BACnet Protocol

Building Automation and Control Networks protocol

OT Security Learning Series

Document 205 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction **3**

2 Protocol Architecture **3**
2.1 Network Options . . . 3
2.2 Object Model . . . 4

3 Network Communication **4**
3.1 BACnet/IP Details . . . 4
3.2 Key Services . . . 4
3.3 Broadcast Management Device (BBMD) . . . 4

4 Security Vulnerabilities **5**
4.1 Protocol Weaknesses . . . 5
4.2 Attack Vectors . . . 5
4.3 Internet Exposure . . . 5

5 BACnet Secure Connect (BACnet/SC) **5**
5.1 BACnet/SC Features . . . 6
5.2 Adoption Challenges . . . 6

6 Security Mitigations **6**
6.1 Network Segmentation . . . 6
6.2 Access Controls . . . 6
6.3 Monitoring . . . 6

7 Building Automation Context **7**
7.1 Critical Facility Risks . . . 7
7.2 Convergence with OT . . . 7

8 Summary **7**

9 Further Reading **7**

1 Introduction

Information

BACnet (Building Automation and Control Networks) is the dominant protocol for building automation systems. It controls HVAC, lighting, access control, fire systems, and elevators in commercial buildings, hospitals, data centers, and critical facilities.

Key characteristics:

- ASHRAE/ANSI/ISO standard (ISO 16484-5)
- Designed for building automation interoperability
- Supports multiple network technologies
- Object-oriented data model
- Used in critical infrastructure (hospitals, data centers)

2 Protocol Architecture

2.1 Network Options

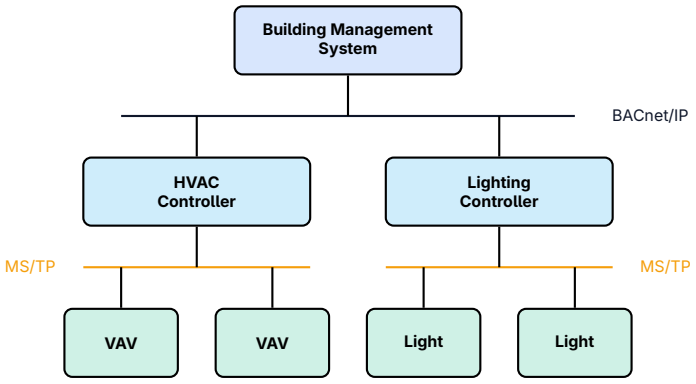

Figure 1: BACnet Building Automation Architecture

BACnet can run over multiple network types:

Network	Common Name	Use Case
BACnet/IP	UDP/47808	Primary modern deployment
BACnet/Ethernet	802.3 direct	Legacy installations
BACnet MS/TP	RS-485 serial	Field-level devices
BACnet/SC	Secure Connect	TLS-secured BACnet/IP

Table 1: BACnet Network Types

2.2 Object Model

BACnet Objects

BACnet uses an object-oriented model where everything is represented as objects with properties:

- **Analog Input/Output** – Temperature, pressure, setpoints
- **Binary Input/Output** – On/off states, alarms
- **Schedule** – Time-based control programs
- **Trend Log** – Historical data storage
- **Device** – Represents the device itself

3 Network Communication

3.1 BACnet/IP Details

Port	Protocol	Purpose
UDP/47808	BACnet/IP	Standard communication
UDP/47808	BBMD	Broadcast management
TCP/47808	BACnet/IP (rare)	Some implementations

Table 2: BACnet/IP Network Ports

3.2 Key Services

- **Who-Is / I-Am** – Device discovery
- **ReadProperty** – Read object properties
- **WriteProperty** – Modify object properties
- **SubscribeCOV** – Change of Value notifications
- **DeviceCommunicationControl** – Enable/disable device
- **ReinitializeDevice** – Reboot or reset device

3.3 Broadcast Management Device (BBMD)

Warning

BBMDs forward BACnet broadcasts across IP subnets. A compromised or misconfigured BBMD can expose BACnet networks to wider attack surface.

4 Security Vulnerabilities

Critical

Traditional BACnet has no authentication or encryption. Any device on the network can read, write, and control building systems. This is particularly dangerous given BACnet's presence in critical facilities.

4.1 Protocol Weaknesses

- **No authentication** – All commands accepted from any source
- **No encryption** – Traffic easily intercepted
- **Broadcast discovery** – Easy to enumerate all devices
- **Powerful commands** – ReinitializeDevice, WriteProperty
- **Internet exposure** – Many systems accessible online

4.2 Attack Vectors

- **HVAC manipulation** – Change temperatures to damage equipment or create discomfort
- **Access control** – Unlock doors, disable alarms
- **Fire system interference** – Suppress alarms or trigger false alarms
- **Energy attacks** – Maximize energy consumption
- **Device disruption** – ReinitializeDevice to cause outages
- **Data exfiltration** – Read occupancy patterns, schedules

4.3 Internet Exposure

Warning

Thousands of BACnet devices are directly accessible on the internet. Shodan and similar tools easily find them via port 47808/UDP.

5 BACnet Secure Connect (BACnet/SC)

Key Point

BACnet/SC is a security-focused update that adds TLS encryption and certificate-based authentication while maintaining BACnet compatibility.

5.1 BACnet/SC Features

- **TLS 1.3** – Encrypted communications
- **X.509 certificates** – Device authentication
- **Hub-and-spoke topology** – Primary/failover hubs
- **WebSocket transport** – Firewall-friendly
- **Backward compatible** – Routers bridge to legacy

5.2 Adoption Challenges

- Requires new hardware or firmware updates
- Certificate management complexity
- Performance overhead
- Mixed environments need careful planning

6 Security Mitigations

6.1 Network Segmentation

- **Dedicated VLAN** – Isolate BACnet traffic
- **Firewall BACnet** – Block 47808 at network perimeter
- **No internet exposure** – Never expose directly online
- **Segment by function** – Separate HVAC, access control, fire

6.2 Access Controls

- Restrict physical access to BACnet infrastructure
- Use VPN for remote building management access
- Implement IP allowlists where possible
- Audit who has access to building automation systems

6.3 Monitoring

- Log all WriteProperty and ReinitializeDevice commands
- Alert on Who-Is broadcasts from unknown sources
- Monitor for unexpected schedule or setpoint changes
- Detect devices appearing or disappearing

- Watch for after-hours control activity

7 Building Automation Context

7.1 Critical Facility Risks

BACnet controls systems in:

- **Hospitals** – HVAC for operating rooms, isolation wards
- **Data centers** – Cooling systems (overheating = outage)
- **Pharmaceutical** – Clean room environmental control
- **Government** – Secure facility access control

7.2 Convergence with OT

Building automation increasingly connects to:

- Enterprise IT networks
- Cloud-based management platforms
- IoT sensors and analytics
- Smart grid demand response

8 Summary

Key Takeaways

- **Building automation standard** – HVAC, lighting, access, fire
- **BACnet/IP dominant** – UDP port 47808
- **No native security** – Traditional BACnet lacks authentication
- **Internet exposure common** – Many systems directly online
- **BACnet/SC** – New secure option with TLS, limited adoption
- **Critical facilities** – Hospitals, data centers at risk
- **Network isolation essential** – Never expose to internet

9 Further Reading

Standards

- **ASHRAE – BACnet Standards**
  https://www.bacnetinternational.org/

- **ISO 16484-5** – Building automation standard
  https://www.iso.org/standard/79079.html

Resources

- **CISA – Building Automation Security**
  https://www.cisa.gov/topics/industrial-control-systems
- **BACnet International**
  https://www.bacnetinternational.org/

Part of the OT Security Learning Series