ANSI/ASHRAE Addendum q to
ANSI/ASHRAE Standard 135-2008

ASHRAE STANDARD

BACnet®—A Data Communication Protocol for Building Automation and Control Networks

Approved by the ASHRAE Standards Committee on January 24, 2009; by the ASHRAE Board of Directors on January 28, 2009; and by the American National Standards Institute on January 29, 2009.

This standard is under continuous maintenance by a Standing Standard Project Committee (SSPC) for which the Standards Committee has established a documented program for regular publication of addenda or revisions, including procedures for timely, documented, consensus action on requests for change to any part of the standard. The change submittal form, instructions, and deadlines may be obtained in electronic form from the ASHRAE Web site, http://www.ashrae.org, or in paper form from the Manager of Standards. The latest edition of an ASHRAE Standard may be purchased from ASHRAE Customer Service, 1791 Tullie Circle, NE, Atlanta, GA 30329-2305. E-mail: orders@ashrae.org. Fax: 404-321-5478. Telephone: 404-636-8400 (worldwide), or toll free 1-800-527-4723 (for orders in US and Canada).

ISSN 1041-2336

Approved American National Standard
ANSI
www.ansi.org

American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.
1791 Tullie Circle NE, Atlanta, GA 30329
www.ashrae.org

SPECIAL NOTE

This American National Standard (ANS) is a national voluntary consensus standard developed under the auspices of the American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE). *Consensus* is defined by the American National Standards Institute (ANSI), of which ASHRAE is a member and which has approved this standard as an ANS, as "substantial agreement reached by directly and materially affected interest categories. This signifies the concurrence of more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that an effort be made toward their resolution." Compliance with this standard is voluntary until and unless a legal jurisdiction makes compliance mandatory through legislation.

ASHRAE obtains consensus through participation of its national and international members, associated societies, and public review.

ASHRAE Standards are prepared by a Project Committee appointed specifically for the purpose of writing the Standard. The Project Committee Chair and Vice-Chair must be members of ASHRAE; while other committee members may or may not be ASHRAE members, all must be technically qualified in the subject area of the Standard. Every effort is made to balance the concerned interests on all Project Committees.

The Assistant Director of Technology for Standards and Special Projects of ASHRAE should be contacted for:

a. interpretation of the contents of this Standard,
b. participation in the next review of the Standard,
c. offering constructive criticism for improving the Standard, or
d. permission to reprint portions of the Standard.

[This foreword and the "rationales" on the following pages are not part of this standard. They are merely informative and do not contain requirements necessary for conformance to the standard.]

FOREWORD

This addendum describes changes to the current standard. These modifications are the result of change proposals made pursuant to the ASHRAE continuous maintenance procedures and of deliberations within Standing Standard Project Committee 135. The changes are summarized below.

In the following document, language to be added to existing clauses of ANSI/ASHRAE 135-2008 and Addenda is indicated through the use of *italics*, while deletions are indicated by ~~strikethrough~~. Where entirely new subclauses are to be added, plain type is used throughout.

SSPC 135 wishes to recognize the efforts of the following people in developing this addendum: Coleman Brumley, Ted Humpal, René Kälin, Jerry Martocci, Bob Old, Bob Thomas, and Cam Williams.

135-2008*q*-1. Allow unicast I-Ams.

Rationale
The BACnet standard currently requires that the I-Am message be broadcast in order to minimize multiple Who-Is broadcasts to locate a particular device. There are assumptions regarding time and bandwidth savings that may be true for wired media, but the costs of sending broadcasts on a high latency mesh network are considerably higher.

Addendum 135-2008*q*-1

[Change **Clause 16.10.4**, p. 377]

The sending BACnet-user shall broadcast *or unicast* the I-Am unconfirmed request. ~~This~~ *If the I-Am is broadcast, this* broadcast may be on the local network only, a remote network only, or globally on all networks at the discretion of the application. If the I-Am is being ~~broadcast~~ *sent* in response to a previously received Who-Is, then the I-Am shall be ~~broadcast~~*sent* in such a manner that the BACnet-user that ~~broadcast~~ *sent* the Who-Is will receive the resulting I-Am. Since the request is unconfirmed, no further action is required. A BACnet-user may issue an I-Am service request at any time.

135-2008*q*-2. Define virtual addressing for data links with MAC addresses longer than 6 octets.

Rationale
BACnet data link addresses currently do not exceed 7 octets (for LonTalk) and many implementations do not reserve storage greater than 6 octets for cached MAC addresses. A new method compatible with existing devices is provided for handling new data link layers with lengths greater than 6 octets, such as ZigBee and IPv6.

Addendum 135-2008*q*-2

[Add new Clause **H.X** to Normative Annex H, p. 599]

H.X Virtual MAC Addressing

H.X.1 General

With the exception of LonTalk, a data link layer with a MAC address size greater than 6 octets shall expose a BACnet Virtual MAC (VMAC) address of 6 octets or fewer to the BACnet network layer.

The VMAC address shall function analogously as the MAC address of the technologies of Clauses 7, 8, 9, and 11.

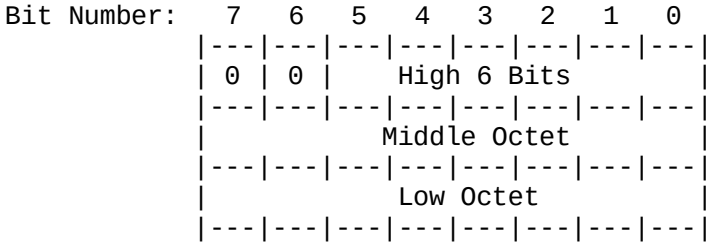
A VMAC table shall exist within the data link layer on all BACnet nodes on a BACnet network that employs VMAC addresses. A VMAC table shall be used to map native MAC addresses of the data link layer to VMAC addresses. The VMAC table contains VMAC entries corresponding to nodes in the BACnet network.

The data link layer uses native MAC addresses when communicating over its data link. The data link translates from VMAC addresses to native MAC addresses when BACnet messages are sent out. The data link translates from native MAC addresses to VMAC addresses when BACnet messages are received. If the address translation fails, the NPDU shall be dropped.

The methods used to maintain a VMAC table are dependent on the specific data link that is using a VMAC table.

H.X.2 Using Device Instance as a VMAC Address

When a particular data link layer specifies that each node's BACnet device instance is to be used as the VMAC address for the node, then the device instance as a VMAC address shall be transmitted as 3 octets, with the high order octet first, and formatted as follows:



135-2008*q*-3. Define the use of ZigBee as a BACnet data link layer.

Rationale
There is a desire to have a wireless data link layer in BACnet. ZigBee has been adopted as a solution.

Addendum 135-2008*q*-3

[Change **Table 6-1**, p.47]

Table 6-1. Maximum NPDU Lengths When Routing Through Different BACnet Data Link Layers

Data Link Technology	Maximum NPDU Length
…	…
ZigBee, as defined in Annex X	*501 octets*

[Change **Table 6-2**, p.51]

Table 6-2. BACnet DADR and SADR encoding rules based upon data link layer technology

BACnet Data Link Layer	DLEN	SLEN	Encoding Rules
…	…	…	…
ZigBee, as defined in Annex X	*3*	*3*	*A VMAC Address encoded as a device instance as shown in Annex H.X Virtual MAC Addressing*

[Change **Clause 25**, p.491.]
[Note: lines beginning with "ZigBee" are to be added as shown.]

25 REFERENCES

…

Konnex Association, *Konnex Handbook Volume 7: Applications Descriptions.*

ZigBee Alliance, *ZigBee® Specification* (053547r17)
ZigBee Alliance, *Commercial Building Automation Profile Specification* (053516r10)

Sources for Reference Material

…

LonMark International, 550 Meridian Avenue, San Jose, CA 95126.

ZigBee Alliance, Inc., 2400 Camino Ramon, Suite 375, San Ramon, CA 94583.

[Add new **Annex X**.]
[Note: references to **Annex H.X** refer to the annex described in Addendum 135-2008*q*-2.]

X BACnet OVER ZigBee AS A DATA LINK LAYER (NORMATIVE)

X.1 General

This normative annex specifies the use of BACnet messaging with the services described in the *ZigBee® Specification* and the *ZigBee Commercial Building Automation Profile Specification*. These ZigBee documents, as amended and extended by the ZigBee Alliance, are deemed to be included in this standard by reference.

X.2 ZigBee Overview

A ZigBee network is a set of wireless nodes that cooperate by forming a mesh network over which messages hop, from node to node, to reach a destination.

ZigBee uses an IEEE 64-bit address, called an EUI64, to identify a ZigBee node on the network.

A ZigBee cluster may be described as a particular service, and a ZigBee endpoint as a port. A ZigBee application profile is an interoperable domain, such as the Commercial Building Automation Profile. ZigBee applications advertise and support clusters on endpoints.

ZigBee devices have up to 240 endpoints. Applications may use endpoints numbered 1-240, but there is no correlation between application and endpoint number. Endpoint 0 is reserved for use by the ZigBee Device Object (ZDO) for discovery services.

Each endpoint provides one Simple Descriptor that describes the application profile and services supported by that endpoint. Services are identified by a list of input and output clusters.

Clusters have mandatory and optional attributes (analogous to BACnet properties) and commands. Commands may also be vendor defined and include a two-octet Manufacturer Code field (analogous to the BACnet vendor identifier).

ZigBee network broadcasts are discouraged for normal operation because a broadcast message must be propagated to all nodes in the network. All nodes must repeat the message, and each node must wait until there is a clear channel to transmit. The interval from the initial transmission to when the final node forwards the message can be a significant amount of time and reduce much of the network bandwidth during this interval.

ZigBee network multicasting can be configured to stop propagating a multicast beyond the proximity of a target group of nodes.

ZigBee supports groups and multicast addressing to a group. Membership in a group is indicated by a GroupID entry in the ZigBee stack's group table. Each entry maps a 16-bit GroupID to a set of endpoints. GroupID endpoint mapping is specific to each node. When a group addressed message reaches a node and the node is a member of the group, the message is sent to each of the mapped endpoints.

ZigBee supports the creation of bindings that map a cluster to one or more targets. A sender of a ZigBee message may specify a cluster instead of an address as a destination and let one or more ZigBee bindings resolve the cluster to a set of targets. A binding may be a multicast binding that maps to a GroupID, which targets a group of nodes.

There are many reasons for the existence of more than one BACnet/ZigBee network on a single ZigBee network. A few such reasons are described below.

A single large ZigBee network may have groups of BACnet/ZigBee nodes that are each geographically clumped together such that inter-clump communication is more efficient through wired routers than across the wireless network. Making each clump a separate BACnet/ZigBee network would be a more optimal solution.

If there is an increase in the number of BACnet nodes and/or traffic on BACnet/ZigBee network so that the BACnet traffic load through the BACnet/ZigBee router is undesirable, one option is to split the one BACnet/ZigBee network into separate BACnet/ZigBee networks, each on its own ZigBee network. However, depending on the wireless environment, each new ZigBee network may not have the wireless mesh density to produce the required redundant routes between ZigBee nodes. A single ZigBee network, with many BACnet/ZigBee networks, does not decrease the wireless mesh density, but it does share the BACnet traffic load between the BACnet/ZigBee routers.

The above example also covers the desire to reduce latency introduced by wireless hops between ZigBee nodes. A BACnet/ZigBee network might be spread out such that some BACnet/ZigBee nodes are too many wireless hops away from a BACnet/ZigBee router. If such BACnet/ZigBee nodes were moved to a new BACnet/ZigBee network, such that a BACnet/ZigBee router is closer (in wireless hops) to the BACnet/ZigBee nodes, wireless hop latency would be reduced.

X.3 Definitions

A BACnet/ZigBee node or router is a BACnet node or router using ZigBee as a data link layer under its BACnet network layer.

A BACnet/ZigBee network is a group of BACnet/ZigBee nodes on the same ZigBee network that operate as a BACnet network.

NOTE: There may be more than one BACnet/ZigBee network on a ZigBee network.

X.4 Unicast Addressing

The ZigBee Generic Tunnel (GT) cluster is a cluster that contains common attributes for tunneling non-ZigBee protocols. The BACnet Protocol Tunnel (BP) cluster is a cluster that indicates that BACnet is being tunneled on the endpoint upon which these two clusters exist. The BACnet Protocol Tunnel and Generic Tunnel clusters, together on an endpoint, identify a node as a BACnet/ZigBee node and as having the capability of transferring BACnet NPDUs.

An endpoint that contains the BACnet Protocol Tunnel and Generic Tunnel cluster on its Simple Descriptor input and output cluster lists is called a BACnet endpoint. A BACnet endpoint is a BACnet/ZigBee node's access to a BACnet/ZigBee network.

BACnet unicast messages shall be sent to a BACnet endpoint. All received unicast messages shall have a BACnet endpoint as a source.

The Application Profile Identifier field of the BACnet endpoint's Simple Descriptor shall be the ZigBee Commercial Building Automation Profile identifier.

A non-routing node shall have one BACnet endpoint. A router shall have a BACnet endpoint for each of its BACnet/ZigBee network ports.

X.5 Broadcast Addressing

A BACnet local broadcast message shall be sent on a BACnet/ZigBee network using a ZigBee group address such that all (and only) the BACnet endpoints on the target BACnet/ZigBee network receive the message. All received group-addressed messages shall have a BACnet endpoint as a source.

A BACnet/ZigBee node shall support groups and group addressing. A BACnet/ZigBee node shall support the ZigBee Cluster Library Groups clusters that can be used to modify a ZigBee node’s group table, and therefore its ZigBee group membership.

ZigBee group membership and ZigBee binding is a local matter that may be accomplished through the ZigBee application interface or with standard ZigBee commands from an external source, such as a wireless configuration tool.

Multiple BACnet/ZigBee networks on a single ZigBee network shall each be mapped to a single unique ZigBee GroupID. A BACnet router between such BACnet/ZigBee networks would be a member of each group (see Figure X-2).

There are many reasons for the existence of more than one BACnet/ZigBee network on a single ZigBee network. A few such reasons are described below.

A single large ZigBee network may have groups of BACnet/ZigBee nodes that are each geographically clumped together such that inter-clump communication is more efficient through wired routers than across the wireless network. Making each clump a separate BACnet/ZigBee network would be a more optimal solution.

If there is an increase in the number of BACnet nodes and/or traffic on BACnet/ZigBee network so that the BACnet traffic load through the BACnet/ZigBee router is undesirable, one option is to split the one BACnet/ZigBee network into separate BACnet/ZigBee networks, each on its own ZigBee network. However, depending on the wireless environment, each new ZigBee network may not have the wireless mesh density to produce the required redundant routes between ZigBee nodes. A single ZigBee network having many BACnet/ZigBee networks does not decrease the wireless mesh density, but it does share the BACnet traffic load between the BACnet/ZigBee routers.

The above example also demonstrates the rationale for reducing latency introduced by wireless hops between ZigBee nodes. A BACnet/ZigBee network might be spread out such that some BACnet/ZigBee nodes are too many wireless hops away from a BACnet/ZigBee router. If such BACnet/ZigBee nodes were moved to a new BACnet/ZigBee network, such that a BACnet/ZigBee router is closer (in wireless hops) to the BACnet/ZigBee nodes, wireless hop latency would be reduced.

X.6 BACnet/ZigBee Data Link Layer (BZLL)

A BACnet/ZigBee Data Link Layer (BZLL) shall exist for each BACnet endpoint on a BACnet/ZigBee node. The BZLL provides the data link layer between the BACnet Network Layer (see Clause 6) and a single BACnet/ZigBee network.

Figure X-1 shows an example of a non-routing BACnet/ZigBee node that is using endpoint 6 as the BACnet endpoint. All nodes on the BACnet network to which this node belongs have membership in the ZigBee group specified by the ZigBee GroupID X'ABCD'. This allows a local BACnet broadcast to be sent as a ZigBee group multicast. GroupID X'ABCD' and endpoint 6 are used here only as an example. Any GroupID that is unique on the ZigBee network may be used. Any endpoint that is unique to the node may be used as a BACnet endpoint.

In Figure X-1, incoming group multicasts are passed through the Group Table and mapped to endpoint 6. When the BZLL wants to send a BACnet broadcast message, it shall send the message to the BACnet Protocol Tunnel cluster that corresponds to GroupID X'ABCD' in the ZigBee Binding Table.

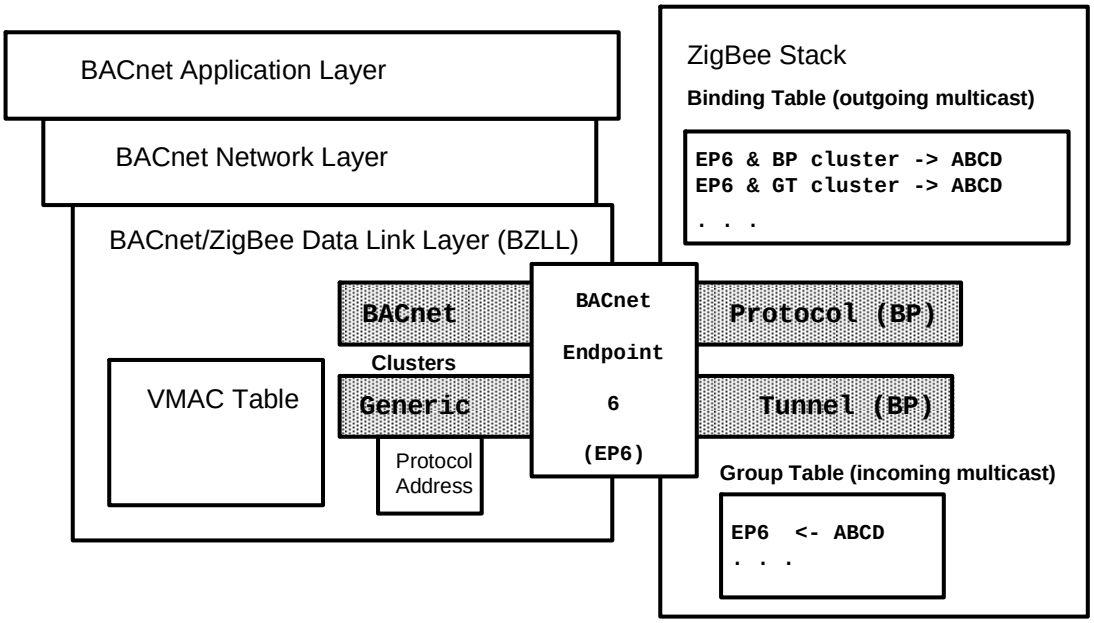


Figure X-1. Diagram of BZLL and other layers and entities on a non-routing BACnet/ZigBee node.

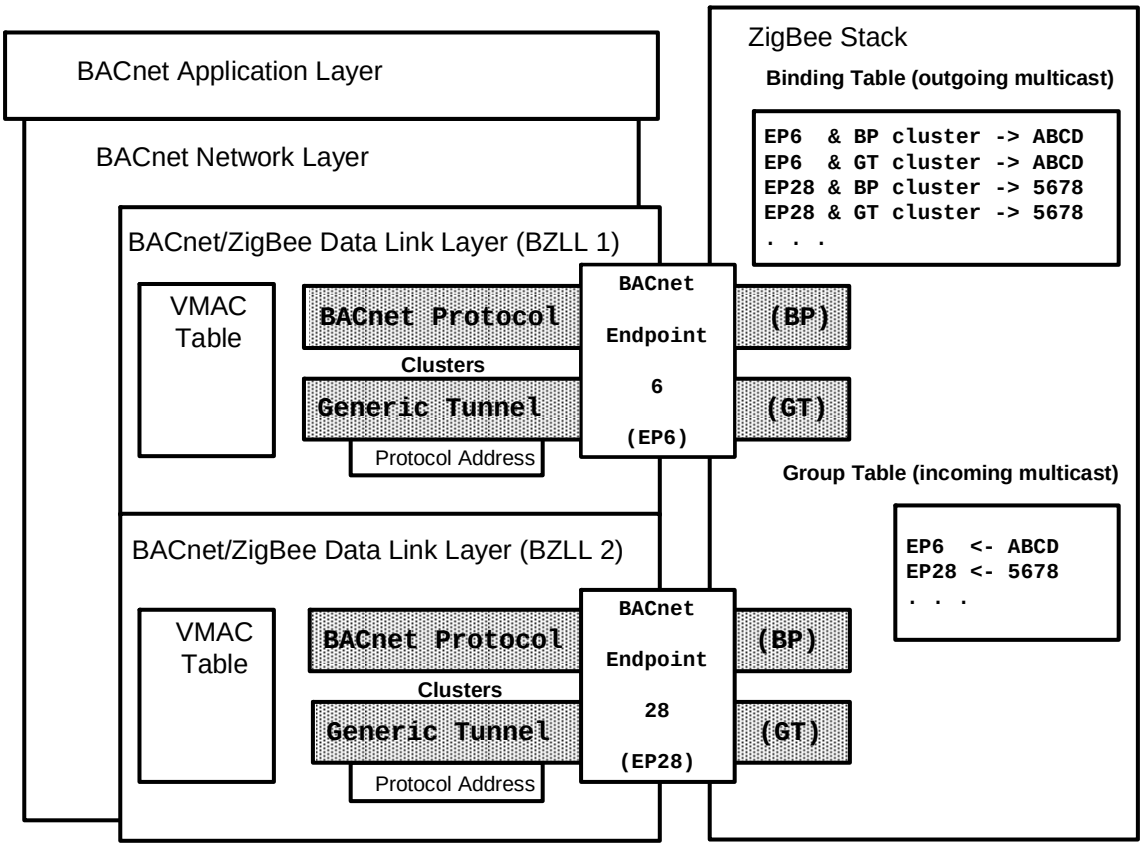


Figure X-2. Diagram of BZLL and other layers and entities on a BACnet/ZigBee router.

Figure X-2 shows entities on a BACnet/ZigBee router that routes to two BACnet/ZigBee networks. A BACnet router routing between two BACnet/ZigBee networks shall have a BZLL for each BACnet/ZigBee network. Each BZLL shall use a separate BACnet endpoint. The ZigBee Binding and Group tables each have entries corresponding to BZLL 1 and BZLL 2 to map the GroupIDs and corresponding BACnet endpoints together for send and receive.

X.6.1 BZLL VMAC Table Management

A BACnet/ZigBee node shall conform to the Annex H.X Virtual MAC Addressing.

The BZLL shall use VMAC addresses. Each VMAC address shall be the device instance of the BACnet Device object on the node in which the BZLL resides. All BACnet/ZigBee nodes shall have a Device object.

A BZLL shall manage a VMAC table. The VMAC entry field MAC Address shall be a ZigBee EUI64 and BACnet endpoint.

The VMAC table shall be maintained by the BZLL by using the commands and responses of the ZigBee Generic Tunnel cluster on the BZLL's BACnet endpoint. These commands are specified in the *ZigBee Commercial Building Automation Profile Specification.*

The VMAC address of the BZLL, the Protocol Address attribute of the Generic Tunnel cluster on the corresponding BACnet endpoint, and the device instance of the BACnet Device object shall be the same value. When one of these is modified, then the others shall be changed to the same value. All of these may be stored in one memory location on the node.

The Protocol Address attribute is of the ZigBee data type Octet String, which is a sequence of octets with a maximum size of 255.

The BZLL shall support all mandatory commands of the Generic Tunnel cluster and BACnet Protocol Tunnel cluster. Table X-1 lists the commands that shall be utilized to access, advertise, and modify the attribute Protocol Address.

Table X-1. Generic Tunnel Cluster Commands

ZigBee Command	Description
Match Protocol Address	Sent to all network nodes to request a matching Protocol Address attribute.
Match Protocol Address Response	Response to the sender of a Match Protocol Address command if the Protocol Address attribute matches.
Advertise Protocol Address	Sent to one or all network nodes to indicate the sender's Protocol Address.
Read Attribute	Sent to one or all nodes to request each receiver’s Protocol Address.
Read Attribute Response	Response to the sender of a Read Attribute command containing the attribute value or indicating an error.
Write Attribute	Sent to a single node to change the receiver's Protocol Address.
Write Attribute Response	Response to the sender of a Write Attribute command confirming the command execution or indicating an error.

The BZLL may create a ZigBee binding that maps its BACnet endpoint and Generic Tunnel cluster to the ZigBee GroupID used by the BACnet/ZigBee network (see Figure X-1). This binding allows the above commands to be issued as a group multicast to all nodes in the BACnet/ZigBee network.

On startup, a router shall issue a group multicast Read Attribute command requesting the Protocol Address attribute from the BZLL on all nodes in the BACnet/ZigBee network. Each node receiving the Read Attribute command shall respond with the VMAC address for that BZLL. When a response is received, the router shall create a VMAC entry for the responding node.

On startup, a node shall issue a group multicast Advertise Attribute command indicating Protocol Address attribute (VMAC address) to all nodes in the BACnet network. When a node acquires a new VMAC address for the BZLL, the node shall issue a group multicast Advertise Attribute command indicating the Protocol Address attribute (new VMAC address).

To be able to detect new nodes on the network, the BZLL on a router shall periodically issue a Read Attribute command requesting the Protocol Address attribute from all network nodes. The period at which a router requests all Protocol Address attributes is a local matter.

To facilitate removal of an obsolete VMAC entry, the following procedure shall be used: After an interval, if there has been no activity indicating a node’s VMAC address for a node represented by a VMAC entry, then the BZLL shall issue a Read Attribute command requesting the node's Protocol Address attribute (VMAC address). If the node fails to respond, the VMAC entry shall be removed. The interval of no activity before a node's Protocol Address attribute is requested is a local matter.

If a node advertises or responds with a new VMAC address, the node's VMAC entry shall be updated.

There shall be no duplicate VMAC addresses in the VMAC table. If a duplicate address is received, a BACnet router shall keep only the most recently verified VMAC address. Otherwise, the means by which a node detects, verifies and prevents duplicate VMAC addresses is a local matter.

Other than the requirements above, the means by which a node maintains a VMAC table is a local matter.

X.6.2 BZLL Transfer NPDU

A BZLL on a node shall transfer BACnet NPDUs to a BZLL on another node using the APSDE-DATA primitives described in the *ZigBee Specification*. A BACnet NPDU shall be transferred as a ZigBee ASDU from an output BACnet Protocol Tunnel cluster to an input BACnet Protocol Tunnel cluster.

The ZigBee ASDU that is passed to the APSDE-DATA.request to transfer a BACnet NPDU shall be a ZigBee Cluster Library (ZCL) client to server frame as shown in Figure X-3.

Frame Control	1 octet	X'01'
Transaction Sequence Number	1 octet	X'00' to X'FF', incrementing with each new request command
Command Identifier	1 octet	X'00' Transfer NPDU request command
Frame Payload	N octets	BACnet NPDU

Figure X-3. ZCL Frame as ZigBee ASDU with BACnet NPDU Payload.

A BACnet unicast NPDU shall be transferred using a ZigBee unicast by specifying the EUI64 and BACnet endpoint of the target as parameters of the APSDE-DATA.request.

A BACnet broadcast NPDU shall be transferred using the BACnet Protocol Tunnel cluster as a destination. The cluster and source endpoint will be used to resolve, through a ZigBee binding, to a ZigBee group.

X.6.3 BZLL Generic Tunnel Cluster Support

The BZLL shall support the ZigBee Generic Tunnel cluster attributes described below.

X.6.3.1 Maximum Incoming Transfer Size

The Maximum Incoming Transfer Size attribute shall be the maximum ZigBee ASDU size, in octets, that may be received by the BZLL. This value is related to the maximum BACnet APDU size described in Clause X.8.

X.6.3.2 Maximum Outgoing Transfer Size

The Maximum Outgoing Transfer Size attribute shall be the maximum ZigBee ASDU size, in octets, that can be sent by the BZLL. This value is related to the maximum BACnet APDU size described in Clause X.8.

X.6.3.3 Protocol Address

The Protocol Address attribute shall be the VMAC address of the BZLL, which is the BACnet device instance.

X.7 Maximum Payload Size

Each BACnet endpoint shall support a ZigBee ASDU size that includes the maximum BACnet APDU size plus the octets in the ZCL and BACnet NPDU headers. The ZigBee ASDU may be fragmented at the source node and reassembled at the destination node. The ZigBee stack options controlling fragmentation/reassembly and payload sizes will ultimately determine the maximum ZigBee APDU size and therefore shall be set accordingly.

X.8 Vendor Specific Commands

The ZigBee Cluster Library frame specification defines a method for sending vendor specific commands. Use of these commands is a local matter.

[Add a new entry to **History of Revisions**, p. 688]

(This History of Revisions is not part of this standard. It is merely informative and does not contain requirements necessary for conformance to the standard.)

HISTORY OF REVISIONS

Protocol		***Summary of Changes to the Standard***
Version	***Revision***	
…	…	**…**
1	8	**Addendum *q* to ANSI/ASHRAE 135-2008** Approved by the ASHRAE Standards Committee January 24, 2009; by the ASHRAE Board of Directors January 28, 2009; and by the American National Standards Institute January 29, 2009. 1. Allow unicast I-Ams. 2. Define virtual addressing for data links with MAC addresses longer than 6 octets. 3. Define the use of ZigBee as a BACnet data link layer.