# 1 PURPOSE

The purpose of this standard is to define data communication services and protocols for computer equipment used for monitoring and control of HVAC&R and other building systems and to define, in addition, an abstract, object-oriented representation of information communicated between such equipment, thereby facilitating the application and use of digital control technology in buildings.

# 2 SCOPE

**2.1** This protocol provides a comprehensive set of messages for conveying encoded binary, analog, and alphanumeric data between devices including, but not limited to:

(a) hardware binary input and output values,
(b) hardware analog input and output values,
(c) software binary and analog values,
(d) text string values,
(e) schedule information,
(f) alarm and event information,
(g) files, and
(h) control logic.

**2.2** This protocol models each building automation and control computer as a collection of data structures called "objects," the properties of which represent various aspects of the hardware, software, and operation of the device. These objects provide a means of identifying and accessing information without requiring knowledge of the details of the device's internal design or configuration.

# 3 DEFINITIONS

## 3.1 Terms Adopted from International Standards

The following terms used in this standard are defined by international standards or draft standards for open system interconnection (OSI). The definitions are repeated here and a reference to the appropriate standard is provided. Clause 25 contains the titles of all national and international standards referenced in this clause and elsewhere in this standard. Words or phrases in italics refer to terms defined elsewhere in this clause.

**abstract syntax:** the specification of application layer data or *application-protocol-control-information* by using notation rules which are independent of the encoding technique used to represent them (ISO 8822).

**application:** a set of a USER's information processing requirements (ISO 8649).

**application-entity:** the aspects of an *application-process* pertinent to OSI (ISO 7498).

**application-process:** an element within a *real open system* which performs the information processing for a particular *application* (ISO 7498).

**application-protocol-control-information:** information exchanged between *application-entities*, using presentation services, to coordinate their joint operation (ISO 9545).

**application-protocol-data-unit:** a unit of data specified in an application protocol and consisting of *application-protocol-control-information* and possibly application-user-data (ISO 9545).

**application-service-element:** that part of an *application-entity* which provides an OSI environment capability, using underlying services when appropriate (ISO 7498).

**concrete syntax:** those aspects of the rules used in the formal specification of data which embody a specific representation of that data (ISO 7498).

**confirm (primitive):** a representation of an interaction in which a *service-provider* indicates, at a particular *service-access-point*, completion of some procedure previously invoked, at that *service-access-point*, by an interaction represented by a *request* primitive (ISO TR 8509).

**indication (primitive):** a representation of an interaction in which a *service-provider* either
(a) indicates that it has, on its own initiative, invoked some procedure; or
(b) indicates that a procedure has been invoked by the *service-user* at the peer *service-access-point* (ISO TR 8509).

**peer-entities:** *entities* within the same layer (ISO 7498).

**real open system:** a *real system* which complies with the requirements of OSI standards in its communication with other *real systems* (ISO 7498).

**real system:** a set of one or more computers, the associated software, peripherals, terminals, human operators, physical processes, information transfer means, etc., that forms an autonomous whole capable of performing information processing and/or information transfer (ISO 7498).

**request (primitive):** a representation of an interaction in which a *service-user* invokes some procedure (ISO TR 8509).

**response (primitive):** a representation of an interaction in which a *service-user* indicates that it has completed some procedure previously invoked by an interaction represented by an *indication* primitive (ISO TR 8509).

**(N)-service-access-point:** the point at which (N)-services are provided by an (N)-*entity* to an (N+1)-*entity* (ISO 7498).

**(N)-service-data-unit:** an amount of (N)-interface-data whose identity is preserved from one end of an (N)-connection to the other (ISO 7498).

**service-user**: an *entity* in a single open system that makes use of a service through *service-access-points* (ISO TR 8509).

**service-primitive**; **primitive**: an abstract, implementation-independent representation of an interaction between the *service-user* and the *service-provider* (ISO TR 8509).

**service-provider**: an abstract of the totality of those entities which provide a service to peer *service-users* (ISO TR 8509).

**transfer-syntax:** that *concrete syntax* used in the transfer of data between open systems (ISO 7498).

**user element:** the representation of that part of an *application-process* which uses those *application-service-elements* needed to accomplish the communications objectives of that *application-process* (ISO 7498).

### 3.2 Terms Defined for this Standard

**access control:** a method for regulating or restricting access to *network resources*.

**access rights (physical access control):** the access privileges granted to a credential.

**access user (physical access control):** the person or asset holding one or more credentials.

**alarm: 1.** An annunciation, either audible or visual or both, that alerts an operator to an off-normal condition that may require corrective action. **2.** An abnormal condition detected by a device or controller that implements a rule or logic specifically designed to look for that condition.

**algorithmic change reporting:** the detection and reporting of an alarm or event, based on an algorithm specified in an Event Enrollment object. See *intrinsic reporting*.

**authentication:** the act of verifying identity

**authentication factor:** a data element of the credential which is used to verify a credential's identity.

**authorization (network security):** the control of access to network resources based on known identity and access rules.

**authorization (physical access control):** the process of determining whether the access user is permitted to enter a protected zone through an access controlled point.

**BACnet device:** any device, real or virtual, that supports digital communication using the BACnet protocol.

**BACnet-user:** that portion of an *application-process* that is represented by the BACnet *user element*.

**bridge:** a device that connects two or more *segments* at the physical and data link layers. This device may also perform message filtering based upon MAC layer addresses.

**broadcast:** a message sent as a single unit, which may apply to more than one device.

**change of state:** an event that occurs when a measured or calculated Boolean or discrete enumerated value changes.

**change of value:** an event that occurs when a measured or calculated analog value changes by a predefined amount.

**client:** a system or device that makes use of another device for some particular purpose via a service *request* instance. A client requests service from a *server*.

**context:** a set of data or information that completely describes a particular communication environment at a particular point in time.

**controller:** a device for regulation or management of a system or component.

**credential (physical access control):** the combination of authentication factors and access rights.

**data confidentiality:** the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

**data integrity:** the property that data has not been altered or destroyed in an unauthorized manner.

**data origin authentication:** the corroboration that the source of data received is as claimed.

**date pattern:** a date that may contain one or more unspecified octets or special date values.

**directly connected network:** a network that is accessible from a router without messages being relayed through an intervening router. A PTP connection is to a directly connected network if the PTP connection is currently active and no intervening router is used.

**download:** a particular type of file transfer that refers to the transfer of an executable program or database to a remote device where it may be executed.

**encrypted message:** a message that is wrapped in a security header, signed, and encrypted.

**entity:** something that has a separate and distinct existence. An identifiable item that is described by a set or collection of properties.

**error detection:** a procedure used to identify the presence of errors in a communication.

**error recovery:** a procedure invoked in response to a detected error that permits the information exchange to continue.

**gateway:** a device that connects two or more dissimilar *networks*, permitting information exchange between them.

**global:** pertaining to all devices or nodes on a communication *internetwork*.

**global broadcast:** a message addressed to all devices or *nodes* on all *networks* in a BACnet *internet*.

**half router:** a device or *node* that can participate as one partner in a PTP connection. The two half-router partners that form an active PTP connection together make up a single *router*.

**incapable device:** a device that is inherently incapable, or has been configured to be appear to be incapable, of producing or consuming secure BACnet messages. All incapable devices are plain devices.

**initialization:** the process of establishing a known state, usually from a power up condition. Initialization may require re-establishment of a node's logical or physical address.

**internetwork:** a set of two or more *networks* interconnected by *routers*. In a BACnet *internetwork*, there exists exactly one message path between any two nodes.

**intrinsic reporting:** the detection and reporting of an alarm or event, based on an algorithm defined as part of the *object type* specification. No external reference to an Event Enrollment is involved. See *algorithmic change reporting*.

**inverted network:** a BACnet internetwork where two or more networks are connected by a network with an NPDU size smaller than the networks it joins.

**key:** a sequence of symbols that controls the operations of encipherment and decipherment.

**local:** pertaining to devices on the same *network* as the referenced device.

**local broadcast:** a message addressed to all devices or *nodes* on the same *network* as the originator.

**medium:** the physical transmission *entity*. Typical media are twisted-pair wire, fiber optic cable, and coaxial cable.

**medium access control:** a process used to maintain order and provide access to the communication *medium*.

**network:** a set of one or more *segments* interconnected by *bridges* that have the same network address.

**network resource:** any physical or logical *entity* that may be accessed via a communication *medium*.

**node:** an addressable device connected to the communication *medium*.

**object**: a specific instance of an *object type*. While an object type is identified by a unique Object_Type property, an object is identified by its Object_Identifier property.

**object profile:** an object profile is a means of defining objects beyond those defined in Clause 12. A profile defines the set of properties, behavior, and/or requirements for a proprietary object, or for proprietary extensions to a standard object.

**object type:** a generic classification of data that is defined by a set of *properties*.

**operator authentication:** the corroboration that the operator logging on to a device is as claimed.

**peer entity authentication:** the corroboration that a peer entity in an association is the one claimed.

**physical access control (PACS):** an electronic system that controls the ability of people or vehicles to enter a protected area, by means of authentication and authorization at access control points.

**physical segment:** a single contiguous *medium* to which BACnet nodes are attached.

**physically insecure:** not physically secure.

**physically secure:** a device or network that is protected from physical access by unauthorized individuals.

**plain device:** a device that does not normally produce or consume secure BACnet messages. All incapable devices are plain devices. However, a plain device that is not an incapable device is capable of producing or consuming secure BACnet messages when communicating with another device that requires it.

**plain network:** a network that does not require signed or encrypted traffic.

**plain message:** a message that is not secured by a BACnet security wrapper.

**printable character:** a character that represents a printable symbol as opposed to a device control character. Printable characters include, but are not limited to, upper- and lowercase letters, punctuation marks, and mathematical symbols. The exact set depends upon the character set being used.

**property:** a particular characteristic of an *object type*.

**proprietary:** within the context of BACnet, any extension of or addition to *object types*, *properties*, PrivateTransfer services, or enumerations specified in this standard.

**receiving BACnet-user:** the *BACnet-user* that receives an *indication* or *confirm* service primitive.

**remote:** pertaining to devices or *nodes* on a different *network* than the referenced device.

**remote broadcast:** a message addressed to all devices or *nodes* on a different *network* than the originator.

**repeater:** a device that connects two or more *physical segments* at the physical layer.

**requesting BACnet-user:** the *BACnet-user* that assumes the role of a *client* in a confirmed service.

**responding BACnet-user:** the *BACnet-user* that assumes the role of a *server* in a confirmed service.

**role-based access control (RBAC):** access privileges that are assigned to specific roles. Access users acquire privileges through their assigned role.

**router:** a device that connects two or more *networks* at the network layer.

**secure network:** a network on which all traffic is required to be signed or encrypted.

**security:** any of a variety of procedures used to ensure that information exchange is guarded to prevent disclosure to unauthorized individuals. Security measures are intended to prevent disclosure of sensitive information even to those who have valid access to the communication *network*. Security is distinct from access control, although some security can be provided by limiting physical access to the communication medium itself.

**segment:** a segment consists of one or more *physical segments* interconnected by repeaters.

**sending BACnet-user:** the *BACnet-user* that issues a *request* or *response* service primitive.

**server:** a system or device that responds to a service *request* instance for some particular purpose. The server provides service to a *client*.

**signed message**: a message that is wrapped in a security header, signed, and not encrypted.

**special date value:** a date value that is one of the special values such as "even months", "last day of month", etc. These special date values are used in subcomponents (octets) of a value of type Date.

**specific date:** a fully specified date. For example, January 24, 1991, Day of week = Thursday. A specific date shall contain no unspecified octets or Special Date Values.

**specific datetime:** a BACnetDateTime construct composed of a specific date and a specific time.

**specific time:** a fully specified time. For example, 17:35:45.17 (= 5:35:45.17 P.M.). A specific time shall contain no unspecified octets.

**standard object type:** an object type defined by this standard where the numerical value is within the range reserved for ASHRAE.

**standard property:** a required or optional property of a standard object type where the numerical value of the property identifier is within the range reserved for ASHRAE and the property is listed in the object type's properties table in Clause 12.

**synchronization:** a facility that allows processes to define and identify specific places in a transmission or exchange that can be used to reset a communication session to a predefined state.

**time pattern:** a time that may contain one or more unspecified octets.

**timestamp:** the indication of the point in time recorded for and accompanying the record of an event or operation.

**trusted:** a term used to refer to devices or networks from which messages are believed to be authentic, either through the use of secure messages or based on the physical security of that device or network.

**unit_time:** the length of time required to transmit one octet with a start bit and a single stop bit. Ten bit-times.

**unspecified date:** a date composed entirely of unspecified octets (A value of X'FF' = D'255').

**unspecified datetime:** a BACnetDateTime construct composed of an unspecified date and an unspecified time.

**unspecified octet:** an octet used in the context of date, time or BACnetWeekNDay values that contains the value X'FF' = D'255'.

**unspecified time:** a time composed entirely of unspecified octets (A value of X'FF' = D'255').

**upload:** the process of transferring an executable program image or a database from a remote device in such a manner as to allow subsequent download.

### 3.3 Abbreviations and Acronyms Used in this Standard

| | |
|---|---|
| **A** | application layer (prefix) |
| **ABA** | American Bankers Association |
| **AE** | application entity |
| **ANSI** | American National Standards Institute |
| **APCI** | application protocol control information |
| **APDU** | application layer protocol data unit |
| **API** | application program interface |
| **ARCNET** | attached resource computer network |
| **ASE** | application service element |
| **ASN.1** | Abstract Syntax Notation One (ISO 8824) |
| **B' '** | denotes that binary notation is used between the single quotes |
| **BAC** | building automation and control |
| **BBMD** | BACnet/IP broadcast management device |
| **BDT** | broadcast distribution table |
| **B/IP** | BACnet/IP |
| **B/IP-M** | BACnet/IP multicast |
| **BVLC** | BACnet virtual link control |