DNP3 Protocol Stack

DNP3 Application Layer	Application Control (1 byte)	Function Code (1 byte)	Indications (2 bytes)	Object Range Header (2 bytes)	DNP3 Objects	...	Object Range Header (2 bytes)	DNP3 Objects
DNP3 Transport Layer	FIN FIR	Sequence Number (6 bits)						
DNP3 Link Layer	Magic (0x0564) (2 bytes)	Length (1 byte)	Control (1 byte)	Destination (2 bytes)		Source (2 bytes)		Header CRC (2 bytes)
TCP Header								
IP Header								
Ethernet Header								

Data Link Layer

Magic / Start (2 bytes)		Length (1 byte) 5 to 255	Control (1 byte)	Destination (2 bytes) 0 to 65535		Source (2 bytes) 0 to 65519		Header CRC (2 bytes)	
0x05	0x64			LSB	MSB	LSB	MSB	LSB	MSB

DIR	PRM	FCB / 0	FCV / DFC	Function Code			
7	6	5	4	3	2	1	0 ← Bit number

PRM = 1

PRM = 0

DIR	Direction	1	From Master
		0	From Outstation
PRM	Primary	1	Primary to Secondary
		0	Secondary to Primary
FCB	Frame Count Bit	1	
		0	
FCV	Frame Count Valid	1	Examine FCB bit
		0	Ignore FCB bit
DFC	Data Flow Control	1	Receive buffer full
		0	Receive buffer available

Primary Function Code	Function Code Name	FCV Bit
0	RESET_LINK_STATES	0
1	-	-
2	TEST_LINK_STATES	1
3	CONFIRMED_USER_DATA	1
4	UNCONFIRMED_USER_DATA	0
5	-	-
6	-	-
7	-	-
8	-	-
9	REQUEST_LINK_STATUS	0
A	-	-
B	-	-
C	-	-
D	-	-
E	-	-
F	-	-

Secondary Function Code	Function Code Name
0	ACK
1	NACK
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
A	-
B	LINK STATUS
C	-
D	-
E	-
F	NOT_SUPPORTED

by Seda Narli

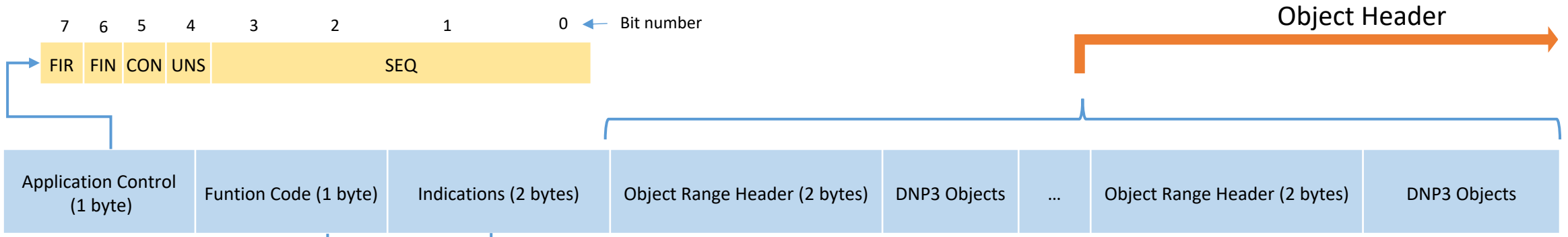
Valid Data Link Layer Control Codes

Outstation to Master	Master to Outstation	Function Code Name	Type	Comment
00	80	ACK	Sec-to-Pri	
01	81	NACK		Link reset required
0B	8B	LINK_STATUS		
0F	8F	NOT_SUPPORTED		
10	90	ACK		Receive buffers full
11	91	NACK		Receive buffers full
1B	9B	LINK_STATUS		Receive buffers full
1F	9F	NOT_SUPPORTED		Receive buffers full
40	C0	RESET_LINK_STATES	Pri-to-Sec	FCB = 0 (secondary ignores FCB)
44	C4	UNCONFIRMED_USER_DATA		FCB = 0 (secondary ignores FCB)
49	C9	REQUEST_LINK_STATUS		FCB = 0 (secondary ignores FCB)
52	D2	TEST_LINK_STATES		FCB = 0
53	D3	CONFIRMED_USER_DATA		FCB = 0
60	E0	RESET_LINK_STATES		FCB = 1 (secondary ignores FCB)
64	E4	UNCONFIRMED_USER_DATA		FCB = 1 (secondary ignores FCB)
69	E9	REQUEST_LINK_STATUS		FCB = 1 (secondary ignores FCB)
72	F2	TEST_LINK_STATES		FCB = 1
73	F3	CONFIRMED_USER_DATA		FCB = 1

Transport Layer

by Seda Narli

Application Layer

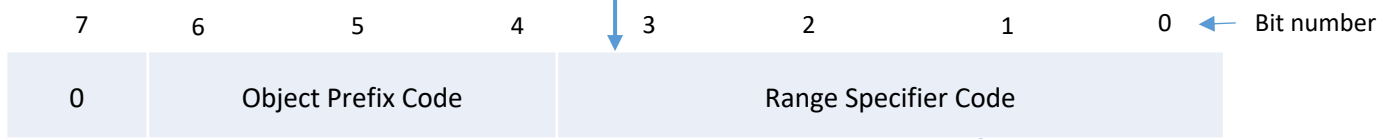


Function Codes			
Requests (Hex)			
0	Confirm	10	Initiliaze Application
1	Read	11	Start application
2	Write	12	Stop application
3	Select	13	Save configuration
4	Operate	14	Enable unsolicited
5	Dir operate	15	Disable unsolicited
6	Dir operate - No resp	16	Assign class
7	Freeze	17	Delay measurement
8	Freeze - No resp	18	Record current time
9	Freeze clear	19	Open file
A	Freeze clear - No resp	1A	Close file
B	Freeze at time	1B	Delete file
C	Freeze at time - No resp	1C	Get file information
D	Cold restart	1D	Authenticate file
E	Warm restart	1E	Abort file
F	Initiliaze data		
Responses (Hex)			
81	Response		
82	Unsolicited response		

Internal Indications	
LSB	
IIN1.0	All stations
IIN1.1	Class 1 events
IIN1.2	Class 2 events
IIN1.3	Class 3 events
IIN1.4	Need time
IIN1.5	Local control
IIN1.6	Device trouble
IIN1.7	Device restart
MSB	
IIN2.0	Function code not supported
IIN2.1	Object unknown
IIN2.2	Parameter error
IIN2.3	Event buffer overflow
IIN2.4	Already executing
IIN2.5	Configuration corrupt
IIN2.6	Reserved 1
IIN2.7	Reserved 2

by Seda Narli

Object Type		Qualifier Field (1 byte)	Range Field(dependent upon qualifier)	Object Data
Group (1 byte)	Variation (1 byte)			



Object Prefix	
0	Objects packed without a prefix
1	Objects prefixed with 1-octet index
2	Objects prefixed with 2-octet index
3	Objects prefixed with 4-octet index
4	Objects prefixed with 1-octet object size
5	Objects prefixed with 2-octet object size
6	Objects prefixed with 4-octet object size
7	Reserved

Range Field Contains	
0	1-octet start-stop indexes
1	2-octet start-stop indexes
2	4-octet start-stop indexes
3	1-octet start – stop virtual addresses
4	2-octet start – stop virtual addresses
5	4-octet start – stop virtual addresses
6	No range field used. Implies all objects
7	1-octet count of objects
8	2-octet count of objects
9	4-octet count of objects
A	Reserved
B	1-octet count of objects (variable format)
C - F	Reserved

by Seda Narli

References Book

The master always initiates control commands. In some systems the master doesn' t always directly initiate data transfer.
The unsolicited message initiates by a Slave/Outstation to report alarms.

DNP3 uses function codes to exchange data between masters and remotes. For instance :
- Enable a Master to request and receive status info from a Slave
- Enable a Master to change a Slave's settings
- Enable a Master to control the Slave
- Enable the Slave to respond with an unsolicited message to particular events that occur in its area.

Fragments, Segments and Frames

Layer or Function	Unit Name	Information
Application Layer	Application Fragment	Permits the setting an upper limit on the memory requirements for message reception. Requests must fit into a single fragment. Responses may require more than one fragment.
Transport Function	Transport Segment	Segmentation breaks a fragment into pieces that fit into a Data Link Layer frame. Each segment contains a Transport Header, but only the first segment of any fragment contains an Application Header. Each segment may have a maximum of 250 octets including the Transport Header.
Data Link Layer	Data Link Frame	A Frame may have as many as 292 octets including its header and CRC octets. Frames are designed for superior error detection.

Comparison of IEC 60870-5 and DNP3 Data Link Layers

Feature	Options Permitted in IEC 60870-5-1 and 2	Chosen by DNP3	Chosen by IEC 60870-5-101
Addressing	Single address, length system-dependent	Two-octet Source address and two-octet Destination address. Considered a single four-octet “structured” address for compliance purposes.	Single address, choice of either zero, one or two octets in length
Frame Format	Choice of FT1.1, FT1.2, FT2, FT3	FT3, transmitted asynchronously	FT1.2
Reliability Mechanism	Varies per frame type	Multiple 16-bit CRCs over each 16 octets of a 255 octet frame. Start and Stop bits, but no parity.	Parity bits and one-octet checksum (not CRC) calculated over 255 octets
Hamming Distance	Varies per frame type	6 for the original FT3. Some debate about the value as currently used.	4
Acknowledge-ments	Either Fixed-length or singleoctet	Fixed 10-octet only	Either fixed-length or singleoctet
Procedures	Balanced (no master) or Unbalanced (master polls)	Balanced only	Either Balanced or Unbalanced
Method for Multi-Drop Links	Unbalanced mode	Collision Avoidance	Unbalanced mode

DNP3 Event	The occurrence of something significant happening. Events are saved at the outstation as information in vendor-specific structures and reported to the master using DNP3 event objects.An event remains in the outstation until confirmation has been received indicating that a description of the event has arrived at the master, after which, the outstation must discard it. With a few exceptions, DNP3 does not define which events are worthy of transmission.
DNP3 Event Object	An object that has a group number and variation that is used to report an event in the outstation to the master.
DNP3 Object	The encoding within a message that refers to a single instance of a group and variation. DNP3 objects can associate with individual point indexes, a set of indexes or to an entire device.
Fragment	A packet of octets that is sized to fit into the buffers of the receiving device's Application Layer.Each fragment contains an application header and a portion of an Application Layer request,response or confirmation.
Frame	A packet of octets transmitted from the Link Layer in one device to the Link Layer in another device over the Physical Layer. Each frame contains a link header, CRC octets and sometimes a segment from the Transport Function.
Input	Refers to values that are measured, read or generated by the device and are reported by an outstation to a master. Examples are the level of fluid in a tank, the open-close state of switch and the calculated sum of the power on all three phases of a power line. Input sometimes refers to the physical source of the value such as a voltage sensor.
Local Issue or Local Matter	The subject of interest that is restricted to an individual device or system and not generally known to other devices, systems, vendors or persons. The method of measuring analog quantities in an outstation is a local issue.
Local Mode	An operating condition whereby outputs are prevented from being controlled by a master. The outputs can be operated locally at the device where the output point is physically located.
Master	A process that desires to obtain data or information in an outstation or that wants to change variables or to control outputs in an outstation. May also refer to a device that contains a master process.
Null Response	A response message wherein the application layer fragment consists of only Application Control,Function Code and Internal Indications octets.
Octet	A group of 8 contiguous digital information bits.
Output	Refers to values in an outstation or lower level device that are controlled by commands from the master. Examples are an analog signal that sets the desired pressure for a gas manifold and electrical contacts which when activated cause a circuit breaker to trip or close. Output sometimes refers to the physical device that receives a control signal such as a circuit breaker.
Outstation	A process that has data, variables or information that another process wants to obtain or wants to set to a new value. May also refer to a device that contains an outstation process. Point An instance of a point type.

Point index	The zero-based numeric identifier that differentiates unique instances of points having the same point type within a DNP3 device.
Point type	The classification for entities having a common set of characteristics and attributes. Examples are binary inputs, analog inputs, counters, binary outputs and analog outputs.
Poll	A poll is a request for data from a master.
Polling	Polling is an interrogate-reply scheme whereby a master schedules the transmission of requests for data to an outstation. Upon receipt of the request, the outstation returns the requested data in a response. The scheduled time of each poll and the specific data requested are a local matter.
Primary Station(when used in context of the Data Link Layer)	The device (master or outstation) that initiates a message transaction between its Data Link Layer and that of a secondary device. The secondary, or non-initiating station, sometimes, but not always, depending upon which function code is used by the primary, sends a response to complete the transaction.
Private	Belonging to or restricted to an individual device or system and not generally known to other devices, systems, vendors or persons. An example of a private application is a control loop implemented within a utility's outstation.
Remote Mode	An operating condition whereby outputs may be controlled from a remotely located master. The outputs may also be operated locally if the system permits this.
Report-by-Exception	A schema whereby changes only are reported from an outstation. The data that remains constant is reported at infrequent intervals, via an integrity poll, as a means of assuring that the data in the master matches the data in the outstation. Report-by-exception is used for both polled and unsolicited responses.
Request	An Application Layer message that asks an outstation to perform a specific action. A poll is only one type of request. There are other types of requests e.g., actuate a control output and set the time.
Response	An Application Layer message from an outstation that is returned to the master as the result of a request from the master.
Secondary Station(when used in context of the Data Link Layer)	The device (master or outstation) that receives a request from a primary station.
Segment	A packet of octets that is sized to fit into a Link Layer frame. Each segment contains a transport header and a portion of a fragment from the Application Layer.
Unsolicited Response	An Application Layer message from an outstation to a master for which no explicit request was received. The request is implied by the act of a master enabling the unsolicited operating mode in an outstation.

References :

https://c3.chipkin.com/assets/uploads/imports/resources/DNP3Introduction-Draft_G.pdf
https://www.dpstele.com/dnp3/tutorials.php

by Seda Narli