Revised December 21, 2024

B3075/B3076 Cybersecurity Disclosure

The Cimetrics B3075 and B3076 products are BACnet Network Segmentation Devices (BNSDs) that are deployed in large BACnet-based systems to segment BACnet/IP networks.

The B3075 and B3076 have identical cybersecurity-related functionality. All information about the B3075 in this document is also applicable to the B3076. To request further information, please contact Cimetrics product support via email (support@cimetrics.com) or via our website (https://www.cimetrics.com/pages/contact-us).

Table of Contents

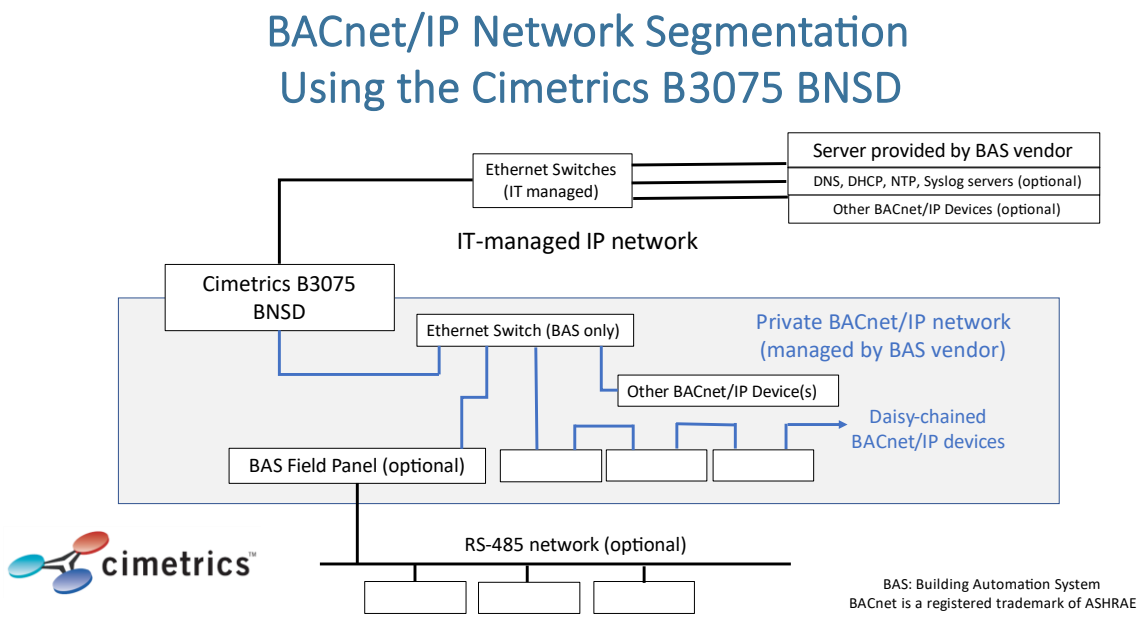
cimetrics™

Product Overview

The B3075 is a hardware appliance that forwards selected BACnet/IP packets between two directly connected Ethernet networks. It is designed to meet the requirements of ANSI/ASHRAE Standard 135 (specifically Clause 6 and Annex J). The B3075 is not an IP router, and it does not support IP routing protocols such as BGP. It does not use IPv6.

In a typical installation the B3075's Customer network port is connected to the facility's shared TCP/IP network (often managed by the IT department), and the B3075's Private network port is connected to a local area network installed by the building automation system integrator for the exclusive use of the building automation system. The B3075's Configuration network port is exclusively used for web-based configuration and diagnostics.

The following diagram illustrates a simple BACnet internetwork incorporating a B3075:



An observer monitoring network traffic on the IT-managed network (see diagram above) will note that the IP address of the B3075's Customer network port will be used for all IP messages sent, received, or forwarded by the B3075.

The B3075 plays a similar role in BACnet internetworks as the legacy B3070, but the B3075 has been enhanced to meet modern IT requirements. Some of the significant differences between the B3070 firmware and the B3075 firmware are summarized in the table below.

Feature	B3070 Ver. 1.0	B3075
Operating system	Debian 8	Debian 11
Ethernet ports used for configuration management	Configuration port	All ports[1]
Configuration management interface protocol	HTTP	HTTPS (using TLS)
Loadable private key and digital certificate for HTTPS	N/A	Yes
Modifiable ‘admin’ account password	No	Yes[2]
OpenVPN virtual NIC (TAP mode)	No	Private port[3]
NTP client for time synchronization	No	Yes[4]
Syslog client for event reporting	No	Yes[5]
DNS client	No	Yes[6]
Packet capture on Customer and Private ports	No	Yes[7]
Assignment of IP address on Customer port	Static	Static or from DHCP
Designed to enable compliance with GSA requirements	No	Yes[8]
Warning banner on login screen	No	Configurable

Cybersecurity-Related Characteristics

Firmware

The B3075’s operating system is currently based on Debian 11 (64-bit), and contains only the minimum necessary packages to implement the B3075’s functionality. The B3075 incorporates a simple web server to allow easy product configuration and diagnostics. Updated firmware will be made available when required to address serious cybersecurity vulnerabilities.

[1] By default, only the Configuration port is enabled for configuration management.
[2] The ‘admin’ account password must be modified on first use.
[3] The OpenVPN-compatible server is attached to the Customer port. It is disabled by default.
[4] The use of NTP to automatically set the system time is optional.
[5] The use of syslog to transmit system events is optional.
[6] The DNS client performs name resolution for enabled services such as NTP and syslog.
[7] Packet capture functionality is disabled by default. It can be enabled from the configuration interface.
[8] See the section of this document that describes configuration for GSA compliance.

Configuration Management

The B3075 can be configured using a web browser running on a PC that is directly connected to the dedicated Configuration port. Optionally remote configuration can be enabled on the other two ports. The administrative ("admin") account must be used in order to make configuration changes. The basic configuration parameters consist of networking parameters such as IP addresses and the desired BACnet UDP ports, plus BACnet networking information (a BACnet network number for each port and the BACnet Device ID). There are several other configuration parameters that are relevant to the B3075's optional functionality, and they are described below. The B3075's configuration settings can be saved and reloaded through its Configuration port.

Authentication & Access Control

There is always one administrative account, which has a fixed username ("admin") and a user-modifiable password that must be changed upon first use. There is also one optional "user" account with limited (read-only) privileges that can be set up using the administrative account.

Physical access to the B3075 should be restricted in order to limit access to the Configuration port. System integrators typically install B3075s in mechanical equipment spaces or control equipment closets. These generally have standard locks and keys, and for added security the B3075 can be installed in a secure data closet.

Privacy Considerations

The B3075 is intended for use as a component of a BACnet-based building automation system (BAS). As such, it does not have any role in security controls related to privacy, such as HIPAA, PCI, or PII. The B3075 simply forwards the necessary BACnet packets between two BACnet/IP networks as specified in *ANSI/ASHRAE Standard 135*. If privacy controls are required on the BAS network, they need to be enforced at the end nodes.

Network Protocols

The B3075 is designed to use a minimal set of network protocols. The B3075 communicates with other BACnet devices using UDP on a specific UDP port chosen by the building automation system integrator, typically 47808. The B3075 also supports ICMP (for monitoring) and uses ARP for address resolution. It supports HTTPS (TCP port 443) on its dedicated, physically separate, Configuration port and on the other two network ports if enabled.

A DNS client, a DHCP client, an NTP client, and a syslog client can be enabled if desired. Likewise, if VPN functionality is desired a built-in OpenVPN-compatible server can be configured and enabled.

Encryption and Key Management

As per ANSI/ASHRAE Standard 135, BACnet/IP communication is not encrypted. The B3075's use of network encryption is limited to the TLS protocol used by its built-in web server. The B3075 ships with a private key and a corresponding self-signed certificate, both of which can be replaced through the configuration interface.

Time Management

The B3075 has a real-time clock that can be set manually during device configuration or automatically using the built-in NTP client. The current time is used in the packet capture and event logging (syslog) functions of the B3075, but it is not used in the core BACnet functionality.

VPN Functionality

In order to permit communication between devices connected to the Customer network and devices on the Private network using protocols other than BACnet, the B3075 may act as a VPN server using TAP mode. This functionality is disabled by default.

If enabled, an OpenVPN server in the B3075 listens for a connection from a VPN client (OpenVPN Community Edition) on the Customer and Private ports. It creates a virtual NIC on the Private port at a configurable IP address. An administrator can configure and set up one or two distinct OpenVPN servers (with distinct virtual NICs): one is protected with a shared secret (the secret is generated by B3075 and the file containing the secret can be downloaded by the administrator), but the other one is completely open and insecure. The insecure one automatically shuts down after a configurable amount of time (no more than one month).

Packet Capture

The B3075 can be configured to allow the capture of BACnet packets on its Customer and Private ports. This feature, which is off by default, is primarily used to assist in the diagnosis of BACnet communication problems. Packet capture files can be stored in RAM for download using a web browser or saved on a USB file storage device plugged into the B3075. See the *B3075 User's Manual* for details.

Event Logging

The B3075 can be configured to send internally generated event messages to an external syslog server. Please note that this is currently the only way to view the B3075's logged events.

Configuration for GSA Compliance

The B3075 is designed to be configurable to achieve compliance with GSA's current IT security requirements. Please consult GSA *CIO 2100.1* for details. The following initial configuration steps should be performed in addition to BACnet-related configuration:

1. Change the password for the "admin" account. The new password must conform to the GSA's current password complexity requirement.

2. The B3075's web server (lighttpd) uses a private key and a corresponding digital certificate. Load a new private key and a corresponding digital certificate to replace the private key and the self-signed certificate that are pre-installed. See the *B3075 User's Manual* for information about supported file formats.

3. Optionally, enter the IP address of a reachable DNS server. Hostname resolution will not work if the DNS server is not reachable.

4. Enter the IP address or hostname of an NTP server. The B3075 will operate even if the NTP server is not reachable.

5. Configure a connection to a remote syslog server. The B3075 will operate even if the syslog server is not reachable.

6. Configure the warning banner as per GSA's current requirement.

7. Disable all optional functionality whose use is prohibited by GSA.

8. Save the configuration and then activate the changes, which will cause the device to reboot.

Reset to Factory Defaults

The B3075 can be reset in two ways:

1. The logged-in administrator can initiate a reset at any time.
2. Anyone can trigger a reset by connecting a USB mouse to one of the B3075's USB ports, power cycling the B3075, navigating to the login screen of the configuration interface using the Configuration port, and then selecting the appropriate option. After the reset is initiated, the USB mouse must be removed.

Either method will cause the B3075 to revert to its factory default configuration and to reboot in that state. All user-modified configuration settings will be erased, including passwords.