The insertion of network information will limit the maximum available size of actual application data, as the overall size of data link layer data is limited to 245 bytes.

NOTE 2 Information about the direction of transfer is available from the PRM bit in the data link layer.

6.4.2 Downstream transfer

Networking functionality specifies the path to the final destination to be used when sending downstream.

NOTE 1 The two byte field for hop information is used to make the data format compatible to the format of routed networks.

NOTE 2 The format of the network layer information is different from the format used for mode P, as it doesn't initially hold the source address and only transmits the remaining path information along with the data.

The network information consists of a pair of count followed by the addresses of the gateways to use. The limit of 10 hops has been chosen as a compromise between the amount of application data space to use on the one hand and possible size of radio networks on the other hand.

The format of the network layer information shall be as shown in Figure 24.

CI	Hop count	Current hop	Address 1	…	Address n	App-CI	Application data
81_h	1 byte	1 byte	8 byte		8 byte	1 byte	x byte
Network information						Application information	

Key

CI	1 byte	81_h, special value indicating that relaying information follows
Hop count	1 byte	the total number of hops to perform, range 1 to 10
Current hop	1 byte	the remaining number of hops to perform, range 1 to 10. This is also the number of address elements in the network layer information
Address 1	8 bytes	the address of the first gateway to use, i.e. the M- and A-field of that gateway
……		
Address n	8 bytes	the address of the last gateway to use
App-CI	1 byte	the CI-field related to the application data, i.e. the CI-field to use when transferring the application data to the meter
Application data	x byte	the data to be transferred to the meter

Figure 24 — Network downstream information format

6.4.3 Downstream relaying rules

These rules are only applicable when data are to be relayed downstream (CI = 81_h). When relaying downstream, the following rules for use of the network information shall apply:

1) if the hop count is outside the range 1 to 10, then reject the frame;

2) if the current hop is outside the range 1 to 'Hop count', then reject the frame;

3) move the information from address 1 into the M- and A-fields in the data link layer;

4) remove 'Address 1' from the network information;

5) decrement the 'Current hop';

6) if 'Current hop' = 0, remove CI, 'Current hop' and 'Hop count' fields;

7) adjust the length (L) field and the CRC check of the data link layer to reflect the reduction of the frame size;

8) send the data.

A configuration with CI = 81_h and 'Hop count' = 0 is a possibility that shall not be used.

6.4.4 Upstream transfer

Network information consists of the address of the end-node (meter) that originally sent the data. The address of the end-node is needed to be able to track the origin of the data at the primary station. This address cannot be carried in the data link layer, as the address of the relay is used in the data link layer to make it possible to filter out relaying nodes not to relay from, to avoid duplication of data. Dummy hop count information is stored in the header to allow for a uniform processing of network layer information in the up- and downstream direction.

The format of the network information shall be as shown in Figure 25.

CI	Hop info	End-node address	App-CI	Application data
81_h	2 bytes	8 bytes	1 byte	x bytes
Network information			Application information	

Key

CI	81_h	special value indicating that relaying information follows
Hop info	2 bytes	a dummy value of 0101_h inserted to achieve a uniform decoding of the network information and application information in upstream and downstream direction
End-node address	8 bytes	the address of the meter (end-node) that originally sent the data
App-CI	1 byte	the CI-field used when the meter transferred the data to the gateway
Application data	x bytes	the data to be transferred from the meter to the primary station

Figure 25 — Network upstream information format

6.4.5 Upstream relaying rules

The rules are only applicable when data are relayed upstream. When relaying upstream, the following rules for use of the network information shall apply.

a) If the data received are from an end-node, i.e. CI ≠ $81_{h,}$ then:

1) if the address of the end-node isn't in the list of end-nodes to relay from and the list is non-empty then drop the data and exit;
2) prepend a CI-field of 81_h and the link layer address of the end-node (the meter) to the CI-field and the application data from the end-node;
3) replace the end-node address at the link layer with the address of the gateway;
4) update the length field (L) and the CRC checks of the link layer frames to reflect the changes in the frame;
5) send the data.

b) If the data received are from a relay node, i.e. CI = 81h, then:

1) if the address of the gateway isn't on the list of gateways to relay from and the list is non-empty, then drop the data and exit;
2) replace the relay address at the link layer with the address of the current gateway;
3) send the data.

6.5 Application layer

6.5.1 CI-field

The CI- or Control Information-field indicates the type of application data that follows. The format of this field is compatible with the applications layer of EN 13757-3:2004 (Table 1). The values that may be used for the application layer CI-field shall be one of the values listed in Table 11. All other values shall be reserved for future use.

Table 11 — Application layer, control information field

CI value	Designation	Remarks
51_h	Data sent by the readout device to the meter without fixed header	For compatibility with the EN 13757-3:2004 Application Layer standard
70_h	Reserved for error report	For compatibility with the EN 13757-3:2004 Application Layer standard
71_h	Reserved for alarm report	For compatibility with the EN 13757-3:2004 Application Layer standard
72_h	EN 13757-3:2004, Application Layer with full header	For compatibility with the EN 13757-3:2004 Application Layer standard
78_h	EN 13757-3:2004, Application Layer without header (to be defined)	For compatibility with the EN 13757-3:2004 Application Layer standard
$7A_h$	EN 13757-3:2004, Application Layer with short header	For compatibility with the EN 13757-3:2004 Application Layer standard
81_h	Network layer data	Not allowed as application layer data,
82_h	For future use	For compatibility with CENELEC TC 205 standard
83_h	Network management application	For management of the network functionality
$A0_h$-$B7_h$	Manufacturer specific application layer	May be assigned manufacturer specific values

6.5.2 Network management services

6.5.2.1 General

A relay node shall contain a network management application. Data shall be passed on to the network management application whenever the CI-field is 83_h.The format of the data shall be as shown in Figure 26. The 1 byte field following the CI-field is the function field or F-field and it defines the way data shall be interpreted.

CI	Function	Application data
83_h	XX_h	Function specific information
1 byte	1 byte	x byte

Figure 26 — Network management data format

The functions listed in the table below covers the following network management requirements:

— There may be a demand for precision time tagging of information the nodes. It shall thus be possible to set the time in the nodes, as there is a drift of the real time clock in the nodes;

— It shall be possible to generate and retrieve a list of the nodes that a gateway is able to receive data from, in order to set up the proper transmission paths;

— It shall be possible to limit the number of nodes to relay from to avoid data duplication as discussed in 4.5.2. It shall be possible to add elements to the list and to clear the list;

— It shall be possible to pass on information about failures in the relaying of information through gateways. Two situations exist: failure in transferring data downstream and failure in transferring data upstream. The purpose of such error messages is to be able to detect a failing link in order to maintain an efficient and robust data transfer network.

The F-field may have the values as defined in Table 12.

Table 12 — F-field, network management functionality list

F-field	Designation	Remarks	Direction
00_h	Time sync	Time synchronisation signal	downstream
10_h	Clear relaying list	Clear list of nodes to relay from	downstream
11_h	End-node relaying list	List of end-nodes to relay from	downstream
12_h	Gateway relaying list	List of gateways to relay from	downstream
14_h	Known nodes list	List of network nodes known to relay node	up- and downstream
15_h	Clear known node list	Clear content of list of nodes known to the relay.	downstream
20_h	Downstream relaying error	Return message on failing downstream relaying	upstream
21_h	Upstream relaying error	Request and return of message on previous failing upstream relaying.	up- and downstream

Values in the range 00_h to $7F_h$ are for standardised use. Values in this range, not listed in the table above are reserved for future use, RFU. Values in the range 80_h to FF_h are available for manufacturer specific use.

The format for the application data following the F-field and the corresponding functionalities are listed in the subsequent subclauses. For all of the functionalities listed, only the application layer data are shown in the figures.

6.5.2.2 Time sync

This function is used when the primary station, the data collection unit, wants to synchronise the time in all of the nodes it receives data from. The data format shall be as shown in Figure 27.

F-field	Year	Month	Day	Hour	Min	Sec	Time Zone
00_h	1 byte	1 byte	1 byte	1 byte	1 byte	1 byte	1 byte

Key

Year 1 byte, unsigned integer, range 5 to 99
Month 1 byte, unsigned integer, range 1 to 12
Day 1 byte, unsigned integer, range 1 to 31
Hour 1 byte, unsigned integer, range 0 to 23
Min 1 byte, unsigned integer, range 0 to 59
Sec 1 byte, unsigned integer, range 0 to 59
Time Zone 1 byte signed integer, range - 12 to 12, offset relative to UTC

NOTE 1 It is assumed that any fractions of seconds in the node are cleared when this command is received.

NOTE 2 This command may be sent using the broadcast address as specified in EN 60870-5-2.

Figure 27 — Time sync format

6.5.2.3 Clear relaying list

This function requests the addressed node to clear its relaying list. It may be the end-node list, the gateway list or both. The format of the function shall be as shown in Figure 28.

F-field	Modifier
10_h	1 byte

Key
F-field 10_h indicator of function type
Modifier 1 byte with bit fields

Bit 7 1 = clear gateway relaying list
0 = don't clear gateway relaying list
Bit 6 1 = clear end-node relaying list
0 = don't clear end-node relaying list
Bit 5..0 reserved for future use (RFU), shall be 0 when not used

Figure 28 — Clear relaying list format

6.5.2.4 End-node relaying list

This function adds elements to the list of non-relaying nodes that the gateway shall relay information for. This is the list that shall be used for EN 13757-4 nodes. The format of the list shall be as shown in Figure 29.

F-field	Node count	Address 1	…..	Address n
11_h	1 byte	8 byte		8 byte

Key
F-field 11_h indicator of function type
Node count 1 byte range 0 to 29, a 'Node count' of 0 may be used for unconditional relaying
Address 8 byte the link layer address of an end-node to relay for upstream

NOTE 1 The frame size at the link layer is the limiting factor for the number of addresses.

NOTE 2 It is possible to generate a list of more than 29 nodes by sending multiple set of data.

Figure 29 — End-node relaying list format

6.5.2.5 Gateway relaying list

This function adds elements to the list of relaying nodes that the gateway shall relay information for. The format of the list shall be as shown in Figure 30.

F-field	Node count	Address 1	…	Address n
12_h	1 byte	8 byte		8 byte

Key
F-field 12_h indicator of function type
Node count 1 byte range 0 to 29, a 'Node count' of 0 may be used for unconditional relaying
Address 8 byte the link layer address of an end-node to relay for upstream

NOTE 1 The frame size at the link layer is the limiting factor for the number of addresses.

NOTE 2 It is possible to generate a list of more than 29 nodes by sending multiple set of data.

Figure 30 — End-node relaying list format

6.5.2.6 Known nodes list

This function requests a gateway to return information about the end-nodes and relays it is able to receive data from. The list contains the addresses of all the nodes known and may as well contain a quality indicator for each of them. The list may be transferred in 'chunks' due to the limitations of the link layer. The format of the command shall be as shown in Figure 31.

F-field	Modifier
14_h	1 byte

Key

F-field 14_h indicator of function type

Modifier 1 byte with bit fields

Bit 7 0 = return first block from the list
1 = return next block from the list

Bit 6 0 = return only node address information
1 = return node address and quality information

Bit 5..0 reserved for future use (RFU), shall be 0 when not used

Figure 31 — Known nodes command format

The format of the response shall be as shown in Figure 32.

F-field	Count/ Modifier	Address 1	Quality indicator 1	…….	Address n	Quality indicator n
14_h	1 byte	8 byte	1 byte (opt)		8 byte	1 byte (opt)

Key

F-field 14_h indicator of function type

Count/Modifier 1 byte, with bit fields

Bit 7 0 = first block from list
1 = subsequent block from list

Bit 6 0 = only node address information returned
1 = node address and quality information returned

Bit 5 0 = more data available
1 = last block from list

Bit 4..0 range 0 to 27, number of address element sets returned

Address 1 8 byte, the full address of the first address in this block from the list of nodes known to this relay

Quality indicator 1 1 byte, range 0 to 255. Optional parameter only returned if bit 6 of the 'Count/Modifier' field is 1. It indicates the quality of the connection from the node to the relay. A large value indicates a good connection, and a small value a bad connection. The algorithm to be used for generation is outside the scope for this standard

NOTE 1 Quality information is optional information. It should only be returned if requested and if the node supports the capability.

Address n 8 byte, the full address of the last address in this block from the list of nodes known by this relay node

Quality indicator n 1 byte, range 0 to 255. Optional parameter only returned if bit 6 of the 'Count/Modifier' field is 1. It indicates the quality of the connection from the node to the relay. A large value indicates a good connection, and a small value a bad connection. The algorithm to be used for generation is outside the scope for this standard

NOTE 2 The frame size at the link layer is the limiting factor for the number of address element sets in a block.

Figure 32 — Known nodes response format

6.5.2.7 Clear known nodes list

This function requests a gateway to clear its known nodes list and restart the collection of this information. The format of the command shall be as shown in Figure 33.

F-field
15_h

Key
F-field 15_h indicator of function type, clear nodes list

Figure 33 — Clear known nodes list command format

6.5.2.8 Downstream relaying error

When transferring data downstream, a gateway shall return an error status if it cannot send information downstream. The error status shall be sent back to the primary node.

The format of a downstream error status shall be as shown in Figure 34.

F-field	Condition	Address
20_h	1 byte	8 byte

Key
F-field 20_h indicator of function type, a downstream relaying error status
Condition 1 byte with bit fields

Bit 7set if frame was rejected due to consistent NACK from next node
Bit 6set if frame was rejected due to time out (no response) from the next node
Bit 5..0 reserved for future use, shall be 0 when not used

Address 8 byte the link layer address of the down stream mode

Figure 34 — Downstream relaying error format

6.5.2.9 Upstream relaying error

The situation is slightly more difficult when an error occurs while transferring data upstream. A fault in the upstream transmission is at the same time a fault in the transmission path for error information as well. The gateway shall handle this error condition in two steps. It shall at first store the error status locally and await restoration of the transmission path. Upstream data transfer is the response to a request. The primary station will detect the missing response and shall retry the request and if this fails, try to establish an alternate transmission path to the gateway.

The gateway may, if the error condition remains for a prolonged time, switch back to installation mode, and send an unsolicited installation request to establish an alternate path from the gateway to the primary station. This can be used to reinstall the connections to the node.

NOTE The mechanism for storing the error status locally and for establishing alternate transmission paths is outside the scope of this standard.

Once the transmission path has been re-established, the information about the error condition can be retrieved by the primary station. The format of an upstream relaying error, the command to request error condition information, as well as the response to it is listed below.

The format of an upstream error status request shall be as shown in Figure 35.

F-field
21_h

Key

F-field 21_h indicator of function type

Figure 35 — Upstream relaying error request format

The format of the upstream relaying error response shall be as shown in Figure 36.

F-field	Count/ Modifier	Time tag 1	Application data 1	…	Time tag n	Application data n
21_h	1 byte	7 bytes	n bytes		7 bytes	n bytes

Key

F-field 21_h indicator of function type

Count/Modifier 1 byte with bit fields

- Bit 7: 1 = time tag is returned for data
  0 = no time tag is returned for data
- Bit 6: 0 = application data is returned
  1 = no application data is returned
- Bit 5: 0 = more data available
  1 = last block from list
- Bit 4..3: reserved for future use, shall be 0
- Bit 2..0: number of error data sets, range 0..7

A Count/Modifier of 00_h shall be returned if no error condition has occurred

NOTE 1 The number and structure of error data stored in the node for later retrieval is outside the scope of this standard.

NOTE 2 The frame size at the link layer may be the limiting factor for the number of error data.

Time tag 1: 7 bytes, optional, the time when the first upstream transmission error occurred. Format as used for the 'Time sync' function

Application Data 1: n bytes, optional, the application data that couldn't be transferred, from the first upstream transmission error

Time tag n: 7 bytes, optional, the time when the most recent upstream transmission error occurred. Format as used for the 'Time sync' function

Application Data 1: n bytes, optional, the application data that couldn't be transferred. Data from the most recent upstream transmission error

NOTE 3 The relaying node cannot, at data transfer in the upstream direction, provide information about the address of the node that couldn't be reached, as is possible in a protocol using routers.

Figure 36 — Relaying error status response format

7 Mode Q, protocol supporting precision timing

7.1 General

This protocol is applicable to communication between nodes requiring and supporting precision timing based on dynamic delay handling.

The protocol is optimised for battery operated units with power strobed radio unit.

7.2 Physical layer protocol

7.2.1 General

All the parameters shall, at the minimum, conform to ETSI EN 300 220-1 and -2, even if some applications may require extended temperature or voltage range. The channel and frequency band shall be as specified in Table 13.

Table 13 — Mode Q, general

Characteristic	Min.	Typ	Max.	Unit
Frequency band [a]	868.0		868.6	MHz
Channel spacing [a]		60		kHz

NOTE The characteristics are, for the SRD band, identical to the characteristics for the S and R2 modes in EN 13757-4.

[a] The standard is optimised for the 868 – 870 MHz band, but with local radio approval, it may allow for operation in other frequency bands and with other channel spacing.

[b] Duty cycle shall be as defined by ETSI EN 300 220-1 in the SRD bands. It may with local radio approval allow for other duty cycles in other frequency bands.

7.2.2 Transmitter

The parameters for the transmitters shall be as specified in Table 14:

Table 14 — Mode Q, transmitter

Characteristic	Sym	Min	Typ	Max	Unit	Remark
Centre frequency [a] (other)			868.330		MHz	
Centre frequency [a] (meter)			868.030 + n × 0.06 [h]		MHz	
Transmitter duty cycle [b]				1	%	
Frequency tolerance [a] (meter / other)			0	± 17	kHz	~ 20 ppm
FSK Deviation [a]		± 4.8	± 6	± 7.2	kHz	
Bit rate, wake-up [c]			3,12		kbps	
Bit rate tolerance, wake-up			0	± 2,5	%	
Wake-up signal duration	t_{WD}	5 200		6 000	µs	
Bit rate communications [c]			4 800,00		bps	
Bit rate tolerance, communications			0	± 100	ppm	
Digital bit jitter [d]				± 5	µs	
Preamble (leader) length including bit / byte-sync	L_{PR}	160			bits	
Postamble (trailer) length [e]	L_{PO}	2		16	bits	
Acknowledge delay [f]	t_{AD}	20		30	ms	
Idle detect [g]	t_{ID}	40		1 000	ms	

NOTE The wake-up bit rate has been selected in such a way that it may be possible to derive it from the same master clock as the communications data rate.

[a] The standard is optimised for the 868 – 870 MHz band, but with local radio approval it may allow for operation in other frequency bands with other channel bandwidths.

[b] Duty cycle shall be as defined by ETSI EN 300 220-1 in the SRD bands. It may with local radio approval allow for other transmission levels and duty cycles in other frequency bands.

[c] The bit rate during wake-up deviates from the bit rate during communication to conserve energy. The difference in bit rate ensures that an ongoing transmission to another node isn't detected as a wake-up signal by a power-strobed unit.

[d] The bit jitter shall be measured at the output of the micro-controller or encoder circuit.

[e] The postamble (trailer) shall consists of n = 1 to 8 "01" i.e. the bit sequence shall be n × (01).

[f] Acknowledge delay: after receiving a data frame, a node shall not start sending the acknowledge frame in less than the minimum acknowledge delay. After receiving a data frame, a node shall start sending the acknowledge frame in less than the maximum acknowledge delay.

[g] Idle detect: prior to transmitting a data frame, a node shall listen and not detect any transmissions for a period of at least minimum idle detect time before transmitting. A node may start transmitting a data frame if it has listened for more than maximum idle detect without detecting an idle channel.

[h] n shall be in the range 0 to 9.

7.2.3 Receiver

The parameters for the receivers shall be as specified in Table 15.

Table 15 — Mode Q, receiver

Characteristic	Class	Sym	Min.	Typ	Max.	Unit	Remark
Sensitivity [b]	H_R	P_o	- 105	- 110		dBm	
Blocking performance	L_R		3			Class [a]	
Blocking performance [c]	M_R		2			Class [a]	
Blocking performance [c, d]	H_R		2			Class [a]	
Acceptable bit rate range		fbit $_{bit}$	4 799,52	4 800,00	4 800,48	bps	± 100 ppm
Wake-up period		t_{WUP}			5 000	ms	
Wake-up time-out [e]		t_{WUT}	16 000			ms	
Acknowledge window [f]		t_{Aw}	16		50	ms	
Acknowledge time-out [g]		t_{AT}	200			ms	

NOTE The characteristics, with respect to frequencies and performance, are the same as for mode R2 in EN 13757-4.

[a] Receiver class according to ETSI EN 300 220-1:2000, 9.3.

[b] The sensitivity shall either be measured at (BER < 10^{-2}) in conducted mode as specified in ETSI EN 300 220-2:2000, 4.1, or if this isn't possible then it shall be measured at (block acceptance rate > 80 %) as specified in ETSI EN 300 220-2:2000, 4.2.

[c] Additional requirement for M_R and H_R receiver class: the receiver shall meet the performance criteria as specified in ETSI EN 301 489-1:2008, 9.2 and ETSI EN 301 489-3:2002, 6.

[d] Additional requirement for the H_R receiver class: adjacent band selectivity shall be > 40 dB and adjacent channel selectivity shall be > 40 dB minimum, as specified in ETSI EN 300 220-1 V1-3-1:2000, 9.1 and 9.2 respectively.

[e] Wake-up time-out: after receiving a wake-up signal or a valid data frame, the receiver shall stay powered on for at least the minimum wake-up time-out.

[f] Acknowledge window: after transmitting a data frame a node shall be ready for the reception of an acknowledge frame in less than the minimum acknowledge window. After transmitting a data frame, a node shall at least continue receiving for the duration of the maximum acknowledge window. A node may use other means than the reception of an acknowledge frame as the detection of the reception of a data frame.

[g] Acknowledge time-out: after transmitting a data frame and waiting for an acknowledge, a node may time out the connection if no acknowledge is received within the minimum acknowledge time-out.

Information in this subclause is limited to the timing requirements at the physical layer. Requirements for routing timing are specified in the network layer subclause. Requirements for end-to-end timing are specified in the application layer subclause.

7.3 Data encoding

7.3.1 NRZ encoding

The individual data bits are encoded using non return to zero coding. This is made possible using the transceiver chips with digital signal processing. A bit of 0 shall correspond to the lower frequency in the FSK.

7.3.2 Order of transmission of the encoded data

Each data byte shall always be transmitted with the least significant bit (LSB) first. The byte sequence of the CRC shall be transmitted with the high byte first. The byte sequence of all other multi-byte fields shall be transmitted with the low byte first.

7.3.3 Wake up and preamble bit sequences

This protocol is designed for use with long lifetime battery powered meters. It is important not to activate such meters at the wrong moment. The communications part of the meter is normally asleep/unpowered. The meter shall with regular intervals listen for a dedicated wake-up signal for a short time. It may, if no-wake up signal is detected, go asleep again.

The bit rate for the wake-up signals shall deviate from the bit rate for normal communication. This ensures that normal data traffic isn't detected as a wake-up signal.

A wake-up signal shall be sent before the preamble, when the sender expects the receiver to be asleep. The wake-up signal shall be immediately followed by the preamble. The total preamble (header + synchronisation) chip sequence for this mode is n × (01) 0001 1101 0110 0110 0110 1101 0011 1001 with $n \geq 64$.

NOTE 1 The long header makes it possible for the receiver to adjust its centre frequency during this period.

The duration of the header in the preamble shall be limited to $n = 64$ during a search frame to ensure that the transmission is within the specified time slot.

NOTE 2 The synchronisation method differs from that of mode P of this European Standard, and mode S and mode R2 of EN 13757-4.

All chips of each frame, including optional wake-up signal, pre- and postamble shall form an uninterrupted bit sequence.

7.4 Data link layer protocol

7.4.1 General

The protocol used shall be symmetrical, i.e. the same formatting of the data is used independent of whether it is an upstream or a downstream data transfer.

7.4.2 Frame format

7.4.2.1 General

Two types of frames exist, a data frame and an acknowledge frame. The format of the frames shall be as specified in Figure 37.

L-field	DA-field	SA-field	FC-field	DLY-field	Data-field	FCS
1 byte	7 bytes	7 bytes	1 byte	2 bytes	n bytes	2 bytes

Data frame

L-field	DA-field	SA-field	FC-field	FCS
1 byte	7 bytes	7 bytes	1 byte	2 bytes

Acknowledge frame

Key
L-field the length field
DA-field the destination address
SA-field the source address
FC-field the frame control field
DLY-field the delay field, used for the dynamic delay calculation
Data-field data for network layer and application layer
FCS frame check sequence

Figure 37 — Data link layer frame formats

7.4.2.2 L-field

The L-field specifies the length of the frame in bytes. The length of the frames shall include the full frame, starting with the synchronisation pattern and including the FCS. The valid range of the L-field shall be 18 – 255.

7.4.2.3 SA- and DA-field

The length of the DA and SA-fields shall be 7 bytes. The SA field designates the data link layer address of the node sending a frame. The DA field designates the data link layer address of the node(s) to receive the frame.

The address may be one of the following four types:

— Device address, i.e. the address specifies a hardware address of a specific node. A device address is identified by the bits of the most significant byte of the address being 0xxx $xxxx_b$. Byte 4 and 5 of the address may have two formats. If the most significant bit of byte 5 is 1 then the format of the remainder of the two bytes is free. If the most significant bit of byte 5 is 0 then the remainder of the two bytes shall contain a user or manufacturer ID. This user or manufacturer ID shall be encoded as specified in EN 13757-3:2004, 5.5.

— Short form address, i.e. transmission of data with a partial address. This type of addressing is used when routing packet through multiple hops to conserve packet size. A short form address is identified by the bits of the most significant byte, byte 1, being 10xx $xxxx_b$ and byte 4 and 5 being FF FF_h. A node receiving a frame with a short form address shall process the frame if the reminder of byte 1 and byte 2 and 3 of the DA-field match the address mask of the node and byte 6 and 7 match a hardware address of the node. A node transmitting a frame shall set byte 1 to 10xx $xxxx_b$ and then insert its own address mask in the remainder of byte 1 and byte 2 and 3 and FF FF_h in byte 4 and 5.

— Multicast address, i.e. the address specifies a group of nodes that all shall receive the frame. A multicast address is identified by the bits of the most significant byte of the address being 11xx $xxxx_b$. A node receiving a frame with a multicast address shall process the frame if the remainder of byte 1 and byte 2 and 3 of the DA-field match the address mask of the node. Byte 4, 5, 6 and 7 of the DA-field are 'don't care' elements when receiving and shall be sent as FF FF FF FF_h.

— Broadcast address is a special version of the multicast address. It specifies that all nodes receiving this frame shall process the frame. The broadcast address is identified by all bits in the DA-field being 1, i.e a DA of FF FF FF FF FF_h.

A node shall support all four types of addresses.

A node shall, when replying with an acknowledge frame, use the actual source and destination address from the initial data frame as the destination and source addresses.

NOTE 1 A node may be multi-homed, i.e. it may respond to multiple device and short form addresses.

NOTE 2 The size of the address field has been chosen as a trade off between the size of the address space, and the amount of space in the frame used for address information, especially when routing multi-hop transmissions.

7.4.2.4 The FC-field

The FC-field is a 1 byte field. The format shall be as shown in Figure 38. It specifies how the frame shall be processed at the data link layer level. It contains the following sub-fields; where bit 7 is the most significant bit.

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2-0
Data	Acknowledge	Reserved	Direct	Search	Reserved

Key

Bit 7 Data frame. The bit shall be set to 1 when a data frame is transmitted, and shall be set to 0 when an acknowledge frame is transmitted.

Bit 6 Acknowledge at the data link layer. The bit shall be 0 in an acknowledge frame. The bit shall, in a data frame, be set to 1 when a acknowledge frame shall be sent back from the receiver(s). The bit shall in a data frame be set to 0 when the receiving node(s) shall not send an acknowledge frame. The transmitting node shall not wait for an acknowledge frame if this bit is 0.

NOTE Broad- and multicast frames should in general not be acknowledged.

Bit 5 Reserved for future use. The bit shall be set to 0 when transmitted, and shall be a 'don't care' bit during reception.

Bit 4 Direct connection indicator. The bit shall be 1 when the end nodes are communication directly without any intermediate nodes and without any other network layer information. The bit shall be 0 when the end nodes are performing a routed communication through intermediate nodes. The field of the network layer header shall not be implemented if the direct connection bit is 1.

Bit 3 Search for other nodes. This bit shall be 1 when the frames transmitted are a part of a 'search for known nodes' sequence. The bit shall be 0 for all other conditions.

Bit 2-0 Reserved for future use. The bit shall be set to 0 when transmitted, and shall be a 'don't care' bit during reception.

Figure 38 — FC field structure

7.4.2.5 The DLY field

This field shall only be present in a data frame. The DLY field holds information about the incremental delay of a frame, as it is being transmitted between nodes. The two bytes shall be interpreted as an unsigned integer. The integer value shall be the incremental delay of the frame, measured in msec. The incremental delay shall be the delay of the synch byte of a frame, relative to the time when the application layer data in the frame was generated in the sending end-node.

If the content of the DLY field has no valid value then it shall be set to FF FF_h during transmission and be 'don’t care' information during reception. If an overflow condition has occurred in the calculation of the DLY information, then the value shall be set to FF FE_h during transmission.

NOTE 1 The way to handle the reception of an overflow condition is outside the scope of this standard.

The incremental delay shall, for an initiating end node, be the delay from the time the packet was generated in the application layer to the time when the synch pattern is transmitted at the physical layer.

For an intermediate (routing) node, the delay from the time the synch pattern was received at the physical layer to the time when the synch pattern is to be transmitted again shall be added to the incremental delay value in the frame.

The manufacturer shall state the accuracy of the delay calculation of the product.

NOTE 2 The DLY field is information related to the application layer, but it cannot be calculated in advance. It can only be calculated on the fly. This is the reason of placing it in the data link layer header.

The value shall reflect whether or not a wake-up header is transmitted. The value shall be updated when a retransmission is performed. The value shall be updated for each intermediate node in a route.

7.4.2.6 The data field

This field shall only be present in a data frame. The data field holds information to be processed by the network layer and the application layer.

7.4.2.7 The FCS

The FCS or Frame Check Sequence ensures the integrity of the data. The FCS shall be the CRC-16 ($X^{16} + X^{12} + X^5 + 1$) as specified in RFC 1662. The FCS shall cover all information from the L-field to the data field (data)/FC field (acknowledge).

7.4.3 Normal data link layer frame handling

7.4.3.1 General

This subclause specifies the normal frame handling requirements at the data link layer level. The basic flow is that a transmitting node sends a data frame to a receiving node. The receiving node may then send an acknowledge frame.

7.4.3.2 Sending a data frame

A node shall, before initiating a data frame transmission, receive on the selected channel, and ensure that the activation of a transmission isn't blocking another ongoing transmission. See Table 14, Idle detect.

A node should, when sending an initial multicast or broadcast frame, prepend the data frame with a wake-up signal.

The sending node shall, when sending a routed frame, initially send the frame without a leading wake-up signal.

A node shall, when a frame is retransmitted due to timeout, resend the frame with a leading wake-up signal.

A node shall, if the transmission hasn't succeeded after 4 attempts, pass information on this to the upper layers.

7.4.3.3 Sending an acknowledge frame

The receiving node shall, if the acknowledge bit in the FC field is 1, send an acknowledge frame. The acknowledge frame shall be sent with the acknowledge and time info bits of the FC field set to 0. There shall be no DLY or data field in an acknowledge frame.

NOTE 1 There is no capability of returning a 'non- acknowledge' frame. Non-acknowledge is handled by using time-out.

An acknowledge frame shall be sent without a leading wake-up signal.

NOTE 2 This is a reply to a node that recently sent a data frame, and the node should still be powered and active.

7.4.3.4 Receiving a data frame

When receiving a data frame, the following shall apply:

a) the node shall drop the frame, if the destination address isn't one of the addresses of the node;

b) the node shall drop the frame if the FCS of the frame fails.

7.4.3.5 Receiving an acknowledge frame

When receiving an acknowledge frame, the following shall apply:

a) the node shall drop the frame, if the destination address isn't the source address from the corresponding data frame;

b) the node shall drop the frame if the FCS fails;

c) the node shall, if all of the above tests are passed, pass the acknowledge information on to the network layer, without error status;

NOTE The node may use other means than an acknowledge frame, as the detection of the correct reception of a data frame.

d) the manufacturer of a node shall state any alternative methods used to detect the acknowledgement of a data frame.

7.4.3.6 Normal timing requirements

The timing requirements specified here are all at the link layer level:

a) the timing parameters referenced in this subclause shall be as specified in Table 14 and Table 15;

b) a node shall, when sending an acknowledge frame, not start the reply before the minimum value of t_{AD};

NOTE 1 This ensures that the receiver in the former transmitting node is able to settle before the message is received.

c) a node shall, when sending an acknowledge frame, start the reply within the maximum value of t_{AD} after the end of the data frame;

d) a node expecting an acknowledge frame shall timeout the transfer if no data has been received within the maximum value of t_{AT}. Timeout may generate a retransmission as specified in 7.4.3.2.

NOTE 2 Timing of requests and responses are handled at the application layer.

7.4.4 Search link layer frame handling

7.4.4.1 General

Special link layer frame handling shall be used when searching for known nodes.

A node will activate the search when it receives a 'Generate known nodes' request, see 7.6.5.4. When searching for known nodes some special conditions shall be present:

a) all nodes (to be interrogated) shall have an internal flag 'has replied' that hold the state about whether or not the node shall respond to the search request;

b) multicast or broadcast and direct connection (without a network layer) shall be used;

c) the nodes shall not respond immediately but in different time slots;

d) the format of the frames differs slightly from the format used for normal data transfer.

7.4.4.2 Frame formats

The command from the searching node shall be framed in a normal data link layer data frame. The frame shall be a multi- or broadcast frame. The frame shall be sent with a wake-up signal. The FC field of the frame shall be set to 1001 0000_b. The data field of the frame shall have the format as specified in Figure 39.

Search Control	Target SNR	Address list
1 byte	1 byte	N × 7 bytes

Key

Search control — Control byte with the following fields

- Bit 7 — 0 = no activity, 1 = initiate search
- Bit 6-0 — reserved for future use, shall be 0 during transmission and don't care during reception

Target SNR — target signal to noise ration threshold in the receiver, expressed in dB

Address list — list of nodes already registered

Figure 39 — Search request data field format

The nodes responding shall reply with a normal link layer data frame. The frame shall be a point-to-point frame. The FC field shall be set to 1001 0000_b. The data field of the frame shall have the format as specified in Figure 40.

SNR level
1 byte

Key

SNR level — signal to noise ration of the signal when receiving the request

Figure 40 — Search response data field format

7.4.4.3 Search sequencing

The sequencing of the search for known nodes shall be as follows:

a) The requesting node shall send the initial search request. The 'initiate search' bit of 'search control' shall be set. The target SNR shall be set to the first value in the SNR-list from the 'generate known nodes list' commands, see 7.6.5.3. The device address of any nodes that shall not reply to the search shall be included in the address list.

b) The surrounding nodes shall read the request. They shall terminate the processing of the request and drop the frame if the signal to noise ratio of the received signal is less that the target SNR. They shall clear their internal 'has replied' flag if the 'initiate search' bit in the request is set. They shall set their internal 'has replied' flag if their device address is included in the address list of the request. They shall, if their internal 'has replied' flag is cleared, select a random reply time slot and reply with a response, formatted as specified above.

c) The requesting node shall collect the information from the different time slots. It shall for each new response store the device address and the bidirectional SNR for the connection. The composite SNR is the minimum of the SNR returned by the responding node, and the measured SNR of the received frame. It shall, if new responses are received, not update the target SNR values. It shall, if no responses from new nodes are received, update the target SNR value to the next (lower) value in the SNR-list. The requesting node may set the 'initiate search' bit in a second cycle, but shall clear the 'initiate search' bit in subsequent cycles. The address list shall be updated to contain the device addresses of the devices detected in this cycle. After this, the node shall send a new request.

NOTE Experience has shown that there may be a big difference in SNR in the two directions. The quality of a link is no better than the worst case SNR of the link. Therefore the minimum of the two SNRs should be used.

d) The surrounding addressed nodes shall process the second and following request as in b).

e) The requesting node shall terminate the cycle when a request with either target SNR of 0 or with the fifth value from the SNR-list has been performed more than 'stop condition' times.

7.4.4.4 Search timing requirements

The timing requirements for the search link layer actions are specified in Table 16.

Table 16 — Search timing

Characteristic	Symbol	Min.	Typ	Max.	Unit
Number of time slots	N_{TS}		24		
Duration of time slot	t_{TS}	118	120	122	ms
Response within time slot	t_{TR}	20		30	ms
Cycle time	t_{TC}	3 500		5 000	ms

7.5 Mode Q, network layer protocol

7.5.1 General

This network layer protocol shall only be used together with the mode Q link layer.

The presence in the data link layer of bit 7 in the FC-field of 1 specifies that higher layer data follows. This is network layer and application layer information.

The presence in the data link layer of bit 4 in the FC-field of 1 specifies that a direct connection is used, that no network layer is used and that the network header shall be empty.

The network layer supports the routing of packets through a network on a hop-by-hop basis. The maximal route length supported is 10 hops.

NOTE 10 hops correspond to 11 nodes in all, and 9 intermediate nodes.

The structure of the network layer information and the network layer protocol are specified in the following.

7.5.2 Network layer format

7.5.2.1 General

The format of the network layer information, a packet, is the network layer header and the application layer data. The network layer header is mainly a list of intermediate nodes to route through. The format shall be specified in Figure 41.

NCtrl	TID	Destin.	Source	TTL	SNR	Nodes	Current	Addr. List	App. data
1 byte	1 byte	7 bytes	7 bytes	1 byte	1 byte	1 byte	1 byte	m × 2 bytes	n bytes

Key
NCtrl Network control
TID Transfer identification
Destin. Destination address, end node
Source Source address, end node
TTL Time to live
SNR Signal to noise ratio
Nodes Total number of nodes involved, number of hops + 1
Current Current node
Addr.List List of addresses of nodes
App. data Application layer data

Figure 41 — Network Layer information format

Data in a network layer packet shall not be moved around as data are transferred through the network. The only fields that shall be modified for each hop are the time to live and current hop fields.

7.5.2.2 Network control

The network control field is a bit mapped one byte field. It specifies additional information at the network layer level. The bit positions inside the field are defined in Figure 42.

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Res. = 0	Req./resp.	Error	Agg. SNR	Res. = 0	Res. = 0	Res. = 0	Res. = 0

Figure 42 — Network control field structure

Positions marked as ‘Res.’ in the figure above are reserved for future use and shall have a reserved value as specified.

Request/Response, bit number 6, is the request/response indicator. The bit shall be 1 when data is transmitted downstream, i.e. in the direction from the data collecting unit to the meter. Data sent in this direction is a ‘request’. The bit shall be 0 when data are transmitted upstream, i.e. in the direction from the meter to the data collecting unit. Data sent in this direction is a ‘response’.

Error indicator, bit number 5: the bit shall be 1 in messages containing error information. It shall be 0 in all other messages.

Agg. SNR, bit number 4: this bit specifies the way the signal to noise ratio for a route is to/has been measured. The bit shall be set to 1 if the SNR aggregated i.e. the worst case (minimum) value detected along the route. The bit shall be set to 0 if the SNR reported is the SNR measured on the hop most downstream on the route, i.e. closest to the metering unit.

NOTE Measuring SNR for the individual hops makes it possible to achieve a better knowledge of the routing capabilities in the network.

7.5.2.3 Transfer identification

The transfer identification is a one byte field interpreted as an unsigned integer. It is generated by the end node initiating a request (the data collection unit). It is incremented for each new request sent to the network. End nodes initiating a response to a request shall copy the transfer identification into the response. The value 0 for the TID shall not be used for a normal application layer request/response. End nodes initiating un-requested messages shall use a TID of 0.

NOTE The use of a transfer identification makes it possible to detect and filter out duplicated packets at the network layer and makes it possible for the application to link the response to a specific request.

7.5.2.4 Destination address

This is the address of the receiving end node. The structure of this address shall be as specified in 7.4.2.3. This shall identify the receiver of the message at the application layer level.

7.5.2.5 Source address

This is the address of the initiating end node. The structure of this address shall be as specified in 7.4.2.3. This shall identify the sender of the message at the application layer level.

7.5.2.6 Time to live

The 'TTL' field is a one byte field. It is a ‘timeout’ function at the network level. It shall be interpreted as an unsigned integer. It shall be in the range 1 to 10. The use of this field is specified in 7.5.4.

7.5.2.7 Signal to noise ratio

The SNR field is a one byte field. It shall be interpreted as an unsigned integer. It is reserved for network management purpose. It is used for collecting information about the signal to noise ratio in the network. A large value shall indicate a high signal to noise ratio and a low value a low signal to noise ratio. The value should be the actually measured signal to noise ratio in dB on the most recently received data frame.

The capability of measuring the SNR should be implemented in a node. The manufacturer shall state whether or not this capability is implemented in a node. The manufacturer shall, if the capability is implemented, state how to interpret the value. Nodes not implementing this capability shall use a default value of 255.

SNR shall be measured bidirectionally, i.e. both in the upstream and in the downstream direction.

An end node receiving a data frame shall record the measured SNR of the transmission.

If bit 4 of the network control field is 1, then the node shall compare the measured value to the value in the received data frame. The value in the data frame shall be updated with the recorded value if the recorded value is less than the received value, i.e. a worst case value is generated.

If bit 4 of the network control field is 0, the transfer is in the upstream direction, and the hop isn't the most downstream hop in the route, then the node shall just pass on the current value in the data frame.

If bit 4 of the network control field is 0, and the hop is the most downstream hop in the route, then the node shall update the value in the data frame to the measured value.

7.5.2.8 Nodes

The 'Nodes' field is a one byte field. It shall be interpreted as an unsigned integer. The value designates the total number of nodes in the route, excluding the end nodes. The value shall be in the range 0 to 9. The use of this bit is specified in 7.5.4. End nodes responding to a request shall copy the value into the response.

NOTE A value of 0 corresponds to a direct connection between two end nodes.

7.5.2.9 Current

The 'Current' field is a one byte field. It shall be interpreted as an unsigned integer. The value designates the current sending node in the routing from end node to end node. The value shall be in the range 0 to 10. It is a pointer into the address list. The use of this field is specified in 7.5.4.

The value shall, when sending downstream, be set to 1 by the initiating end node (the data collecting unit) and be incremented for each hop by the intermediate nodes. The value shall, when sending upstream, be set to 'Nodes' by the initiating end node (the meter) and be decremented for each hop by the intermediate nodes.

NOTE This makes it possible to have a static address list of routes, independent of the direction of the transfer.

7.5.2.10 Address list

This field is a sequence of 2 byte fields. The number of fields shall be equal to the value of the nodes field. Each 2 byte field is an abbreviated form of the full 7 byte address of a node. The conversion from 2 byte to 7 byte format is specified in section 7.5.3. The first element in the list shall be the abbreviated address of the routing node closest to the upstream end node. The last element in the list shall be the abbreviated address of the routing node closest to the downstream end node.

NOTE This list may be empty if two end nodes communicate directly.

7.5.3 Address conversion rules

Node addresses exists in a full and in an abbreviated form. The full address is a 7 byte field. An abbreviated address is a 2 byte field. A full address may be converted to an abbreviated address and an abbreviated address may be converted to a special full address named a short form address.

An abbreviated address shall be generated from a full address by extracting the two least significant bytes of the full address.

A short form address shall be generated by prepending to the abbreviated address with a 5 byte address. The first byte (most significant) shall have the form $10xx\ xxxx_b$. This shall be followed by the address mask of the node (in bytes 1, 2 and 3). Byte 4 and 5 shall be $FF\ FF_h$. See 7.4.2.3 for more information.

A multi-homed node can have multiple address masks. A multi-homed node shall use the address mask matching when receiving as the address mask used when transmitting the data to the next node.

An initiating node shall use the address mask of the source address.

7.5.4 Routing rules

7.5.4.1 General

These are the rules to be used when handling information at the network layer, and the rules to be used when passing information from the network layer to the link layer. The rules are specified for the individual types of nodes. An initiating end node starts the transfer to a receiving end node. The transfer may pass through a number of intermediate nodes on its route from one end node to another end node.

The structure used is a master/slave structure, i.e. a central node will request information from peripheral nodes, and the peripheral nodes will then revert with a response. There is aside of that a special mode, unsolicited response, where a peripheral node will send information to the central node, without any prior request. This mode may be used when sending alarms and when initially connecting to the network.

NOTE This subclause is not applicable to nodes using a non-routed transfer, i.e. a direct connection.

7.5.4.2 Rules for an initiating node

a) The fields 'NCtrl', 'TID', 'Source', 'Destin.', 'Nodes' and 'Addr. List' shall only be modified by the initiating node. Other nodes shall not modify these fields.

b) The setting of the 'TID' field depends on the direction of transmission and the type of message:

1) the 'TID' field shall, when the transfer is in the downstream direction, be set to a value that is incremented for each new transfer, typically a new request; the value assigned shall skip over the 0 value;
2) the 'TID' field shall, when the transfer is in the upstream direction and the message is a response, be set to the value from the corresponding request;

NOTE 1 This makes it possible for the application layer to relate request and responses.

3) the 'TID' field shall, when the transfer is in the upstream direction and the message is an unsolicited response, be set to 0.

c) The 'Source' field shall be set to a device address of the initiating node.

NOTE 2 A node may be multi-homed and support multiple device addresses. The selection amongst the device addresses of a node is outside the scope of this standard.

d) The 'Destin.' field shall be set to a device address of the end node to receive the data.

e) The 'TTL' field shall be set to the total number of hops on the route between the end nodes.

f) The 'SNR' field shall, if the transmission is in the downstream direction, be set to 255. The 'SNR' field shall, if the transmission is in the upstream direction, be set to the 'SNR' of the corresponding request. The 'SNR' field shall, if the information is an unsolicited response, be set to 255.

g) The 'Nodes' field shall be set to the number intermediate nodes in the route, excluding the end nodes.

NOTE 3 This value is equal to ‘number of hops – 1'.

h) The 'Current' field shall, if the transfer is in the downstream direction, be set to 1 by the initiating node. The 'Current' field shall, if the transfer is in the upstream direction, be set to ‘nodes’ by the initiating node.

i) The 'Addr. List' shall contain a list of the abbreviated addresses of the intermediate nodes in the route. The order of the elements shall be the order of the nodes when routing in the downstream direction.

NOTE 4 The list is, if a response is to be generated, available from the foregoing request.

j) The network layer shall transfer a device address of the node to the link layer as the SA-field.

k) The DA-field of the link layer shall be set to 'Source' if 'Current' = 0. The DA-field of the link layer shall be set to 'Destin.' if 'Current' = 'Nodes' + 1. Otherwise the network layer shall use 'Current' as a pointer to the ‘Addr. List’. The link layer DA-field shall be set to the element pointed to in the ‘Addr. List’ and converted to a short form address.

7.5.4.3 Rules for receiving routed frames

The network layer shall process routed packets received from the link layer in the following way:

a) If an error condition is received from the link layer, then this information shall be passed on to the application layer.

b) If the TTL field is 0 then an error condition shall be generated and passed on to the application layer, else the TTL field shall be decremented by 1.

c) If the end of the route has been reached and the destination field is equal to a device address of the node then:

   1) the application data shall be passed to the application layer;
   2) if the message is a request (network control bit 6 is 1) then the 'TID', ' 'Source', 'SNR', 'Nodes' and 'Addr. List' shall be stored for later use;
   3) no further processing of this packet shall be performed in the network layer.

NOTE End of route may be detected in one of the following ways:

— TTL = 0;

— transmission is in the downstream direction and 'Current' = 'Nodes' + 1;

— transmission is in the upward direction and 'Current' = 0.

d) If the end of the route has been reached and the 'Destin.' field isn't equal to a device address, then an error condition shall be generated and passed on to the application layer.

e) If the end of the route hasn't been reached then the processing shall be continued with the rules for intermediate nodes.

7.5.4.4 Rules for receiving direct connection frames

Alarm and error condition may generate frames with the direct bit set in the FC field. Such frames shall be processed in the following way.

The node shall, if the frame is the reporting of an alarm or error and a route to and upstream end node exists, send the data as routed frame. The application layer data of this frame shall be the full 'direct' application data as the data information.

The frame shall be discarded if no route exists or if the routing fails.

The node shall, if it is a searchframe, handle the frame as specified in 7.6.5.3.

NOTE Direct connection is used for unsolicited responses and generation of the known nodes list. Unsolicited responses can be alarm or error reporting, see 7.6.3 and 7.6.4.

7.5.4.5 Rules for intermediate nodes

The network layer of an intermediate node shall, in addition to the rules for receiving nodes, process data from the link layer in the following way:

a) It shall process the 'SNR' as specified in 7.5.2.7.

b) The 'Current' field shall, if the data transfer is in the downstream direction, be incremented by 1 and, if the transfer is in the upstream direction, be decremented by 1.

c) The network layer shall transfer a device address of the node to the link layer as the SA-field.

d) The network layer shall, if 'Current' = 0, transfer 'Source' to the link layer as the DA-field. The network layer shall, if 'Current' = 'Nodes' + 1, transfer 'Destination' to the link layer as the DA-field. Otherwise the network layer shall use 'Current' as a pointer to the ‘Address list’. The link layer DA-field shall then be set to the element pointed to in the ‘Address list’ and converted to a short form address.

The intermediate nodes shall also update the dynamic delay field as a part of the routing. This is specified in 7.4.2.5.

7.5.4.6 Rules for sending unsolicited responses

The network layer of a node that tries to send an unsolicited response shall process the information in the following way.

A node shall, if a specific route for unsolicited responses is stored in the node, use this route and process the information following the rules for an initiating node.

A node should, if no specific route is stored, but a route to an upstream end node from a previous transfer is recorded/available, use this route and process the information following the rules for an initiating node.

A node should, if no route to an upstream end node is available, broadcast or multicast the frame using direct communication, see 7.4.2.4.

7.5.5 Timing requirements

This subclause specifies timing requirements specific to the network layer. The requirements are listed in Table 17.

Table 17 — Network routing timing

Characteristic	Type	Sym	Min.	Typ	Max.	Unit	
Routing delay [a]	t_{RO}				150	ms	

[a] Routing delay: after receiving a packet that shall be forwarded, the node shall start forwarding the packet onto the next hop in less than the maximum routing delay.

7.6 Mode Q, application layer protocol

7.6.1 General

The format of application layer data is as specified below. The application layer data may contain multiple sets of application layer requests/responses. Each set of application layer data is TLV encoded. The format of application layer information is specified in Figure 43.

Tag 1	Length 1	Value 1	Tag 2	Length 2	Value 2	Tag n	Length n	Value n
1 byte	1 byte	N bytes	1 byte	1 byte	M bytes	1 byte	1 bytes	P bytes

Figure 43 — Application layer information format

NOTE 1 TLV is a standard abbreviation for Tag – Length – Value encoding.

The tag specifies the type of information, the length field specifies the length of the value field and the value field holds the actual information.

The tag field of a data set specifies the type of application data that follows. The current standard does not in general specify the types of applications in the application layer. Only some functions related to the management of the network are defined. Certain values have been reserved for compatibility with existing standards in EN 13757-1, EN 13757-3 and EN 13757-4 family of standards.

NOTE 2 The availability of transfer of multiple requests in a single frame may cause the response to be larger than supported by the frame size. This will cause an error condition. Handling of such conditions is outside the scope of this standard.

Table 18 — Application layer, tag field

Tag value	Designation	Remarks
00_h – $1F_h$	Reserved	Compatible with EN 13757-1
20_h – $6F_h$	Reserved	Reserved for future use
70_h	Error reporting	Compatible with EN 13757-3
71_h	Alarm reporting	Compatible with EN 13757-3
72_h – $7F_h$	Application layer information	Compatible with EN 13757-4
81_h – 82_h	Reserved	To avoid overlap with mode P of the current standard
83_h	Network management	Application layer functionality to support the management of the network layer and lower layers.
$A0_h$– FF_h	Manufacturer specific information	To be used for manufacturer specific application layer

The error bit in the network control field of the network layer header shall be set when an alarm or an error type data set is transferred. See 7.5.2.2 for further details.

7.6.2 EN 13757-1 Application layer

A node supporting an EN 13757-1 application layer shall have a tag field of 01_h. The application layer data shall be prepended with a transport sub-layer consisting of CI, STSAP and DTSAP as specified in EN 13757-1:2002, 10.2.3.

The encoding of the application layer data shall follow the requirements as specified in EN 13757-1:2002, 10.3.

A node supporting an EN 13757-1 application layer shall be able to receive error reporting, alarm reporting and network management data prepended with a transport sub-layer, as specified above. A node supporting an EN 13757-1 application layer may send error reporting, alarm reporting and network management data prepended with a transport sub-layer, as specified above.

7.6.3 Error reporting

7.6.3.1 General

Error reporting is to be used when a node for some reason cannot provide a requested response. This may be an intermediate node as well as an end node.

A routing node shall contain an error reporting service. The node shall use the service to return error status information. Error information returned shall use a tag field of 70_h. The first byte of the value field is a one byte type.

The error bit of the control field in the network layer header shall also be set as stated in 7.5.2.2.

The type field may have the values as defined in Table 19.

Table 19 — Type field, error status information

Type value	Designation	Remarks
00_h	Unspecified	Unspecified error, compatible with EN 13757-3
01_h	No application	Unimplemented tag field
02_h – 09_h	Application error	Compatible with EN 13757-3
$0A_h$ – 10_h	Reserved	
11_h	No mgmt. function	Function not implemented in network management
12_h	Data error	Data to be supplied are not available
13_h	Routing error	Cannot route data further
14_h	Access violation	Data access right violation
15_h	Parameter error	Error in the parameters supplied in the request
16_h	Size error	The amount of data requested cannot be handled
17_h – BF_h	Reserved	Reserved for future use
$C0_h$ – FF_h	Manuf.	Manufacturer specific error information

7.6.3.2 No application

This error status shall be returned by the application layer, if the requested application tag field isn't implemented in the node. The type field shall be followed by a copy of the incorrect tag field.

7.6.3.3 Application error

This type of error codes may be used if an EN 13757-3 application layer is implemented.

7.6.3.4 No mgmt. function

This error status shall be returned by the application layer if the requested network management function isn’t implemented in the actual application layer. The type field shall be followed by a copy of the not implemented function field.

7.6.3.5 Data error

This error status shall be returned by the application layer if the request is correct, but the data cannot be provided by the application layer in the response.

7.6.3.6 Routing error

This error status shall be returned by the application layer if the node cannot forward data downstream to the next node. The format of the data returned shall be as shown in Figure 44.

Type	Status	TID	Ctrl	Source	Destin.	TTL	SNR	Nodes	Curr.	Addr. List
13_h	1 byte	1 byte	1 byte	7 bytes	7 bytes	1 byte	1 byte	1 byte	1 byte	M × 2 bytes

Key

Type — 13_h indication routing error

Status — Enumerated, showing status of an attempt

0 no response from node, timeout four times
1 node reacts, but with error in answer

TID, Ctrl, Source, Destin, TTL — Copies of the network layer header information in the frame that cannot be routed. See 7.5.2.1 for detailed information on these fields

SNR — If the node supports SNR measurement, then this field shall contain the SNR received by the node while trying to route the frame. The SNR shall be FF_h if the SNR measurement isn't supported, or 00_h if a timeout condition occurred

Nodes, Curr, Addr.List — Copies of the network layer header information from the frame that cannot be routed. See 7.5.2.1 for detailed information on these fields

Figure 44 — Routing error format

The data returned shows the frame that cannot be routed. It contains a header followed by the network layer header of the data that can't be routed.

The network layer of an initiating node shall not generate a routing error if it cannot send a message, but just return the error status to its own application layer.

7.6.3.7 Access violation

This type of error status shall be returned by the application layer if the request isn't allowed to access the data requested. This may be due to an incorrect access code.

7.6.3.8 Parameter error

This error status shall be returned by the application layer if parameters in the request are outside the current valid range.

7.6.3.9 Size error

This error status shall be returned by the application layer if the request is correct, but the total data in the corresponding response cannot be handled inside a single frame.

7.6.4 Alarm reporting

7.6.4.1 General

Alarm reporting is to be used when a node has critical information for the central node that will not be requested. Alarm reporting should be sent as an unsolicited response.

NOTE The error bit of the network control field in the network layer header should also be set as stated in 7.4.2.2.

A routing node should contain an alarm reporting service. The node shall use the service to return persistent alarm conditions. Alarm information returned shall use a tag field of 71_h. The first byte of the value field is a one byte type field. The format of the data shall be as shown in Figure 45.

Type	Application data
XX_h	Further alarm information
1 byte	n bytes

Figure 45 — Alarm information data format

The type field may have the values as defined in Table 20.

Table 20 — Type field, alarm information

Type value	Designation	Remarks
00_h	General error	The overall status of the node
01_h	Installation	The node is in an uninstalled mode
02_h – 09_h	Application error	Compatible with EN 13757-3
$0A_h$ – 10_h	Reserved	
$C0_h$ – FF_h	Manufact.	Manufacturer specific type of alarms

7.6.4.2 General error

This function shall be used by a node to signal that an alarm condition has existed for a prolonged time without being serviced. The condition has caused the node to stop its normal function (consumption counting).

The manufacturer shall state the conditions that will cause a node to generate such errors.

7.6.4.3 Installation mode

This function shall be used by a node to signal that it is in installation mode, i.e. not configured. A node may revert to installation mode when it for a prolonged time isn't able to communicate with the network.

The procedure to use during installation mode is outside the scope of this standard.

The manufacturer shall state the conditions that will cause a node to revert back to installation mode.

7.6.5 Network management service

7.6.5.1 General

A routing node shall contain a network management application. Data shall be passed on to the network management application whenever the tag field is 83_h. The general format shall be as specified in Figure 46. The first byte of the value field is a one byte function type field that defines the way data shall be interpreted.

Type of function	Application data
XX_h	Function specific information
1 byte	x byte

Figure 46 — Network management data format

The functions listed in the table below covers the following generic network management requirements:

- There will be a demand for precision time tagging of information the nodes as there is a drift of the real time clock in the nodes. It shall thus be possible to set the time in the nodes. This time setting shall include corrections for the delay in any intermediate nodes.
- It shall be possible to generate and retrieve a list of the nodes that a routing node is able to receive data from, in order to set up the proper routes/transmission paths.
- It shall be possible to pass on information about failures in the relaying of information through routing nodes. Two situations exist: failure in the transfer downstream and failure in the transfer upstream. The purpose of such error messages is to be able to detect failing link in order to maintain an efficient and robust data transfer network.

The type field may have the values as defined in Table 21.

Table 21 — Types of network management functions

Type	Designation	Remarks
01_h	Time sync	Time synchronisation signal
13_h	Generate known nodes list	Start generating a list of network nodes known to the node
14_h	Get known nodes list	Submit a list of network nodes know to the node
21_h	Relaying status	Request and return of message on any previous failing upstream relaying
22_h	Wait	Cannot provide data yet, try again later
80_h - FF_h	Manufact.	Manufacturer specific type of functions

Values of type in the range 00_h to $7F_h$ are for standardised use. Values, in this range, not listed in the table above are reserved for future use (RFU) and shall not be used. Values in the range 80_h to FF_h may be used for manufacturer specific functions.

For the type of commands listed above the format for the application data following the type and the corresponding functionality is listed below.

7.6.5.2 Time sync

This function is used when the primary station, the data collection unit, wants to synchronise the time in the nodes it receive data from. The format of the request shall be as specified in Figure 47.

NOTE 1 This request may be sent using broadcast or multicast addresses.

Type	Year	Month	Day	Hour	Min	Sec	Time Zone	Acc.Ctrl
01_h	1 byte	1 byte	1 byte	1 byte	1 byte	1 byte	1 byte	4 bytes (opt)

Key

Type 01_h indicating time sync

Year 1 byte, unsigned integer, years since 2000, range 5 to 99

Month 1 byte, unsigned integer, range 1 to 12

Day 1 byte, unsigned integer range, 1 to 31

Hour 1 byte, unsigned integer, range 0 to 23

Min 1 byte, unsigned integer, range 0 to 59

Sec 1 byte, unsigned integer, range 0 to 59

Time Zone 1 byte signed, range - 12 to 12, offset relative to UTC

NOTE 2 This makes it possible to handle time zones and Daylight Saving Time.

Access Ctrl 4 bytes, optional, shall be present if the node uses access control on this request; the algorithm to use for access control is outside the scope of the current standard.

Figure 47 — Time sync request format

The initiating node shall ensure that the time-info bit of the FC-field at the link layer is set and shall insert a value into the DLY field at the link layer. The value shall correspond to the delay from the time the clock value was read from the clock source and until the sync sequence in the preamble is transmitted.

Any intermediate node shall, to the current value of the DLY-field at the link layer, add the delay from detecting the sync sequence in the preamble during reception to the transmission of the sync sequence on the next hop.

The format of the response shall as specified in Figure 48.

Type	Offset
01_h	1 byte

Key

Type 01_h indicating Time sync

Offset 1 byte, time offset, this is the numerical value of offset in seconds between the time from the internal clock in device and the time in the command, taking dynamic delay into account. The signal may be used as a quality indicator of the stability and drift of the clock on the device. The offset shall be set to '255' if the actual offset is larger than 255.

Figure 48 — Time sync response format

The manufacturer shall state the precision of the delay calculation in initiating as well as in intermediate nodes.

7.6.5.3 Generate known nodes list

This is the network management request to use or to activate a search for neighbour nodes that can be heard.

The format of the request shall be as specified in Figure 49:

Type	SNR-list	Stop cond.	Access Control
13_h	5 bytes	1 byte	4 bytes (optional)

Key

Type 13_h indicating generate known nodes list

SNR-list 5 bytes, signal to noise ratio list, a list 5 of threshold values to use in the search. Each value is a detection threshold for the signal to noise ratio. The threshold values shall be listed in descending order. If less than 5 thresholds are used, then the non-used values shall be 0.

Stop.cond. 1 byte, stop condition, number of times the last search for nodes shall be performed, without getting a response from a node, range 1 to 6

Access Ctrl 4 byte, optional, shall be present if the node uses access control on this request; the algorithm to use for access control is outside the scope of the current standard.

Figure 49 — Generate known nodes list request format

The way to react to this command is specified in 7.4.4.

The format of the response shall be as specified in Figure 50:

Type	Num. nodes
13_h	1 byte

Key

Type 01_h indicating generate known nodes

Num.nodes 1 byte, number of nodes detected during the search

Figure 50 — Time sync response format

The algorithm to use to generate the SNR-list is outside the scope of the current standard.

7.6.5.4 Get known nodes list

This is the network management request to use to retrieve a list of known nodes from a specific node. The format of the request as well as the response shall be as listed below.

The format of the request shall be as specified in Figure 51.

Type	Pointer
14_h	1 byte

Key

Type 14_h indicating get known nodes

Pointer 1 byte, indicating where to read data from; a value of 1 shall be used to get data from the start of the list.

Figure 51 — Get known nodes request format

The format of the response shall be as specified in Figure 52.

Type	Pointer	Node Info1	...	Node Info n
14_h	1 byte	8 bytes		8 bytes

Key

Pointer 1 byte, indicating where to read next block of data from. A value of 0 shall be returned when all data has been read. Using the pointer returned as parameter in the next request shall return the subsequent block of data. The algorithm used to generate this pointer is outside the scope of this standard.

Node Info 8 bytes with the following content

Address 7 bytes, a device address of the node, i.e. the source address detected at the link layer level

SNR 1 byte, range 0 to 255, the signal to noise ratio in dB measured during the most recent node search sequence

Figure 52 — Get known nodes response format

7.6.5.5 Relaying status

An error while transferring data upstream is at the same time a fault in the transmission path for information. This inhibits the transfer of information to the central node. If this condition occurs, then the router should store the error status locally and await restoration of the transmission path.

Upstream data transfer is normally the response to a request. The central node will detect the missing response and shall retry the request. The central node shall if this fails try to establish an alternate transmission path to this node.

A routing node may, if the error condition remains for a prolonged time, switch back to installation mode. See 7.6.4.3 for further details.

NOTE 1 The mechanism for storing the error status locally and for establishing alternate transmission paths is outside the scope of this standard.

Once the transmission path has been re-established the information about the error condition may be retrieved by the central node. The format of a relaying error status, the request as well as the response is listed below.

If implemented, the format of a relaying error status request shall be as specified in Figure 53.

Type	Modifier
21_h	1 byte

Key

Type 21_h indicating relaying status

Modifier 1 byte, with bit fields

Bit 7 0 = return first block from list
1 = return subsequent block from list

Bit 6..0 0, reserved for future use

Figure 53 — Relaying status request format

This error status should be available from the application layer if the node cannot forward data upstream to the next node. The format of the data returned shall be as shown in Figure 54. One set of error information shall be returned for each request.

Type	Status	NCtrl	TID	Destin.	Source	TTL	SNR	Nodes	Curr.	Addr. List
21_h	1 byte	1 byte	1 byte	7 bytes	7 bytes	1 byte	1 byte	1 byte	1 byte	m×2 bytes

Key

Type 21 $_h$ indication relaying status

Status 1 byte, enumerated, showing status of attempt

- 0 no response from node, timeout three times
- 1 node reacts, but with error in answer
- 2 no pending errors

NCtrl, TID, Destin., Source, TTL, SNR, Nodes, Curr. and Addr. List

Copies of the network layer header information in the frame that cannot be routed. See 7.5.2 for detailed information on these fields.

Figure 54 — Routing error format

The data returned shows the frame that cannot be routed. It contains a header followed by the network layer header of the data that cannot be routed.

A 'Status' of 02 $_h$ and no further data shall be returned if no error condition information has been recorded.

NOTE 2 The number and structure of error data stored in the node for later retrieval is outside the scope of this standard.

7.6.5.6 Wait extension

Certain request at the application layer may have a long response time. This could cause timeout at the application layer with following retransmissions. To limit the number of timeout conditions, the wait extension response has been introduced. A node that has received a request may return a wait extension response. This indicates that the node isn't able to respond yet and that the request will be returned at a later time. A wait extension response shall only be sent from an end node. The format of the response shall be as specified in Figure 55.

F-field
22_h

Key

F-field 22 $_h$ indicating the wait extension request

Figure 55 — Wait extension response format

The wait extension response shall be sent with a 'TID' of 0. The node sending the wait extension response shall reply with the actual response without further requests. This response shall use the original TID.

The manufacturer shall, for nodes implementing wait extension, state the maximum response time after a wait extension.

7.6.6 Timing requirements

The timing requirements that shall apply at the application layer level are listed in Table 22.

Table 22 — Application layer timing

Characteristic	Symbol	Min.	Typ	Max.	Unit
Response delay [a]	t_{RD}	20		10 000	ms
Response wait [b]	t_{RW}			21 000	ms

[a] Response delay: after receiving a request, the node shall not start sending the response back in less than the minimum response delay and shall start sending the response back in less than the maximum response delay.

[b] Response wait: after sending a request and expecting a response, a node shall, at the application layer, not time out the connection in less than the maximum response wait time. The maximum value takes into account that a wake-up signal must be sent to some of the nodes. The maximum value may be extended, after agreement with the operator.

7.6.7 COSEM extension

7.6.7.1 Introduction

It has been recognised that there is a need for some new dedicated interface classes when new lower layer and new functionalities are added.

7.6.7.2 Wireless Mode Q Channel, interface class

Instances of this interface class define the operational parameters for communication using the mode Q interfaces. The attributes and their use is defined in Table 23 and Table 24 below.

Table 23 — Interface class description

Wireless Mode Q Channel		**0..*n***	**class_id = 73, version = 1**		
Attribute(s)		***Data Type***	***Min.***	***Max.***	***Def.***
1. logical_name	(static)	octet-string			
2. addr_state	(static)	enum			
3. device_address	(static)	octet-string			
4. address_mask	(static)	octet-string			
Specific Method(s)		***m/o***			

Table 24 — Class attribute description

Attribute description

addr_state	Defines whether or not the device has been assigned an address since last power up of the device enum (0) not assigned an address yet (1) assigned an address either by manual setting or by automated method
bus_address	The currently assigned address of the device on the network octet-string
address_mask	The group address the device will respond to when short form addressing is used octet-string

7.6.7.3 Wireless Mode Q Setup

This COSEM object defines and controls the behaviour of the device regarding the communications parameters according to mode Q of this European Standard. It is an instance of the interface class "Wireless Mode Q Channel". The OBIS code for this interface class is defined in Table 25 below.

Table 25 — OBIS code

Wireless mode Q Setup	**OBIS identification**						
	IC	**A**	**B**	**C**	**D**	**E**	**F**
Wireless Mode Q Channel Object	Wireless mode Q channel	0	X	31	0	0	0xFF

If more than one object of the type is instantiated in a physical device, then value group B shall be used to number the communications channel.

NOTE A node having more than one network address, i.e. a multi-homed node, will have multiple objects of this type.

Bibliography

[1] COM(2003) 739 final, 10 December 2003, *Proposal for a Directive of the European Parliament and of the Council on energy end-use efficiency and energy services*

[2] IEEE Std. 1588 - 2002, *Standard for A Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*