Packet Structure and Encoding

- Network Layer details
- Application Layer details
  - Abstract Syntax Notation One (ASN.1)
  - Encoding Application Services and Properties
    - Context Specific and Application Tags
    - Primitive Application Datatypes
    - PDU Types in Detail
- BACnet Arrays and Lists
- Command Prioritization
- Reject, Abort, and Error

Network Layer Details

NPDU Field Format

Field	Size	Notes
Version	1 octet	
Control	1 octet	← Which fields are present is determined by the control octet
DNET	2 octets	
DLEN	1 octet	← DLEN = 0 denotes broadcast MAC DADR and DADR field is absent. DLEN > 0 specifies length of DADR field
DADR	variable	
SNET	2 octets	
SLEN	1 octet	← SLEN = 0 Invalid. SLEN > 0 specifies length of SADR field
SADR	variable	
Hop Count	1 octet	
Message Type	1 octet	
Vendor ID	2 octets	
APDU	N octets	

2

Figure 6-1. NPDU field format. Which fields are present is determined by the bits in the control octet.

DNET = 2-octet ultimate destination network number.
DLEN = 1-octet length of ultimate destination MAC layer address
    (A value of 0 indicates a broadcast on the destination network.)
DADR = Ultimate destination MAC layer address.
DA   = Local network destination MAC layer address.
SNET = 2-octet original source network number.
SLEN = 1-octet length of original source MAC layer address.
SADR = Original source MAC layer address.
SA   = Local network source MAC layer address.

The multi-octet fields, DNET, SNET, and Vendor ID, shall be conveyed with the most significant octet first. Allowable network number values for DNET shall be from 1 to 65535 and for SNET from 1 to 65534.

NPDU Control Octet

Bit Number: 7   6   5   4   3   2   1   0

| Net Msg. | 0 | Dest | 0 | Src | DER | Priority |

Bit 7: 1 indicates that the NSDU conveys a network layer message.
Message Type field is present. 0 indicates that the NSDU contains a
BACnet APDU. Message Type field is absent.
Bit 6: Reserved. Shall be zero.
Bit 5: Destination specifier where:
   0=DNET, DLEN, DADR, and Hop Count absent
   1=DNET, DLEN, and Hop Count present
Bit 4: Reserved. Shall be zero.
Bit 3: Source specifier where:
   0=SNET, SLEN, and SADR absent
   1=SNET, SLEN, and SADR present
Bit 2: 1 indicates that a BACnet-Confirmed-Request-PDU,
a segment of a BACnet-ComplexACK-PDU, or a network layer
message expecting a reply is present.
Bits 1,0: Network priority

3

Bits 1,0: Network priority where:
   B'11' = Life Safety message
   B'10' = Critical Equipment message
   B'01' = Urgent message
   B '00' = Normal message

ASN.1 Primer

BACnet clause 20.2 defines BACnet's encoding of ASN.1.

name ::= expression
defines "name" in terms of the expression.

SEQUENCE {}
means that one of each item in the bracketed construct is included, unless it is marked with the keyword OPTIONAL, in which case it may or may not be included.

SEQUENCE OF item
means a list of zero or more items. The item may be another ASN.1 definition, or it may be a SEQUENCE {}. Note the difference between the one-shot SEQUENCE and the list defined by SEQUENCE OF.

CHOICE {}
means a selection of one item of the bracketed construct is included.

ENUMERATED {name (value),...}
defines an enumeration, where a list of "names" are assigned values shown in parenthesis.

[n]
A number in square brackets denotes a context tag, which will generally appear in the encoding (the exception being tags defined in the APDU header productions)

Encoding Application Services

- Context Specific and Application Datatypes

- Primitive Application Datatypes

```
20.2.1.4 Application Tags
The Tag Number field of an encoded BACnet application tag shall specify the
application datatype as follows:
Tag Number:      0 = Null
                 1 = Boolean
                 2 = Unsigned Integer
                 3 = Signed Integer (2's complement notation)
                 4 = Real (ANSI/IEEE-754 floating point)
                 5 = Double (ANSI/IEEE-754 double precision floating point)
                 6 = Octet String
                 7 = Character String
                 8 = Bit String
                 9 = Enumerated
                10 = Date
                11 = Time
                12 = BACnetObjectIdentifier
                13, 14, 15 = Reserved for ASHRAE
```

PDU Types

PDU_TYPE_CONFIRMED_SERVICE_REQUEST = 0,
PDU_TYPE_UNCONFIRMED_SERVICE_REQUEST = 0x10,
PDU_TYPE_SIMPLE_ACK = 0x20,
PDU_TYPE_COMPLEX_ACK = 0x30,
PDU_TYPE_SEGMENT_ACK = 0x40,
PDU_TYPE_ERROR = 0x50,
PDU_TYPE_REJECT = 0x60,
PDU_TYPE_ABORT = 0x70

Confirmed Services

/* Alarm and Event Services */
SERVICE_CONFIRMED_ACKNOWLEDGE_ALARM = 0,
SERVICE_CONFIRMED_COV_NOTIFICATION = 1,
SERVICE_CONFIRMED_EVENT_NOTIFICATION = 2,
SERVICE_CONFIRMED_GET_ALARM_SUMMARY = 3,
SERVICE_CONFIRMED_GET_ENROLLMENT_SUMMARY = 4,
SERVICE_CONFIRMED_GET_EVENT_INFORMATION = 29,
SERVICE_CONFIRMED_SUBSCRIBE_COV = 5,
SERVICE_CONFIRMED_SUBSCRIBE_COV_PROPERTY = 28,
SERVICE_CONFIRMED_LIFE_SAFETY_OPERATION = 27,
/* File Access Services */
SERVICE_CONFIRMED_ATOMIC_READ_FILE = 6,
SERVICE_CONFIRMED_ATOMIC_WRITE_FILE = 7,
/* Object Access Services */
SERVICE_CONFIRMED_ADD_LIST_ELEMENT = 8,
SERVICE_CONFIRMED_REMOVE_LIST_ELEMENT = 9,
SERVICE_CONFIRMED_CREATE_OBJECT = 10,
SERVICE_CONFIRMED_DELETE_OBJECT = 11,
SERVICE_CONFIRMED_READ_PROPERTY = 12,
SERVICE_CONFIRMED_READ_PROP_CONDITIONAL = 13,
SERVICE_CONFIRMED_READ_PROP_MULTIPLE = 14,
SERVICE_CONFIRMED_READ_RANGE = 26,
SERVICE_CONFIRMED_WRITE_PROPERTY = 15,
SERVICE_CONFIRMED_WRITE_PROP_MULTIPLE = 16,
/* Remote Device Management Services */
SERVICE_CONFIRMED_DEVICE_COMMUNICATION_CONTROL = 17,

/* Remote Device Management Services */
SERVICE_CONFIRMED_PRIVATE_TRANSFER = 18,
SERVICE_CONFIRMED_TEXT_MESSAGE = 19,
SERVICE_CONFIRMED_REINITIALIZE_DEVICE = 20,
/* Virtual Terminal Services */
SERVICE_CONFIRMED_VT_OPEN = 21,
SERVICE_CONFIRMED_VT_CLOSE = 22,
SERVICE_CONFIRMED_VT_DATA = 23,
/* Security Services */
SERVICE_CONFIRMED_AUTHENTICATE = 24,
SERVICE_CONFIRMED_REQUEST_KEY = 25,

7

Unconfirmed Services

```
SERVICE_UNCONFIRMED_I_AM = 0,
SERVICE_UNCONFIRMED_I_HAVE = 1,
SERVICE_UNCONFIRMED_COV_NOTIFICATION = 2,
SERVICE_UNCONFIRMED_EVENT_NOTIFICATION = 3,
SERVICE_UNCONFIRMED_PRIVATE_TRANSFER = 4,
SERVICE_UNCONFIRMED_TEXT_MESSAGE = 5,
SERVICE_UNCONFIRMED_TIME_SYNCHRONIZATION = 6,
SERVICE_UNCONFIRMED_WHO_HAS = 7,
SERVICE_UNCONFIRMED_WHO_IS = 8,
SERVICE_UNCONFIRMED_UTC_TIME_SYNCHRONIZATION = 9,
```

BACnet Arrays and Lists

- Ordered sequence of a data elements
- Each element may be accessed using index
- Index 0 is count of elements
- Omitted Index is all elements
- "List of" is a sequence of data elements that cannot be accessed or counted using Index.

9

A "BACnetARRAY" datatype is a structured datatype consisting of an ordered sequence of data elements, each having the same datatype. The components of an array property may be individually accessed (read or written) using an "array index," which is an unsigned integer value. An index of 0 (zero) shall specify that the count of the number of data elements be returned. If the array index is omitted, it means that all of the elements of the array are to be accessed. An array index N, greater than zero, shall specify the Nth element in the sequence. When array properties are used in BACnet objects, the notation "BACnetARRAY[N] of datatype" shall mean an ordered sequence of N data elements, each of which has that datatype.

If the size of an array may be changed by writing to the array, then array element 0 shall be writable. If the value of array element 0 is decreased, the array shall be truncated and the elements of the array with an index greater than the new value of array element 0 are deleted. If the value of array element 0 is increased, the new elements of the array, those with an index greater than the old value of array element 0, shall be created; the values that are assigned to those elements shall be a local matter except where otherwise specified. Where the size of an array is allowed to be changed, writing the entire array as a single property with a different number of elements shall cause the array size to be changed. An attempt to write to an array element with an index greater than the size of the array shall result in an error and shall not cause the array to grow to accommodate the element. Arrays whose sizes are fixed by the Standard shall not be resizable.

A "List of" datatype is a structured datatype consisting of a sequence of zero or more data elements, each having the same datatype. The length of each "List of" may be variable. Unless specified for a particular use, no maximum size should be assumed for any "List of" implementation. The notation "List of datatype" shall mean a sequence of zero or more data elements, each of which has the indicated type.

The difference between a "BACnetARRAY" property and a "List of" property is that the elements of the array can be uniquely accessed by an array index while the elements of the "List of" property cannot. Moreover, the number of elements in the BACnetARRAY may be ascertained by reading the array index 0, while the number of elements present in a "List of" property can only be determined by reading the entire property value and performing a count.

Command Prioritization

Priority Level	Application	Priority Level	Application
1	Manual-Life Safety	9	Available
2	Automatic-Life Safety	10	Available
3	Available	11	Available
4	Available	12	Available
5	Critical Equipment Control	13	Available
6	Minimum On/Off	14	Available
7	Available	15	Available
8	Manual Operator	16	Available

Relinquish_Default

10

19.2.2   Application Priority Assignments

Commanding entities are assigned one of the 16 possible priority levels. The assignment of most priorities is site dependent and represents the objectives of the site management. Table 19-1 contains the standard priorities. Other applications that need prioritization include Temperature Override, Demand Limiting, Optimum Start/Stop, Duty Cycling, and Scheduling. The relative priorities of these applications may vary from site to site and are not standardized. For interoperability at any particular site, the only requirement is that all devices implement the same priority scheme. The positions marked Available are open for assignment to DDC programs, EMS programs, etc. The interpretation of what conditions constitute Manual-Life Safety or Automatic-Life Safety decisions is a local matter.

19.2.1.3   Relinquish Commands

When a commanding entity no longer desires to control a commandable property, it issues a relinquish command. A relinquish command is also either a WriteProperty service request or a WritePropertyMultiple service request. In either case, the request primitive shall contain (among others) the following parameters:

> Property Identifier: Commandable_Property
> Property Value: NULL
> Priority: Priority

The placement of NULL in the value parameter indicates the absence of any command at that priority. When all elements of the priority table array contain NULL, the commandable property shall assume the value defined in the Relinquish_Default property of the object. It is possible for an application entity to relinquish at a priority other than its own, resulting in unpredictable behavior. If more than one application is assigned the same priority, it is possible for one application entity to write-over (or relinquish) the commands from the other application entity, resulting in unpredictable operation. To minimize this possibility, it is very important not to allow more than one commanding entity to assume the same priority level within the system.

Reject, Abort, Error

- Reject PDU
  - Reject based on syntactical flaws or other protocol errors that prevent PDU from being interpreted
  - Requested service is not available
  - Only confirmed request PDUs may be rejected.

11

Reject, Abort, Error

- Abort used to terminate transaction between two peers

- Error for APDU failures

  – Indicates the reason why a previous confirmed service request failed in its entirety.

  – Prescribed in Service procedure, although listed in Clause 18.