

BACnet/IP in Detail

- BACnet/IP Overview
- Essential Packet Types
- Foreign Device Registration
- BACnet Broadcast Management Device
- NAT and IPv6

1

A BACnet/IP network is a collection of one or more IP subnetworks (IP domains) that are assigned a single BACnet network number. A BACnet internetwork (3.2.26) consists of two or more BACnet networks. These networks may be BACnet/IP networks or use the technologies specified in Clauses 7, 8, 9, and 11. This standard also supports the inclusion of IP multicast groups in a fashion analogous to IP subnets, as described below in J.8.

The BACnet Virtual Link Layer (BVLL) provides the interface between the BACnet Network Layer (Clause 6) and the underlying capabilities of a particular communication subsystem

BACnet/IP Overview

- UDP/IP on port 47808 (0xBAC0)
- NDPU, APDU same as others
- MAC address is IP Address, Port Number
- Unicast, Broadcast
- BACnet Ethernet, BACnet/IP Share Wire

2

The default UDP port for both directed messages and broadcasts shall be X'BAC0' and all B/IP devices shall support it. In some cases, e.g., a situation where it is desirable for two groups of BACnet devices to coexist independently on the same IP subnet, the UDP port may be configured locally to a different value without it being considered a violation of this protocol. Where the "B/IP broadcast address" is referred to in this Annex, it means an IP address with the subnet of the broadcasting device in the network portion and all 1's in the host portion of the address and the UDP port of the devices on the B/IP network in question.

Six octets consisting of the four-octet IP address followed by a two-octet UDP port number (both of which shall be transmitted most significant octet first) shall function as the MAC address.

A BACnet/IP network shall function in concept identically to the other non-IP network types with respect to directed messages and broadcast messages, including local, remote, and global broadcasts, as defined in 6.3.2: a directed message shall be sent directly to the destination node; a "local broadcast" shall reach all nodes on a single B/IP network; a "remote broadcast" shall reach all nodes on a single BACnet network with network number different from that of the originator's network; a "global broadcast" shall reach all nodes on all networks.

BACnet/IP Packet

0x81	BVLC Type	1 octet
BVLC Function		1 octet
Length (inclusive)		2 octets, most significant octet first, includes BVLC Type and Function.
Optional BVLC data		} Varies depending on the BVLC Function
Optional NPDU		
Optional APDU		

3

Note that each BVLL message has at least three fields. The 1-octet BVLC Type field indicates which underlying communication subsystem or microprotocol is in use. In this case, a BVLC Type of X'81' indicates the use of BACnet/IP as defined in this Annex. The 1-octet BVLC Function field identifies the specific function to be carried out in support of the indicated communication subsystem or microprotocol type. The 2-octet BVLC Length field is the length, in octets, of the entire BVLL message, including the two octets of the length field itself, most significant octet first.

Essential Packet Types

- Original-Unicast-NPDU (0x0A)
- Original-Broadcast-NPDU (0x0B)
- Forwarded-NPDU (0x04)

4

Although there are 12 BVLC functions defined, only 3 are essential for a BACnet/IP device. 9 BVLC functions are defined to serve BACnet Broadcast Management Devices.

Original-Unicast-NPDU

0x81	BVLC Type	1 octet
0x0A	BVLC Function	1 octet
Length (inclusive)		2 octets, most significant octet first, includes BVLC Type and Function.
NPDU		} Variable Length
APDU		

5

This message is used to send directed NPDUs to another B/IP device or router.

Original-Broadcast-NPDU

0x81	BVLC Type	1 octet
0x0B	BVLC Function	1 octet
Length (inclusive)		2 octets, most significant octet first, includes BVLC Type and Function.
NPDU		} Variable Length
APDU		

6

This message is used by B/IP devices and routers which are not foreign devices to broadcast NPDU's on a B/IP network.

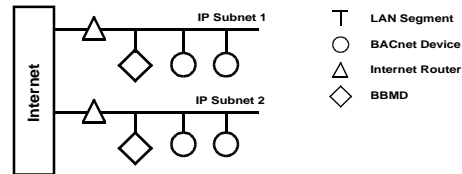
Forwarded-NPDU

0x81	BVLC Type	1 octet
0x04	BVLC Function	1 octet
Length (inclusive)		2 octets, most significant octet first, includes BVLC Type and Function.
BACnet/IP Address of Originating Device		4 octets
0xBA	IP Port Number of Originating Device	2 octets (port number may vary)
0xC0		
NPDU		} Variable Length
APDU		

7

This BVLL message is used in broadcast messages from a BBMD as well as in messages forwarded to registered foreign devices. It contains the source address of the original node as well as the original BACnet NPDU.

Broadcast Management



8

J.4.3 BBMD Concept

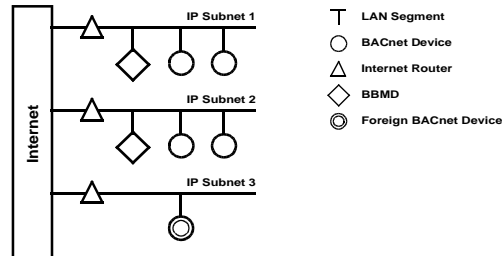
Each IP subnet that is part of a B/IP network comprised of two or more subnets shall have one, and only one, BBMD. Each BBMD shall possess a table called a Broadcast Distribution Table (BDT) which shall be the same in every BBMD in a given B/IP network. If the BBMD has also been designated to register foreign devices as described below, it shall also possess a Foreign Device Table (FDT).

J.4.3.1 Broadcast Distribution

There are two ways that a BBMD may distribute broadcast messages to remote IP subnets. The first is to use IP "directed broadcasts" (also called "one-hop" distribution). This involves sending the message using a B/IP address in which the network portion of the address contains the subnet of the destination IP subnet and the host portion of the address contains all 1's. While this method of distribution is efficient, it requires that the IP router serving the destination subnet be configured to support the passage of such directed broadcasts.

Since not all IP routers are configured to pass directed broadcasts, a BBMD may be configured to send a directed message to the BBMD on the remote subnet ("two-hop" distribution) which then transmits it using the B/IP broadcast address. Since the use of one-hop distribution requires an IP router configuration that may or may not be possible, while the two-hop method is always available, the choice of which method to use in any given case is a local matter.

Foreign Device Registration



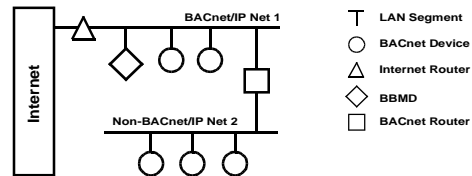
9

A "foreign" device is a BACnet device that has an IP subnet address different from those comprising the BACnet/IP network that the device seeks to join. The foreign device may be a full-time node on the foreign subnet or may be a part-time participant, as would be the case if the device accessed the internet via a SLIP or PPP connection. See Figure J-3.

J.5.2 BBMD Operation - Foreign Devices

In order for a foreign device to fully participate in the activities of a B/IP network, the device must register itself with a BBMD serving one of the IP subnets comprising that network. "Full participation" implies the ability to send and receive both directed and broadcast messages. Registration consists of sending a BVLL Register-Foreign-Device message to an appropriate BBMD and receiving a BVLC-Result message containing a result code of X'0000' indicating the successful completion of the registration. Ascertaining the IP address of such a BBMD is a local matter but could involve the use of a domain nameserver or the distribution of a numeric IP address to authorized users. The UDP port X'BAC0' shall be considered the default, but the use of other port values is permitted if required by the local network architecture, e.g., where two B/IP networks share the same physical LAN.

BACnet/IP Routing



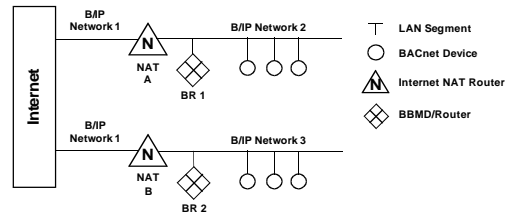
10

n concept, a router between a B/IP network and a non-B/IP network functions identically to the routers described in Clause 6.

There are two possible differences. First, on the B/IP side, the B/IP address is used in place of the MAC layer address referred to throughout Clause 6. Second, if B/IP and non-B/IP BACnet devices reside on the same physical LAN, then all traffic is typically sent and received through a single physical port. The collection of B/IP devices would, in such a case, have a network number distinct from the network number of the non-B/IP devices. Such a scenario could easily occur on an Ethernet network where some devices are IP-capable while others are not.

BACnet/IP and NAT

135-2004 Addendum o
Accommodates remote operator access via Annex J
BACnet/IP through NAT firewalls.



11

Figure J-7. The configuration of the NAT and BBMD / Router devices is described as follows:

NAT A Configuration

Internet IP 201.1.1.1

Forward 201.1.1.1:47808 □ 192.168.1.1:47809

NAT B Configuration

Internet IP 202.2.2.2

Forward 202.2.2.2:47808 □ 192.168.1.1:47809

BR1 - BBMD/Router Configuration

Global IP Address 201.1.1.1:47808 (public B/IP address of NAT A)

B/IP Address Net 1 192.168.1.1:47809

BDT Net 1 192.168.1.1:47809 (self), 202.2.2.2:47808 (public B/IP of NAT B)

B/IP Address Net 2 192.168.1.1:47808

BDT Net 2 192.168.1.1:47808 (self)

BR2 - BBMD/Router Configuration

Global IP Address 202.2.2.2:47808 (public B/IP address of NAT B)

B/IP Address Net 1 192.168.1.1:47809

BDT Net 1 192.168.1.1:47809 (self), 201.1.1.1:47808 (public B/IP of NAT A)

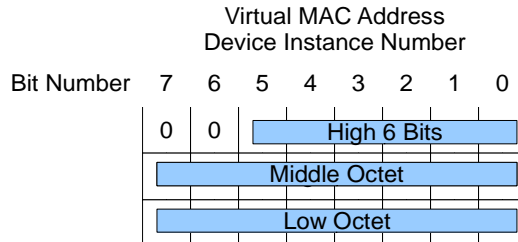
B/IP Address Net 3 192.168.1.1:47808

BDT Net 3 192.168.1.1:47808 (self)

The NAT devices translate public Internet IP/Port addresses into private addresses. Different networks behind NAT devices may use the same IP/Port address range as demonstrated here.

BACnet/IP and IPv6

135-2004 Addendum q
Define virtual addressing for data links with MAC
addresses longer than 6 octets



12

H.X Virtual MAC Addressing (NORMATIVE)

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 employ 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 over its data link. The data link translates from a native MAC addresses to a VMAC addresses when BACnet messages are received over its data link. 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.

A particular data link layer specification might specify that each node's BACnet device instance is to be used as the VMAC address for the node.